ODLICZAJĄC DO ZERO

DNIA

X

KIM ZETTER

X

STUXNET, CZYLI PRAWDZIWA HISTORIA CYFROWEJ BRONI

Helion

Helion kocha dla: Adam Kufel adam.kufel@gmail.com

Tytuł oryginału: Countdown to Zero Day:
Stuxnet and the Launch of the Worlds First Digital Weapon

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-283-3713-8

Copyright © 2014 by Kim Zetter. All rights reserved.

This translation published by arrangement with Crown, an imprint
of the Crown Publishing Group, a division of Penguin Random House LLC.

CROWN and the Crown colophon are registered trademarks of Random House LLC.

Portions of this work were originally published in different form in "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" copyright © Wired.com. Used with permission. First published July 2011.

Polish edition copyright © 2018 by Helion SA. All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock Images LLC.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/oddodn_ebook
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

- Poleć książkę na Facebook.com
- Kup w wersji papierowej
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dla S. C. i moich rodziców z miłością i wielką wdzięcznością;
ta druga jest niewystarczająca wobec tego wszystkiego,
co dla mnie zrobiliście.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

SPIS TREŚCI

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PROLOG

SPRAWA WIRÓWEK

W styczniu 2010 r. oficjele z Międzynarodowej Agencji Energii Atomowej (MAEA), jednostki Organizacji Narodów Zjednoczonych odpowiedzialnej za monitorowanie irańskiego programu nuklearnego, po raz pierwszy dostrzegli nietypowe zjawiska w zakładzie wzbogacania uranu pod Natanzem w środkowym Iranie.

W wielkiej hali, umiejscowionej jak bunkier ponad 15 m pod powierzchnią pustyni, tysiące lśniących aluminiowych wirówek obracały się z ponaddźwiękową szybkością, wzbogacając sześciofluorek uranu. Urządzenia pracowały tak już od przeszło dwóch lat. Jednak w ostatnich tygodniach pracownicy zakładu zaczęli zastępować grupy starych wirówek nowymi i robili to w wielkim pośpiechu.

W Natanzie czas życia wirówek IR-1 wynosi ok. dziesięciu lat. Urządzenia te są jednak wrażliwe na usterki i często się psują. W standardowych warunkach Iran musiał każdego roku wymieniać do 10% wirówek z powodu wad materiałowych, problemów z konserwacją lub wypadków powodowanych przez pracowników.

W listopadzie 2009 r. Irańczycy używali w Natanzie ok. 8700 wirówek, dlatego nie było niczym dziwnym, że technicy w ciągu roku wymienili mniej więcej 800 z nich, gdy urządzenia z różnych powodów zaczęły zawodzić. Jednak gdy oficjele MAEA policzyli wirówki zdemontowane w ostatnich tygodniach 2009 r. i na początku stycznia następnego roku, zrozumieli, że Iran wymieniał urządzenia z niespotykaną częstotliwością.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Inspektorzy z wydziału bezpieczeństwa MAEA odwiedzali zakład w Natanzie średnio dwa razy w miesiącu — czasem po umówieniu się, a czasem niezapowiedzianie — aby kontrolować przebieg irańskiego programu wzbogacania uranu[1]. Kiedy pracownicy zakładu wycofywali z użytku uszkodzone i nieprzydatne już urządzenia, musieli umieszczać je w obszarze kontrolnym przy drzwiach hali wirówek. Urządzenia pozostawały tam do czasu, gdy inspektorzy z MAEA mogli je skontrolować w trakcie kolejnej wizyty. Inspektorzy badali każdą wirówkę ręcznym spektrometrem promieniowania gamma, aby się upewnić, że w urządzeniach nie są przemycane materiały nuklearne, a następnie zatwierdzali usunięcie wirówek. W raportach przesyłanych do siedziby głównej MAEA w Wiedniu kontrolerzy za każdym razem podawali liczbę wycofywanych urządzeń.

Kamery cyfrowe agencji MAEA, zainstalowane przy drzwiach każdej sali wirówek na potrzeby monitorowania irańskiego programu wzbogacania uranu, zarejestrowały przemykających się techników w białych fartuchach i niebieskim plastikowym obuwiu. Technicy wynosili kolejne lśniące cylindry o długości niecałych 2 m i średnicy ok. 15 cm. Ci pracownicy, zgodnie z ustaleniami z MAEA, musieli ręcznie przenosić te delikatne urządzenia, opakowane w plastikowe rękawy lub w otwartych skrzynkach. Dzięki temu kamery mogły zarejestrować wszystko, co jest wynoszone z sal.

Kamery, nieinstalowane w salach z wirówkami, rejestrowały obraz na potrzeby późniejszych kontroli. Inspektorzy w trakcie każdej wizyty w Natanzie przeglądali zarejestrowane nagrania, aby się upewnić, że Irańczycy nie wynieśli z sal dodatkowych wirówek ani nie podjęli innych niedozwolonych działań[2]. Wraz z upływem tygodni i przesyłaniem do Wiednia kolejnych raportów kontrolerzy zauważyli, że liczba demontowanych wirówek znacznie przekroczyła normalne wartości[3].

---

[1] Liczba inspekcji w Natanzie od tego czasu wzrosła. Od 2010 r. kontrole były przeprowadzane raz w tygodniu, a od podpisania w 2013 r. nowej umowy z Iranem inspektorzy są w Natanzie każdego dnia.

[2] Inspektorzy MAEA nie mogą wynieść zarejestrowanych obrazów poza Natanz. Mogą je przeglądać tylko na miejscu, gdzie są przechowywane.

[3] Następuje regularna rotacja inspektorów kontrolujących Natanz i inne obiekty nuklearne na świecie. Dlatego kolejne wizyty mogą odbywać inni inspektorzy z MAEA. Z tego powodu na wysoką liczbę wymienionych wirówek zwrócono uwagę dopiero wtedy, gdy do Wiednia spłynęło kilka raportów na ten temat i analitycy oraz urzędnicy uzyskali zagregowane dane.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Oficjalnie MAEA nie podała, ile wirówek Iran wymienił w opisywanym okresie. W wiadomościach reporterzy cytujący europejskich „dyplomatów" oszacowali tę liczbę na 900 do 1000. Jednak jeden z byłych wysokich urzędników MAEA uważa, że w rzeczywistości liczba ta była znacznie wyższa. „Szacuję, że uszkodzonych zostało 2000 urządzeń" — powiedział Olli Heinonen, który do czasu rezygnacji w październiku 2010 r. zajmował stanowisko zastępcy dyrektora w wydziale bezpieczeństwa.

Niezależnie od liczb było oczywiste, że z urządzeniami dzieje się coś złego. Niestety, Iran nie był zobowiązany do informowania inspektorów o przyczynach wymiany wirówek. Oficjalnie inspektorzy MAEA nie mieli też prawa o to pytać. Agencja miała uprawnienia do kontrolowania tego, co dzieje się z uranem w zakładzie wzbogacania, a nie do badania uszkodzonego sprzętu.

Inspektorzy nie wiedzieli, że odpowiedzi mieli na wyciągnięcie ręki — ukryte w bitach i pamięci komputerów w sterowni przemysłowej w Natanzie. Kilka miesięcy wcześniej, w czerwcu 2009 r., ktoś dyskretnie uruchomił niszczycielską cyfrową broń na komputerach w Iranie. Ta broń po cichu wśliznęła się do krytycznych systemów w Natanzie z zadaniem dokonania sabotażu programu wzbogacania uranu i zapobieżenia zbudowaniu bomby atomowej przez prezydenta Mahmuda Ahmadineżada.

Odpowiedź znajdowała się więc w Natanzie, ale minął prawie rok, zanim inspektorzy zdołali do niej dotrzeć. Udało się to dopiero po tym, jak kilkunastu ekspertów ds. zabezpieczeń informatycznych z całego świata miesiącami analizowało coś, co zostało uznane za najbardziej zaawansowany z kiedykolwiek wykrytych wirusów. Było to oprogramowanie na tyle wyjątkowe, że przeszło do historii jako pierwsza na świecie cyfrowa broń i pierwszy strzał zwiastujący erę wojen cyfrowych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 1

PIERWSZE OSTRZEŻENIE

Siergiej Ulasen nie jest człowiekiem, jaki mógłby być zamieszany w międzynarodowy incydent. Ulasen to 31-letni Białorusin z krótko obciętymi jasnymi włosami, szczupłą, chłopięcą sylwetką, pełną otwartości twarzą i uprzejmością kogoś, kto w życiu narobił sobie niewielu wrogów i był źródłem jeszcze mniejszej liczby kontrowersji. Jedną z jego ulubionych rozrywek jest spędzanie weekendów w wiejskim domu babci pod Mińskiem, gdzie może wypocząć od codziennego stresu, z dala od zasięgu telefonów komórkowych i internetu. Jednak w czerwcu 2010 r. Ulasen trafił na coś niezwykłego, przez co szybko zdobył międzynarodową popularność i naraził się na dodatkowy stres[1].

W ciepłe czwartkowe popołudnie Ulasen, kierujący wówczas wydziałem antywirusowym małej białoruskiej firmy zajmującej się zabezpieczeniami komputerowymi, VirusBlokAda, siedział ze swoim współpracownikiem, Olegiem Kupriejewem, w biurze w centrum Mińska w szarym postsowieckim budynku niedaleko rzeki Świsłocz. Obaj metodycznie badali podejrzane pliki komputerowe, które niedawno znaleziono na komputerze w Iranie. Kupriejew nagle zauważył coś zaskakującego. Opadł na oparcie krzesła i zawołał Ulasena. Ulasen przejrzał kod raz, a potem ponownie, aby się upewnić, że zobaczył to, co mu się wydawało, że ujrzał. Cicho westchnął.

[1] Ulasen i jego zespół natrafili na to złośliwe oprogramowanie w tygodniu obejmującym 24 czerwca 2010 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Kod, który analizowali przez kilka ostatnich dni i uważali do tej pory za stosunkowo ciekawego, ale standardowego wirusa, właśnie okazał się dziełem cichego diabolicznego geniusza.

Napastnik nie tylko wykorzystał pomysłowy rootkit, aby ukryć wirusa przed programami antywirusowymi, ale też zastosował sprytny eksploit typu zero-day w celu przesyłania wirusa z komputera na komputer. Ten eksploit wykorzystywał tak podstawowy mechanizm systemu operacyjnego Windows, że na infekcję narażone były miliony komputerów.

Eksploit to używany w trakcie ataków kod, który hakerzy stosują do instalowania wirusów i innych szkodliwych narzędzi na komputerach. Eksploity wykorzystują luki w zabezpieczeniach w przeglądarkach takich jak Internet Explorer lub aplikacjach takich jak Adobe PDF Reader, aby wprowadzić do systemu wirusa lub konia trojańskiego. Podobnie włamywacz posługuje się łomem, aby podważyć okno i wejść do domu. Jeśli ofiara przejdzie do szkodliwej witryny, na której działa eksploit, lub kliknie załącznik e-maila zawierający eksploit, narzędzie wykorzysta lukę w zabezpieczeniach oprogramowania do wprowadzenia do systemu niebezpiecznych plików. Gdy producent oprogramowania odkrywa lukę w produkcie, zwykle przygotowuje „łatki", aby uniemożliwić napastnikom dostęp do aplikacji. Firmy piszące programy antywirusowe (takie jak firma Ulasena) dodają do swoich skanerów specjalne sygnatury, aby program mógł wykrywać eksploity próbujące wykorzystać luki.

Jednak eksploity typu zero-day nie są zwykłym oprogramowaniem. To najbardziej cenione w świecie hakerów narzędzia, ponieważ wykorzystują luki wciąż nieznane producentom oprogramowania i programów antywirusowych. Oznacza to, że programy antywirusowe nie obejmują sygnatur wykrywających takie eksploity. Nie istnieją też łatki zabezpieczające luki wykorzystywane przez te eksploity.

W praktyce eksploity typu zero-day są rzadkie. Odkrywanie nowych luk i pisanie wykorzystujących je eksploitów wymaga od hakerów czasu i umiejętności. Dlatego zdecydowana większość napastników do rozpowszechniania szkodliwego oprogramowania wykorzystuje znane luki i eksploity, licząc na to, że większość użytkowników komputerów nie instaluje łatek ani aktualnych programów antywirusowych. Ponadto opracowanie łatki dla znanej luki może zająć producentom tygodnie lub miesiące. Każdego roku wykrywanych jest ponad 12 mln wirusów i innych szkodliwych plików.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wśród nich znajduje się tylko kilkanaście eksploitów typu zero-day. Jednak w omawianym przypadku napastnicy zastosowali niezwykle cenny eksploit tego typu i pomysłowy rootkit na potrzeby wirusa, który — na ile Ulasen i Kupriejew mogli stwierdzić — występował tylko na komputerach w Iraku. Było to bardzo podejrzane.

TAJEMNICZE PLIKI ZWRÓCIŁY uwagę informatyków tydzień wcześniej, gdy irański dystrybutor oprogramowania firmy VirusBlokAda zgłosił uporczywy problem z komputerem klienta z tego kraju. Komputer wpadł w pętlę restartowania. Nieustannie ulegał awarii i restartował się, uniemożliwiając technikom zbadanie maszyny[2]. Zespół pomocy technicznej z firmy VirusBlokAda zdalnie (z Mińska) przeskanował system w poszukiwaniu szkodliwego oprogramowania, które program antywirusowy mógł przeoczyć, ale niczego nie znalazł. To wtedy wezwano Ulasena.

Ulasen został zatrudniony przez firmę VirusBlokAda jeszcze w trakcie studiów. Początkowo był programistą, jednak zespół w firmie był tak mały, a umiejętności Ulasena tak wysokie, że po trzech latach, w wieku 26 lat, Siergiej zaczął kierować grupą odpowiedzialną za rozwijanie i konserwację silnika programu antywirusowego. Od czasu do czasu współpracował też z zespołem badawczym analizującym zagrożenia. Było to ulubione zajęcie Ulasena, choć nieczęsto miał możliwość je wykonywać. Dlatego gdy zespół pomocy technicznej poprosił go o ocenę zagadki z Iranu, chętnie się zgodził[3].

Ulasen przyjął, że problem musi wynikać z błędnej konfiguracji oprogramowania lub z niezgodności aplikacji zainstalowanych na komputerze i systemu operacyjnego. Jednak później odkrył, że podobna awaria dotyczy większej liczby maszyn w Iranie, w tym komputerów, które administratorzy

---

[2] Ulasen nigdy nie ujawnił nazwy tego dystrybutora. Jednak w witrynie firmy VirusBlokAda odnośnik prowadzący do irańskiego dystrybutora kieruje użytkownika do witryny *vba32-ir.com*. Jest to witryna należąca do Deep Golden Recovery Corporation, irańskiej firmy zajmującej się odzyskiwaniem danych.

[3] Informacje o natrafieniu na omawiane złośliwe oprogramowanie w firmie VirusBlokAda pochodzą z wywiadów z Siergiejem Ulasenem i Olegiem Kupriejewem, a także z materiałów opublikowanych przez Kaspersky Lab w 2011 r., po tym jak ta rosyjska firma antywirusowa zatrudniła Ulasena. Wywiad *The Man Who Found Stuxnet — Sergey Ulasen in the Spotlight* został opublikowany 2 listopada 2011 r. pod adresem: *http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

sformatowali, aby od nowa zainstalować system operacyjny. Dlatego podejrzewał, że przyczyną może być robak kryjący się w sieci ofiary, ponownie infekujący sformatowane maszyny. Sądził też, że rootkit posłużył do ukrycia szkodliwego kodu przed programem antywirusowym. Ulasen w przeszłości pisał dla firmy narzędzia do zwalczania rootkitów, dlatego miał pewność, że zdoła znaleźć takie narzędzie, jeśli to ono jest problemem.

Po uzyskaniu pozwolenia na połączenie się z jedną z maszyn z Iranu i zbadanie jej Ulasen z Kupriejewem skupili się na sześciu podejrzanych plikach. Były to dwa moduły i cztery inne pliki, które zdaniem informatyków mogły stanowić źródło problemu[4]. Następnie z pomocą współpracowników Ulasen i Kupriejew poświęcili kilka dni na wyrywkowe badanie tych plików, przeklinając czasem, gdy próbowali odszyfrować zaskakująco skomplikowany kod. Pracownicy małej firmy zajmujący się głównie pisaniem programów antywirusowych dla klientów rządowych nie byli przyzwyczajeni do zmagania się z tak trudnymi zadaniami. Większość czasu przeznaczali na świadczenie rutynowej pomocy technicznej klientom, a nie na analizowanie niebezpiecznych zagrożeń. Robili jednak postępy i ostatecznie ustalili, że jeden z modułów, sterownik, jest w rzeczywistości rootkitem z poziomu jądra — tak jak Ulasen podejrzewał[5].

Istnieją różne rodzaje rootkitów. Najtrudniejsze do wykrycia są rootkity z poziomu jądra. Kryją się one głęboko w jądrze maszyny, gdzie mogą uzyskać takie same uprawnienia, z jakimi działają skanery antywirusowe. Wyobraź sobie strukturę komputera jako koło na tarczy do strzelania z łuku. Jądro znajduje się w samym środku takiej tarczy. Jest to część systemu operacyjnego, dzięki której wszystko może działać. Większość hakerów pisze rootkity działające w zewnętrznych warstwach maszyny — na poziomie użytkownika, gdzie pracują aplikacje — ponieważ jest to łatwiejsze.

---

[4] Moduł to niezależny komponent. Często jedne moduły można zastępować innymi i stosować w różnych programach.

[5] Sterowniki to oprogramowanie używane jako interfejs między urządzeniem a komputerem. Dzięki sterownikom urządzenie może współpracować z komputerami. Sterownik jest potrzebny np. po to, aby umożliwić komputerowi komunikowanie się z podłączonymi do niego drukarkami lub aparatami cyfrowymi. Dostępne są różne sterowniki dla różnych systemów operacyjnych, dlatego to samo urządzenie może współpracować z dowolnym komputerem. W omawianej historii sterowniki były rootkitami zaprojektowanymi w celu instalowania i ukrywania w maszynach szkodliwych plików.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak skanery wirusów potrafią wykryć takie narzędzia. Dlatego hakerzy o naprawdę wysokich umiejętnościach umieszczają rootkity na poziomie jądra maszyny, gdzie mogą się one ukryć przed skanerem. Z tego poziomu rootkit pełni funkcję pomocnika szkodliwych plików, zakłócając pracę skanera, tak aby złośliwe oprogramowanie mogło niewykryte bez przeszkód wykonywać swoją brudną robotę. Rootkity z poziomu jądra nie są rzadkie, jednak zbudowanie skutecznego narzędzia tego rodzaju wymaga zaawansowanej wiedzy i dużej zręczności. Omawiany tu rootkit był bardzo skuteczny[6].

Kupriejew ustalił, że ten rootkit został zaprojektowany w celu ukrycia czterech szkodliwych plików .LNK — czterech innych podejrzanych plików znalezionych w systemie w Iranie. Zastosowane złośliwe oprogramowanie było eksploitem składającym się z tych plików i rozpowszechnianym za pomocą zainfekowanych pendrive'ów, a rootkit uniemożliwiał dostrzeżenie plików .LNK na pendrive'ach. To po tym odkryciu Kupriejew zawołał Ulasena.

Eksploity rozpowszechniające złośliwe oprogramowanie za pośrednictwem pendrive'ów nie są tak popularne jak te rozsyłające wirusy w internecie (w witrynach i załącznikach e-maili), ale nie są też niczym wyjątkowym. Jednak wszystkie tego typu eksploity, które dwaj wspomniani informatycy napotkali do tego czasu, korzystały z mechanizmu automatycznego uruchamiania w systemie operacyjnym Windows, który to mechanizm umożliwiał złośliwym

[6] Restartowanie nie występowało na innych maszynach zainfekowanych omawianym złośliwym oprogramowaniem. Dlatego część badaczy podejrzewała, że problem może wynikać z niezgodności między jednym ze sterowników ze złośliwego oprogramowania a oprogramowaniem antywirusowym firmy VirusBlokAda. Złośliwe oprogramowanie używało sterownika na etapie instalacji, a badacze z rosyjskiej firmy Kaspersky Lab podejrzewali, że gdy sterownik wstrzykiwał główny plik oprogramowania do pamięci maszyn w Iranie, mogło to skutkować awarią niektórych z nich. Badacze z tej firmy próbowali później odtworzyć ten problem, ale uzyskali różne efekty. Czasem komputer ulegał awarii, a czasem nie. Paradoksalne jest to, że napastnicy włożyli dużo pracy w przetestowanie swojego złośliwego oprogramowania pod kątem skanerów antywirusowych z firm Kaspersky, Symantec, McAfee i innych. Robili to, aby się upewnić, że kod nie zostanie wykryty przez te skanery i nie spowoduje awarii komputerów. Najwyraźniej jednak nie przeprowadzili testów z użyciem skanera firmy VirusBlokAda. Dlatego jeśli skaner tej firmy *rzeczywiście* stanowił źródło problemu, oznaczało to, że ten niewielki białoruski producent oprogramowania był nie tylko źródłem klęski napastników z powodu ujawnienia ataku, ale też przyczynił się do powstania awarii, która zwróciła na niego uwagę.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

programom z pendrive'a rozpoczęcie pracy zaraz po podłączeniu urządzenia do komputera. Jednak ten eksploit działał w sprytniejszy sposób[7].

Pliki .LNK w systemie Windows odpowiadają za wyświetlanie ikon prezentujących zawartość pendrive'a lub innych przenośnych urządzeń podłączanych do komputera. Gdy umieścisz pendrive'a w komputerze, eksplorator plików lub podobne narzędzie automatycznie wyszuka pliki .LNK, aby wyświetlić ikony powiązane z plikami muzycznymi, dokumentami Worda lub programami z pendrive'a[8]. Jednak w omawianej sytuacji napastnicy umieścili w specjalnie zmodyfikowanym pliku .LNK eksploit. Gdy eksplorator plików skanował plik, uruchamiał eksploit, który niezauważalnie przenosił na komputer szkodliwą zawartość pendrive'a, podobnie jak wojskowy samolot transportowy zrzuca spadochroniarzy w kamuflażu nad obszarem wroga.

Eksploit z plików .LNK atakował tak podstawowy mechanizm systemu Windows, że Ulasen zastanawiał się, dlaczego nikt wcześniej na to nie wpadł. Ten atak był znacznie groźniejszy niż eksploity związane z mechanizmem automatycznego uruchamiania, z którymi można łatwo sobie poradzić, wyłączając ten mechanizm w komputerze. Jest to krok, na który decyduje się wielu administratorów sieci, ponieważ mechanizm automatycznego uruchamiania jest znanym zagrożeniem dla bezpieczeństwa. Nie da się jednak w prosty sposób wyłączyć obsługi plików .LNK, nie przysparzając użytkownikom problemów.

Ulasen przeszukał rejestr innych eksploitów wykorzystujących pliki .LNK, jednak nie znalazł niczego podobnego. Wtedy zaczął podejrzewać, że natrafił na eksploit typu zero-day.

Wziął pendrive'a zainfekowanego szkodliwymi plikami i podłączył go do testowej maszyny z Windowsem 7 — najmłodszą wówczas wersją systemu operacyjnego Microsoftu. Na tym komputerze zainstalowane były wszystkie najnowsze poprawki bezpieczeństwa. Gdyby ten eksploit był znany

[7] Mechanizm automatycznego uruchamiania to wygodna funkcja systemu Windows, umożliwiająca programom z pendrive'ów oraz płyt CD-ROM i DVD automatyczne uruchomienie po włożeniu danego nośnika do komputera. Funkcja ta stanowi jednak znane zagrożenie bezpieczeństwa, ponieważ w ten sposób uruchomiony może zostać także dowolny szkodliwy program z nośnika.

[8] Jeśli z przyczyn bezpieczeństwa mechanizm automatycznego uruchamiania jest wyłączony, szkodliwy kod z pendrive'a wykorzystujący tę funkcję nie będzie mógł automatycznie rozpocząć pracy. Uruchomienie go będzie wymagało kliknięcia pliku przez użytkownika.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Microsoftowi, łatki z systemu uniemożliwiłyby przeniesienie szkodliwych plików na komputer. Jednak gdyby używany był eksploit typu zero-day, nic by go nie powstrzymało. Ulasen odczekał kilka minut przed sprawdzeniem komputera i, jak pewnie się domyślasz, znalazł na nim szkodliwe pliki.

Nie mógł w to uwierzyć. VirusBlokAda, maleńka firma z dziedziny zabezpieczeń, o której słyszała garstka ludzi na świecie, właśnie odkryła najcenniejsze dla łowców wirusów trofeum. Nie tylko był to eksploit typu zero-day, ale działał we wszystkich wersjach systemu Windows od edycji 2000. Napastnicy zastosowali pakiet czterech wersji eksploita w czterech różnych plikach .LNK, aby mieć pewność, że atak powiedzie się we wszystkich wersjach systemu Windows, w których eksploit może się znaleźć[9].

Ulasen próbował na tej podstawie oszacować liczbę komputerów zagrożonych infekcją. Wtedy jednak wpadł na coś równie niepokojącego jak eksploit typu zero-day. Szkodliwy moduł sterownika i inny moduł przenoszony na docelowe maszyny w ramach złośliwego ładunku instalowały się niezauważalnie na testowej maszynie, a na ekranie nie pojawiało się żadne ostrzeżenie dotyczące tej operacji. System Windows 7 obejmuje mechanizm zabezpieczeń, który powinien informować użytkowników o próbie instalacji niepodpisanego sterownika lub sterownika podpisanego za pomocą niezaufanego certyfikatu. Jednak oba złośliwe sterowniki zostały zainstalowane bez problemów. Stało się tak, co Ulasen zauważył ze zgrozą, ponieważ były podpisane za pomocą najwyraźniej prawidłowego certyfikatu cyfrowego należącego do firmy RealTek Semiconductor[10].

Certyfikaty cyfrowe to zaufane dokumenty z obszaru zabezpieczeń działające jak cyfrowe paszporty. Producenci oprogramowania używają ich do podpisywania programów, aby potwierdzić, że to oprogramowanie jest legalnym produktem danej firmy. Na przykład Microsoft lub firmy rozwijające

[9] Eksploit działał w siedmiu wersjach systemu Windows: Windows 2000, WinXP, Windows 2003, Vista, Windows Server 2008, Windows 7 i Windows Server 2008 R2.

[10] W systemach Windows Vista i Windows 7 sterownik, który nie jest podpisany zaufanym certyfikatem cyfrowym rozpoznawanym przez Microsoft, będzie miał trudności z zainstalowaniem się na komputerze. W maszynach z 32-bitowymi wersjami tych systemów pojawi się ostrzeżenie z informacją, że plik jest niepodpisany lub że nie jest podpisany za pomocą zaufanego certyfikatu. Użytkownik musi wtedy podjąć decyzję, czy pozwolić na instalację takiego oprogramowania. W 64-bitowych wersjach wymienionych systemów plik niepodpisany zaufanym certyfikatem w ogóle się nie zainstaluje. Złośliwe oprogramowanie wykryte przez firmę VirusBlokAda działało tylko na komputerach z 32-bitowymi wersjami systemu Windows.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

antywirusy podpisują cyfrowo swoje programy i aktualizacje. Komputery przyjmują, że plik podpisany za pomocą poprawnego certyfikatu cyfrowego jest godny zaufania. Jeśli jednak napastnik ukradnie certyfikat Microsoftu i prywatny klucz kryptograficzny używany w Microsofcie razem z certyfikatem do podpisywania plików, będzie mógł zmylić komputer, tak aby szkodliwy kod został uznany za kod od Microsoftu.

Napastnicy stosowali już w przeszłości certyfikaty cyfrowe do podpisywania szkodliwych plików. Posługiwali się jednak fałszywymi, samodzielnie podpisanymi certyfikatami naśladującymi certyfikaty prawidłowe. Czasem za pomocą oszustw zdobywali rzeczywiste certyfikaty, np. zakładając firmę wydmuszkę w celu nakłonienia jednostki certyfikacyjnej do wydania certyfikatu na nazwę tej firmy[11]. W obu tych scenariuszach napastnicy narażali się na to, że komputer uzna certyfikat za podejrzany i odrzuci plik. W omawianym przypadku wykorzystali poprawny certyfikat firmy RealTek, wiarygodnego tajwańskiego producenta sprzętu, do przekonania komputerów, że sterowniki to legalne oprogramowanie od RealTeka.

Ulasen nigdy wcześniej nie zetknął się z taką strategią i zastanawiał się, w jaki sposób napastnikom udało się ją zrealizować. Jedną z możliwości była kradzież komputera programisty z RealTeka i wykorzystanie tej maszyny wraz z danymi uwierzytelniającymi do podpisania kodu[12].

---

[11] Jednostki certyfikacyjne wydają certyfikaty używane przez firmy do podpisywania kodu i witryn. Takie jednostki powinny sprawdzać, czy organizacja występująca o certyfikat ma do niego prawo (zapobiega to sytuacji, w której firma inna niż Microsoft uzyska certyfikat z nazwą tej korporacji), a także upewniać się, że dana firma rzeczywiście zajmuje się tworzeniem kodu. Jednak niektóre jednostki certyfikacyjne nie przeprowadzają odpowiednich badań, dlatego certyfikaty są czasem wydawane niebezpiecznym podmiotom. Ponadto niektóre firmy za opłatą używają własnych kluczy i certyfikatów do podpisywania cudzego kodu. W przeszłości hakerzy wykorzystywali takie firmy do podpisywania swojego złośliwego oprogramowania.

[12] We wrześniu 2012 r. przytrafiło się to firmie Adobe. Ten gigant z branży oprogramowania, udostępniający popularne programy Adobe Reader i Flash Player, poinformował wówczas, że napastnicy włamali się na serwer służący do podpisywania kodu i podpisali dwa szkodliwe pliki certyfikatami firmy Adobe. Firma przechowywała używane do podpisywania kodu prywatne klucze w tzw. sprzętowym module bezpieczeństwa, który powinien zapobiec dostępowi napastników do kluczy. Hakerzy włamali się jednak na serwer używany do rozwijania oprogramowania, który mógł komunikować się z systemem podpisywania kodu, i w ten sposób podpisali swoje pliki.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Możliwe było też to, że napastnicy wykradli klucz używany do podpisywania i certyfikat. Z przyczyn bezpieczeństwa przezorne firmy przechowują certyfikaty i klucze na serwerach bez dostępu do sieci lub w zabezpieczonych modułach sprzętowych zapewniających dodatkową ochronę. Jednak nie wszyscy tak postępują. Z pewnych poszlak wynika, że certyfikat firmy RealTek rzeczywiście został skradziony. Znacznik czasu z certyfikatów wskazuje na to, że oba sterowniki zostały podpisane 25 stycznia 2010 r. Choć jeden ze sterowników został skompilowany rok wcześniej, 1 stycznia 2009 r., kompilacja drugiego nastąpiła tylko 6 min przed jego podpisaniem. Tak błyskawiczne podpisanie sterownika wskazuje na to, że napastnicy mogli mieć dostęp do klucza i certyfikatu firmy RealTek.

Wynikały z tego niepokojące wnioski. Zastosowanie poprawnych certyfikatów cyfrowych do uwierzytelnienia szkodliwych plików podważyło wiarygodność architektury podpisów w świecie komputerów. Legalność plików podpisanych za pomocą certyfikatów cyfrowych stała się tym samym wątpliwa. Skopiowanie tej strategii przez innych napastników i rozpoczęcie wykradania certyfikatów było tylko kwestią czasu[13]. Ulasen musiał poinformować o tym innych.

Odpowiedzialne ujawnienie tych informacji wymagało, aby badacze, którzy odkryli luki, poinformowali najpierw producentów oprogramowania, a dopiero potem upublicznili dane. Daje to producentom czas na załatanie luk. Dlatego Ulasen wysłał e-maile do firm RealTek i Microsoft, powiadamiając o odkryciach zespołu.

[13] Na ironię zakrawa fakt, że 12 lipca 2010 r., czyli w dniu, gdy Ulasen upublicznił informacje o wykrytym złośliwym oprogramowaniu, badacz z F-Secure, fińskiej firmy z branży zabezpieczeń, opublikował prezentację o certyfikatach cyfrowych, w której stwierdził, że jak dotąd nie wykryto złośliwego oprogramowania wykorzystującego skradzione certyfikaty. Zauważył jednak, że z pewnością się to zmieni, ponieważ nowe wersje systemu Windows z podejrzliwością traktują niepodpisane sterowniki. Zmusza to hakerów do kradzieży legalnych certyfikatów na potrzeby podpisywania złośliwego oprogramowania (zob. prezentację Jarna Niemelego, „It's Signed, Therefore It's Clean, Right?", z konferencji CARO w Helsinkach w Finlandii: *https://f-secure.com/weblog/archives/Jarno_Niemela_its_signed.pdf*). Rzeczywiście, niedługo po wykryciu w firmie VirusBlokAda certyfikatu RealTeka inni hakerzy zaczęli próbować stosować tę samą technikę. We wrześniu 2010 r. firmy antywirusowe odkryły konia trojańskiego Infostealer.Nimkey, zaprojektowanego specjalnie w celu wykradania z komputerów certyfikatów opartych na kluczu prywatnym. W ciągu następnych dwóch lat pojawiło się wiele szkodliwych programów podpisanych za pomocą certyfikatów skradzionych z różnych zaufanych firm.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak po upływie dwóch tygodni bez odpowiedzi od żadnej z tych firm Ulasen i Kupriejew zdecydowali, że nie mogą dłużej milczeć[14]. Społeczność zajmująca się zabezpieczeniami musiała się dowiedzieć o wykrytym eksploicie plików .LNK. Informatycy dodali już sygnatury eksploita do programu antywirusowego firmy VirusBlokAda, aby wykrywać szkodliwe pliki. Okazało się, że zainfekowane maszyny znajdują się na całym Bliskim Wschodzie, a także w innych obszarach. Robak (wirus) był na wolności i szybko się rozprzestrzeniał. Informatycy musieli upublicznić tę wiadomość[15].

Dlatego 12 lipca Ulasen zamieścił w firmowej witrynie i na anglojęzycznym forum poświęconym zabezpieczeniom krótką informację na temat eksploita typu zero-day. Ostrzegał przed wybuchem epidemii infekcji[16]. Ujawnił jednak niewiele szczegółów na temat luki, aby uniknąć dostarczania innym hakerom danych, które mogłyby pomóc w jej wykorzystaniu. Członkowie forum szybko zrozumieli możliwe konsekwencje, zauważając, że ataki mogą okazać się „zabójcze dla wielu jednostek".

Trzy dni później Brian Krebs, dziennikarz zajmujący się zabezpieczeniami komputerowymi, natrafił na wiadomość i zamieścił na blogu poświęcony jej artykuł. Podsumował w nim dostępne wówczas ubogie informacje na temat luki i eksploita[17]. Wiadomość rozniosła się po społeczności zajmującej się zabezpieczeniami i sprawiła, że wszyscy mogli się przygotować na falę ataków ze strony opisanego robaka i naśladowców używających

[14] Ulasen skontaktował się z Microsoftem za pośrednictwem ogólnego adresu e-mail stosowanego przez zespół ds. bezpieczeństwa w tej korporacji. Zespół ten otrzymuje ponad 100 tys. e-maili rocznie, dlatego było zrozumiałe, że e-mail przesłany na ogólny adres przez nieznaną białoruską firmę antywirusową utknął w kolejce wiadomości.

[15] Badacze odkryli później, że to złośliwe oprogramowanie było kombinacją robaka i wirusa. Robak umożliwiał autonomiczne rozpowszechnianie kodu bez udziału użytkownika. Gdy kod znajdował się już w systemie, inne komponenty infekowały pliki (jak robi to wirus), a dalsze ich rozprzestrzenianie wymagało aktywności użytkowników.

[16] Ulasen opublikował informacje w firmowej witrynie (*http://www.anti-virus.by/en/tempo.shtml*) i na forum Wilders Security (*http://wilderssecurity.com/showthread.php?p=1712146*).

[17] Krebs, były reporter gazety „Washington Post", prowadzi blog *http://krebsonsecurity.com/* poświęcony zabezpieczeniom komputerów i cyberprzestępczości. Wspomniany artykuł opublikował 15 lipca 2010 r. pod adresem: *http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

podobnych eksploitów[18]. Równocześnie szef niemieckiego instytutu badającego i testującego programy antywirusowe skontaktował znane mu osoby z Microsoftu z Ulasenem i ponaglił Microsoft, aby rozpoczął prace nad łatką[19]. Po ujawnieniu luki Microsoft zdecydował się natychmiast opublikować dotyczącą tego krytycznego problemu wskazówkę dla użytkowników. Przedstawił też zestaw rad pozwalających zmniejszyć ryzyko infekcji. Jednak z powodu braku łatki, która miała pojawić się dopiero za dwa tygodnie, trudno było uznać to za rozwiązanie problemu[20].

Także w branży zabezpieczeń komputerowych zabrano się do pracy, aby poradzić sobie z robakiem, który teraz miał już nazwę — Stuxnet. Było to określenie utworzone w Microsofcie z liter nazwy jednego z plików sterownika (*mrxnet.sys*) i innego fragmentu kodu. Gdy firmy z branży zabezpieczeń zaczęły dodawać do swoich produktów sygnatury wykrywające robaka i eksploit, na maszynach zainfekowanych klientów zostały ujawnione tysiące szkodliwych plików[21].

Prawie natychmiast pojawiła się następna niespodzianka. Siedemnastego lipca firma antywirusowa ze Słowacji, ESET, wykryła kolejny szkodliwy sterownik, który wydawał się powiązany ze Stuxnetem. Sterownik ten też był podpisany za pomocą certyfikatu cyfrowego tajwańskiej firmy, przy czym innej niż RealTek. Była to firma JMicron Technology — producent układów scalonych.

---

[18] Lenny Zeltser, „Preempting a Major Issue Due to the .LNK Vulnerability — Raising Infocon to Yellow". Tekst został opublikowany 19 lipca 2010 r. na stronie: *http://isc.sans.edu/diary.html?storyid=9190*.

[19] Andreas Marx, szef niemieckiej firmy AV-TEST.org, skorzystał ze swoich bezpośrednich kontaktów w Microsofcie.

[20] Wskazówki Microsoftu zostały opublikowane na stronie: *https://technet.microsoft.com/library/security/2286198*.

[21] Większość firm antywirusowych korzysta z automatycznych systemów zgłoszeń, które powiadamiają o wykryciu szkodliwych plików na maszynach klientów (jeśli dany użytkownik zaakceptował taką opcję). W większości przypadków do firmy przesyłany jest tylko skrót pliku — kryptograficzna reprezentacja zawartości pliku obejmująca łańcuch liter i cyfr, wygenerowana w wyniku przetworzenia pliku przez algorytm. Dane o ofierze obejmują tylko adres IP nadawcy. Jednak w niektórych sytuacjach firmy mogą otrzymać cały szkodliwy plik, jeśli ofiara zdecyduje się go przesłać. Firma antywirusowa może też na podstawie adresu IP ustalić tożsamość ofiary i poprosić o kopię szkodliwego pliku.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ten sterownik został odkryty na komputerze sam, bez innych plików Stuxneta, ale wszyscy uznali, że musi być powiązany z robakiem, ponieważ był podobny do innych sterowników znalezionych w firmie VirusBlokAda[22]. Zauważono też ciekawą rzecz dotyczącą daty kompilacji sterownika. Gdy hakerzy przekazali kod źródłowy do kompilatora, aby uzyskać czytelny dla komputerów kod binarny, kompilator umieszczał w pliku binarnym znacznik czasu. Choć napastnicy zmienili znacznik czasu, by utrudnić pracę badaczom, tym razem czas wydawał się prawidłowy. Wynikało z niego, że sterownik został skompilowany 14 lipca, dwa dni *po* tym jak firma VirusBlokAda upubliczniła informacje o Stuxnecie. Czy twórcy Stuxneta wykorzystali sterownik do nowego ataku, zupełnie nieświadomi tego, że mało znana firma antywirusowa z Białorusi właśnie ich zdemaskowała? A może wiedzieli, że ich tajna misja wkrótce zostanie ujawniona, i próbowali pospiesznie umieścić Stuxneta na większej liczbie komputerów, zanim zostanie on zablokowany? Pojawiły się poszlaki, zgodnie z którymi napastnicy pominęli pewne kroki w trakcie podpisywania sterownika z użyciem certyfikatu firmy JMicron. Oznaczałoby to, że rzeczywiście mogli się spieszyć, aby umieścić szkodliwy kod na docelowych komputerach[23]. Jedna rzecz była pewna: napastnicy potrzebowali nowego certyfikatu do podpisania sterownika, ponieważ certyfikat firmy RealTek wygasł miesiąc wcześniej, 12 czerwca. Certyfikaty cyfrowe mają ograniczony czas ważności, dlatego po wygaśnięciu certyfikatu RealTeka napastnicy nie mogli dłużej stosować go do podpisywania nowych plików. Ponadto po ujawnieniu Stuxneta certyfikat został cofnięty przez jednostkę certyfikacyjną, dlatego komputery

[22] Badacze spekulowali, że ten sterownik mógł zostać użyty w nowej wersji Stuxneta, którą jego twórcy wypuścili po dopracowaniu kodu w taki sposób, aby zapobiec wykrywaniu ataku na podstawie sygnatur. Nie wykryto żadnych późniejszych wersji Stuxneta (por. przypis 41. w rozdziale 17.).

[23] Zob. Costin G. Raiu, Alex Gostev, *A Tale of Stolen Certificates*. Tekst ten został opublikowany w drugim kwartale 2011 r. w „SecureView", kwartalnym newsletterze firmy Kaspersky Lab. Błędy pojawiły się w bloku z sygnaturą cyfrową certyfikatu, gdzie firmy podają informacje na swój temat. Napastnicy podali błędny adres URL firmy JMicron, dlatego po próbie otwarcia witryny pojawiał się błąd „serwera nie znaleziono". Napastnicy nie wypełnili też kilku pól z nazwą firmy, prawami autorskimi i innymi danymi. W ośmiu z tych pól zamiast informacji znajdowały się słowa *change me*, czyli „zmodyfikuj mnie".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

z systemem Windows zaczęły odrzucać lub odpowiednio oznaczać podpisane przy jego użyciu pliki[24].

Odkrycie drugiego certyfikatu doprowadziło do dalszych spekulacji na temat tego, jak hakerzy zdobyli te dokumenty. Siedziby główne firm RealTek i JMicron są oddalone od siebie tylko o dwie przecznice i znajdują się w tajwańskiej miejscowości Xinzhu w parku przemysłowym Xinzhu Science and Industrial Park. Ze względu na geograficzną bliskość tych firm część osób spekulowała, że napastnicy mogli fizycznie włamać się do obu biur i wykraść klucze i certyfikaty. Zdaniem innych to Chiny stały za atakami z użyciem Stuxneta i to hakerzy z tego kraju złamali zabezpieczenia obu tajwańskich firm, aby zdobyć klucze i certyfikaty cyfrowe.

Niezależnie od scenariusza napastnicy prawdopodobnie mieli też inne wykradzione certyfikaty. A skoro włożyli tyle wysiłku w upewnienie się, że ich atak będzie skuteczny, prawdopodobnie mieli poważne cele i dysponowali znacznymi środkami. Wiele osób w społeczności zajmującej się zabezpieczeniami było niespokojnych i zdumionych. „Rzadko widzimy tak profesjonalnie przeprowadzone operacje" — napisał w internecie badacz Pierre-Marc Bureau z firmy ESET[25].

Gdy firmy antywirusowe przeanalizowały napływające od klientów pliki Stuxneta, natrafiły na jeszcze jedną niespodziankę. Na podstawie dat z niektórych plików wydawało się, że Stuxnet został zastosowany już w czerwcu 2009 r. Oznaczało to, że czaił się w komputerach przynajmniej przez rok przed wykryciem go przez firmę VirusBlokAda. Wydawało się też, że napastnicy przeprowadzili atak w trzech falach: w czerwcu 2009 r. oraz w marcu i kwietniu 2010 r. Za każdym razem wprowadzali drobne zmiany w kodzie.

Jednak pewna kwestia wciąż pozostawała zagadką: jakie było przeznaczenie Stuxneta? Badacze w żadnym z plików nie znaleźli oznak tego, że Stuxnet wykradał hasła do kont bankowych lub inne dane osobowe. Różnił się pod tym względem od dużej części szkodliwego oprogramowania.

---

[24] Certyfikat RealTeka był ważny od 15 marca 2007 r. do 12 czerwca 2010 r. Certyfikat firmy JMicron był aktywny do 26 lipca 2012 r., jednak po jego wycofaniu przez jednostki certyfikacyjne napastnicy nie mogli się już nim posługiwać.

[25] Pierre-Marc Bureau, „Win32/Stuxnet Signed Binaries". Tekst został opublikowany 9 sierpnia 2010 r. na stronie: *https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Badacze długo nie znajdowali w kodzie także żadnych innych oczywistych wskazówek co do motywów napastników. Dopiero pewien niemiecki analityk trafił na poszlakę, która mogła sugerować przeznaczenie Stuxneta.

„Cześć wszystkim — napisał Frank Boldewin na forum, na którym Ulasen po raz pierwszy zamieścił informacje o Stuxnecie. — Czy ktoś […] dokładniej przyjrzał się temu wirusowi?". Boldewin odpakował pierwszą warstwę z jednego z plików Stuxneta i znalazł nieoczekiwane referencje do oprogramowania rozwijanego przez niemiecką firmę Siemens. Napastnicy najwyraźniej szukali komputerów z zainstalowanymi zastrzeżonymi programami Siemensa (SIMATIC Step 7 lub SIMATIC WinCC). Oba te programy to część przemysłowego systemu sterowania zaprojektowanego do współpracy ze sterownikami PLC Siemensa — małymi komputerami, zwykle wielkości tostera, używanymi w fabrykach na całym świecie do kontrolowania takich mechanizmów jak ramiona robotów i taśmociągi na liniach montażowych.

Boldewin nigdy wcześniej nie zetknął się ze szkodliwym oprogramowaniem atakującym przemysłowe systemy sterowania. Hakowanie wyposażenia fabryki takiego jak sterowniki PLC nie prowadziło do oczywistych korzyści finansowych — a przynajmniej nie tego rodzaju, jak szybkie pieniądze, jakie można zyskać dzięki włamaniom na konta bankowe lub do systemów kart kredytowych. Zdaniem Boldewina mogło to oznaczać tylko jedno. „Wygląda na to, że ten wirus został opracowany na potrzeby szpiegostwa" — napisał[26]. Napastnicy najprawdopodobniej chcieli wykraść plany fabryki konkurencji lub projekty produktów.

Wiele osób ze społeczności informatyków zbyt szybko zaakceptowało taką ocenę sytuacji. Stuxnet najwyraźniej atakował tylko systemy z zainstalowanym oprogramowaniem Siemensa, co oznaczało, że pozostałe maszyny były bezpieczne, a ich właściciele mogli spać spokojnie. Ulasen stwierdził, że w irańskich systemach, które wpadły w pętlę restartowania, takie oprogramowanie nie było zainstalowane. Wyglądało na to, że Stuxnet nie wyrządził na tych komputerach żadnych trwałych szkód (oprócz powtarzających się awarii systemu).

[26] Boldewin opublikował swoje informacje na stronie: *http://wilderssecurity.com/showthread.php?p=1712146*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dlatego mniej więcej tydzień po krótkiej chwili sławy tajemniczego robaka Stuxnet znalazł się na dobrej drodze do zapomnienia. Microsoft wciąż pracował nad łatką, która miała wyeliminować lukę w zabezpieczeniach wykorzystaną przez eksploit z plikami .LNK, jednak większość firm zajmujących się zabezpieczeniami tylko dodała do skanerów sygnatury wykrywające szkodliwe pliki robaka i przestała interesować się Stuxnetem.

Historia pierwszej cyfrowej broni na świecie mogłaby się na tym zakończyć. Jednak kilku badaczy nie chciało jeszcze się z tym pogodzić.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 2

500 KB TAJEMNICY

Liam O'Murchu analizował wirusy i robaki od sześciu lat. Nigdy wcześniej nie natrafił na kod, jaki właśnie badał. W tym kodzie wykorzystano techniki znacznie wykraczające poza wszystko, z czym zetknął się w innym szkodliwym oprogramowaniu. Zupełnie czegoś innego się spodziewał, gdy usiadł przy swoim komputerze w biurze firmy Symantec w południowej Kalifornii i przyjrzał się plikom Stuxneta, które w nocy przesłali mu jego współpracownicy z Europy.

Było to w piątek 16 lipca, dzień po tym jak informacje o Stuxnecie pojawiły się w społeczności informatyków. O'Murchu zajmował się czymś, co — jak sądził — będzie rutynowym i pobieżnym przeglądem kodu. Ten 33-letni Irlandczyk był menedżerem ds. operacji w wydziale reagowania na zagrożenia w biurze Symanteca w Culver City. Jego zadaniem był przegląd nowego złośliwego oprogramowania, aby ustalić, czy zasługuje ono na dokładniejsze zbadanie.

Analitycy z biura firmy w Dublinie otrzymali pliki Stuxneta późnym popołudniem i mieli tylko kilka godzin na zapoznanie się z kodem przed przekazaniem go do zespołu O'Murchu w Kalifornii, gdzie dzień dopiero się zaczynał. Zespół analizy zagrożeń w firmie Symantec pracuje na kilku kontynentach. Dzięki temu zawsze, gdy pojawi się coś ważnego, ktoś może się tym zająć. Gdy słońce zachodzi nad jednym biurem i wschodzi nad innym, pracownicy z jednej strefy czasowej przekazują — jak w sztafecie — swoje uwagi analitykom z innej strefy.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nie całe złośliwe oprogramowanie jest analizowane w modelu „podążania za słońcem". Spośród miliona szkodliwych plików, jakie Symantec i podobne firmy znajdują każdego miesiąca, większość jest wzorowana na znanych narzędziach, które hakerzy modyfikują w celu zmiany „odcisków palców" i przechytrzenia skanerów antywirusowych. Te standardowe zagrożenia są przetwarzane za pomocą algorytmów, które szukają w kodzie sygnatur lub operacji pasujących do znanego złośliwego oprogramowania. Kod jest przekazywany badaczom do ręcznej analizy tylko wtedy, gdy algorytmy natrafią na coś, czego nie potrafią rozpoznać. Złośliwe oprogramowanie zawierające (lub potencjalnie obejmujące) eksploit typu zero-day zawsze jest badane ręcznie. Był to jedyny powód, dla którego Stuxnet trafił na biurko O'Murchu.

O'Murchu jest zapalonym snowboardzistą z lirycznym akcentem i krótkimi brązowymi włosami, postawionymi z przodu pionowo, przez co przypominają niewielki half-pipe. Irlandczyk niedawno przeniósł się do Stanów Zjednoczonych z Dublina i w momencie wykrycia Stuxneta pracował w kalifornijskim biurze Symanteca od ok. dwóch lat, jednak z tą firmą związany był od 2004 r. Kierował zespołem doświadczonych analityków złośliwego oprogramowania i specjalistów od inżynierii odwrotnej, zaangażowanych w nieustającą walkę z natłokiem cyfrowych zagrożeń, z których każde kolejne jest bardziej zaawansowane od poprzedniego. To jednak nie przygotowało go na coś, co znalazł w Stuxnecie.

O'Murchu spodziewał się, że przeprowadzi tylko rutynową analizę kodu, aby potwierdzić obecność eksploita typu zero-day wykrytego już przez Ulasena i Kupriejewa. Dlatego przekazał kod młodszemu inżynierowi, uznając, że będzie to dobra okazja do nauczenia go czegoś o eksploitach tego typu. Sam zbadał kod jedynie w celu sprawdzenia współpracownika i upewnienia się, że ten ostatni niczego nie pominął. Jednak gdy tylko otworzył pliki, natychmiast zrozumiał, że w kodzie dzieje się coś dziwnego.

Główny plik Stuxneta był bardzo duży. Zajmował 500 kB, podczas gdy podobne pliki zwykle zajmują od 10 do 15 kB. Nawet Conficker, groźny robak, który w ciągu dwóch poprzednich lat zainfekował ponad 6 mln maszyn, zajmował tylko 35 kB. Większe złośliwe oprogramowanie zwykle obejmowało tylko zajmujące miejsce dane graficzne, np. fałszywą stronę internetową banku, która pojawiała się w przeglądarce zainfekowanej maszyny, aby nakłonić ofiary do podania danych uwierzytelniających. Jednak

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

w Stuxnecie nie występowały dane graficzne ani inny nadmiarowy kod. A gdy O'Murchu zaczął rozkładać pliki na części, zdał sobie sprawę, że kod jest znacznie bardziej złożony, niż on i inni analitycy do tej pory sądzili.

Gdy ktoś widział tak dużo złośliwego oprogramowania jak O'Murchu, potrafi spojrzeć na kod wirusa lub konia trojańskiego i natychmiast stwierdzić, jakie jest jego przeznaczenie. Ten rejestruje wciśnięte klawisze, aby zapisać wszystko, co wpisuje ofiara, tamten to koń trojański wykradający dane uwierzytelniające do internetowych kont bankowych. Łatwo można też stwierdzić, czy dany fragment kodu został napisany niechlujnie, czy też opracowany umiejętnie i ze starannością. Stuxnet w oczywisty sposób zaliczał się do drugiej z tych kategorii. Wyglądał na spójny i dobrze zorganizowany zbiór danych i poleceń o bardzo bogatych funkcjach. Czym były te funkcje, pozostawało na razie tajemnicą, jednak O'Murchu natychmiast zainteresował się tym kodem.

O'MURCHU PO RAZ pierwszy zetknął się ze złośliwym oprogramowaniem w 1996 r., gdy studiował nauki komputerowe na University College Dublin. Jeden ze studentów wypuścił własnoręcznie napisanego wirusa, który zainfekował wszystkie maszyny w pracowniach komputerowych uczelni. W idy marcowe wirus przejął kontrolę nad terminalami, utrudniając dostęp do maszyn. Użytkownicy mogli się zalogować tylko po udzieleniu odpowiedzi na serię dziesięciu pytań pojawiających się na ekranach. Większość osób była zirytowana tą przeszkodą, jednak O'Murchu chciał tylko zdobyć kopię wirusa, aby rozebrać go na części. Rozkładanie leżało w jego naturze. Irlandczyk dorastał na wsi w okolicach miasteczka Athy w hrabstwie Kildare i już jako dziecko mniej interesował się zabawą samochodzikami niż rozbieraniem ich na części w celu sprawdzenia, jak działają.

O'Murchu początkowo nie zamierzał zostać pogromcą wirusów. Rozpoczął studia, sumiennie uczestnicząc w kursach z zakresu fizyki i chemii, aby uzyskać planowany dyplom z dziedziny nauk ścisłych. Jednak później zapisał się na kurs nauk komputerowych, które stały się jego pasją. Szybko porzucił laboratorium chemiczne na rzecz pracowni komputerowej. Hakerzy stanowili coraz poważniejszy problem na uczelni, jednak O'Murchu początkowo nie myślał o karierze w branży zabezpieczeń komputerowych. Zmieniło się to dopiero wtedy, gdy intruzi zaczęli włamywać się na serwery

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

uczelnianego klubu komputerowego i grupa studentów dostała za zadanie zabezpieczyć serwery oraz pozbyć się napastników. O'Murchu zafascynował się późniejszą grą w kotka i myszkę, obserwując, jak intruzom wielokrotnie udawało się przechytrzyć obrońców i ponownie włamać się na serwery.

Ta lekcja łamania cyfrowych granic przydała mu się, gdy po studiach razem z grupą znajomych wyjechali do Stanów Zjednoczonych i na krótko zatrudnili się przy testowaniu kiosków internetowych w zlokalizowanym w San Diego start-upie. Ich zadanie polegało na próbie obejścia systemu opłat w kiosku w celu uzyskania darmowego dostępu do internetu. Właściciele start-upu myśleli, że zatrudniają zwykłych użytkowników komputerów, jednak zamiast tego przypadkowo zrekrutowali zespół uzdolnionych hakerów. Gdy w magazynie, w którym były montowane systemy, stanęło kilka kiosków, O'Murchu i jego znajomi mieli spróbować złamać zabezpieczenia. Testy systemu miały trwać tylko dwa tygodnie, po czym firma planowała przekazać kioski klientom. Jednak O'Murchu ze znajomymi wciąż znajdowali nowe sposoby na obejście systemu opłat. Gdy minęły dwa miesiące, a zespół wciąż wykrywał luki, firma anulowała dalsze testy i wprowadziła kioski do sprzedaży.

Kilka następnych lat O'Murchu spędził, podróżując po świecie i jeżdżąc na snowboardzie. Odczuwał nieskonkretyzowane pragnienie zajęcia się zabezpieczeniami, ale nie miał pomysłu, jak je zrealizować. W 2002 r. otrzymał pracę w antyspamowej firmie Brightmail w Dublinie. Przyjął ją tylko po to, aby zdobyć pieniądze na podróże, ale gdy w 2004 r. przejął tę firmę Symantec, O'Murchu potraktował to jako okazję do wkroczenia w świat zabezpieczeń. W trakcie oprowadzania pracowników firmy Brightmail po dublińskim biurze Symanteca z trudem krył niecierpliwość, gdy pokazywano mu kolejne wydziały. Jedynym, co go interesowało, był zespół ds. analizy wirusów, do którego chciał dołączyć. Jednak gdy w końcu spotkał Erica Chiena, kierującego tym zespołem Amerykanina, jego marzenia o zatrudnieniu zostały rozwiane. O'Murchu myślał, że Symantec zatrudnia setki analityków w różnych częściach świata, dlatego łatwo będzie dostać taką posadę. Lecz Chien poinformował go, że zespół składa się z tylko sześciu osób i że wszystkie z nich zajmują swoje stanowiska od lat. „Nikt nie odchodzi — powiedział Chien. — Wszyscy uwielbiają swoją pracę".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

To jednak nie odstraszyło O'Murchu. Poznał narzędzia używane przez analityków do odszyfrowywania szkodliwego kodu i pisania sygnatur, a gdy po kilku miesiącach gwałtownie wzrosła liczba programów typu spyware oraz adware i Symantec musiał powiększyć wspomniany zespół, Irlandczyk był przygotowany. Przez cztery lata pracował w dublińskim biurze Symanteca, gdzie firma wciąż utrzymuje największą grupę badaczy, po czym w 2008 r. został przeniesiony do Culver City.

O'Murchu i zespół Symanteca przez lata pracowali nad wieloma zaawansowanymi i złożonymi zagrożeniami, ale żadne z nich nie było tak fascynujące i wymagające jak Stuxnet.

GDY O'MURCHU ANALIZOWAŁ główny plik Stuxneta, natychmiast natrafił na kilka poziomów szyfrowania maskujących wiele fragmentów i wewnętrzny rdzeń kodu. Na szczęście pierwszą warstwą był zwykły paker, który łatwo złamać.

Pakery to cyfrowe narzędzia, które kompresują i przekształcają kod, co programom antywirusowym utrudnia wykrycie sygnatur, a analitykom śledczym — szybkie ustalenie działania kodu. Złośliwe oprogramowanie przetworzone przez paker za każdym razem wygląda nieco inaczej. Dlatego ten sam kod zmodyfikowany przez paker tysiąc razy będzie miał tysiąc różnych wersji, choć w następnej warstwie pozostanie taki sam. Programy antywirusowe potrafią wykryć przetworzenie szkodliwego pliku przez znany paker i „w locie" wypakować kod w celu znalezienia sygnatur. Aby to utrudnić, doświadczeni napastnicy projektują niestandardowe pakery, których efekty działania niełatwo jest wykryć lub usunąć. Jednak twórcy Stuxneta tak nie postąpili. Zamiast tego posłużyli się gotowym pakerem UPX (ang. *Ultimate Packer for eXecutables*), który udało się łatwo zidentyfikować, po czym można było odwrócić efekty jego pracy. Z powodu zaawansowanego charakteru całego ataku — eksploita typu zero-day i wykradzionych certyfikatów cyfrowych — taki wybór twórców Stuxneta wydawał się dziwny. Dlatego O'Murchu przyjął, że głównym powodem zastosowania pakera była tylko kompresja plików i zmniejszenie ilości pamięci zajmowanej przez Stuxneta. Po wypakowaniu i dekompresji główny moduł zwiększył objętość do 1,18 MB.

Po usunięciu pakera O'Murchu mógł łatwo dostrzec odkryte przez Franka Boldewina łańcuchy znaków dotyczące Siemensa. Ważniejsze było jednak to, że zobaczył również zaszyfrowany blok kodu, który okazał się

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

główną częścią Stuxneta. Był to duży plik .DLL (ang. *Dynamic-Link Library*) zawierający ponad 30 innych plików .DLL i komponentów. Wszystkie te elementy tworzyły zaszyfrowane warstwy, kryjące się jedna w drugiej jak matrioszki. O'Murchu odkrył też długi plik konfiguracyjny zawierający zestaw ponad 400 ustawień, jakie napastnicy mogli dostosować, aby zmienić dowolne aspekty kodu: od adresu URL serwerów C&C (ang. *command-and-control*), z którymi komunikował się Stuxnet, po liczbę komputerów, jakie Stuxnet miał zainfekować za pomocą pendrive'ów przed zakończeniem pracy eksploita[1]. Co ciekawe, O'Murchu znalazł też datę zakończenia infekcji — 24 czerwca 2012 r. Za każdym razem, gdy Stuxnet napotykał nową maszynę, sprawdzał w jej kalendarzu, czy ta data jeszcze nie nadeszła. Jej przekroczenie sprawiało, że Stuxnet nie infekował danego komputera. Kod wcześniej zainstalowany na innych maszynach nadal miał działać, jednak od tej daty Stuxnet nie miał infekować dodatkowych komputerów. Datę końcową ustalono na trzy lata od momentu zainfekowania pierwszych maszyn w Iranie. Można przyjąć, że do tego czasu napastnicy spodziewali się zrealizować swoje cele[2].

Jednak dla O'Murchu najbardziej zaskakujący był skomplikowany mechanizm ukrywania plików Stuxneta na zainfekowanych maszynach i przejmowania standardowych funkcji do wykonywania szkodliwych operacji. Ustalenie szczegółów zajęło mu prawie cały dzień, a gdy wreszcie zakończył pracę, był zdumiony.

Kod wykonujący w komputerach z systemem Windows typowe zadania, takie jak otwieranie i wczytywanie plików lub zapisywanie ich zawartości na dysku, jest zwykle przechowywany w plikach .DLL systemu operacyjnego. Gdy system operacyjny lub inna aplikacja chce wykonać jedno z takich zadań, wywołuje odpowiedni kod z pliku .DLL (podobnie jak użytkownik biblioteki wypożycza książkę) i uruchamia go w pamięci maszyny. Tradycyjni hakerzy starają się umieścić kod szkodliwych operacji w plikach .DLL systemu Windows, jednak skanery antywirusowe potrafią wykryć w bibliotece

[1] Eksploit z pendrive'ów wykorzystujący pliki .LNK był skonfigurowany w taki sposób, aby umieszczał Stuxneta na tylko trzech nowych maszynach, a następnie kończył pracę i usuwał pliki z pendrive'a.

[2] Dowody znalezione w wersjach Stuxneta analizowanych przez Symantec wskazywały na to, że pierwsza infekcja w Iranie wystąpiła 23 czerwca 2009 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

kod, który nie powinien się tam znajdować. Dlatego Stuxnet umieszczał szkodliwy kod w pamięci komputera, gdzie trudniej jest go wykryć programom antywirusowym. Samo to nie było godne uwagi, ponieważ wielu pomysłowych hakerów stosowało to podejście. Niezwykły był natomiast *sposób* uruchamiania kodu przez Stuxneta.

Szkodliwy kod kryjący się w pamięci zwykle musi zażądać od systemu wczytania dodatkowego kodu z plików przechowywanych na dysku komputera. Jednak programy antywirusowe potrafią to wykryć, dlatego twórcy Stuxneta zastosowali lepsze rozwiązanie. Stuxnet cały potrzebny kod zawierał w sobie, przechowując go w wirtualnych plikach o specjalnych nazwach. Standardowo takie rozwiązanie nie powinno zadziałać, ponieważ w momencie wywołania kodu przez Stuxneta system operacyjny nie rozpoznałby nazw lub szukałby na dysku nieistniejących plików o dziwnych nazwach. Jednak Stuxnet „zwiódł" (przeprogramował) część interfejsu API systemu Windows (jest to interfejs między systemem operacyjnym a działającymi w nim programami) w taki sposób, że po wywołaniu plików o dziwnych nazwach system operacyjny zwracał się do dostępnego w pamięci Stuxneta i pobierał od niego kod. Stuxnet był też przygotowany na to, że program antywirusowy podejrzliwie potraktuje pliki z pamięci i spróbuje je zbadać. Ponieważ robak kontrolował fragmenty interfejsu API systemu Windows odpowiedzialne za określanie atrybutów plików, potrafił przekonać skaner, że pliki te są puste. Była to informacja: „Nie ma tu czego oglądać, proszę iść dalej"[3].

To jeszcze nie wszystko. Zwykłe złośliwe oprogramowanie uruchamia kod w prosty sposób, wywołując i odpalając go. Jednak w Stuxnecie to byłoby zbyt proste. Stuxnet był zbudowany jak maszyna Rube'a Goldberga i zamiast bezpośrednio wywoływać oraz uruchamiać kod, umieszczał go w innym bloku, który był już wykonywany w jednym z procesów maszyny. Następnie umieszczał kod z tego procesu w bloku działającym w *innym* procesie, aby dodatkowo utrudnić zrozumienie tego, co się dzieje.

---

[3] Nicolas Falliere, Liam O'Murchu, Eric Chien, „W32.Stuxnet Dossier". Jest to raport z lutego 2011 r., s. 13 – 15, dostępny na stronie: *https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*. W tym obszernym raporcie Symanteca szczegółowo opisane są specyfikacja techniczna Stuxneta oraz przeznaczenie poszczególnych komponentów kodu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

O'Murchu był zdumiony ilością pracy, jaką napastnicy włożyli w skok. Nawet najbardziej złożone ataki, z jakimi zetknął się we wcześniejszych latach, nie były aż tak skomplikowane. Przeciętny autor złośliwego oprogramowania robił tylko to, co konieczne, aby atak się powiódł i nie został wykryty. Niewiele można było zyskać, poświęcając dużo czasu na pisanie kodu, który miał tylko szybko przechwycić hasła lub inne dane. Nawet w zaawansowanych narzędziach szpiegowskich, których źródła dopatrywano się w Chinach, nie stosowano sztuczek wykorzystanych w Stuxnecie. Wiele miejsc kodu było alarmujących, a O'Murchu zbadał tylko pierwszych 5 kB z 1 MB zagrożeń.

Było jasne, że jest to niestandardowy atak wymagający dokładnej analizy. Jednak długość i złożoność kodu sprawiały, że potrzebny był cały zespół ludzi do zastosowania inżynierii odwrotnej i zbadania plików. O'Murchu zastanawiał się, czy w ogóle powinien się tym zajmować. Nikt nie winiłby Symanteca, gdyby pracownicy firmy zrezygnowali z dalszych analiz kodu i przeszli do innych zadań. W końcu głównym zadaniem każdego producenta programów antywirusowych jest powstrzymanie infekcji lub pozbycie się z zainfekowanych systemów złośliwego oprogramowania, które już się w nich znajduje. To, co szkodliwy kod robi z zainfekowanymi komputerami, jest mniej istotne.

Jednak choć podstawowe zadanie kończy się w momencie wykrycia zagrożenia, każdy klient zainfekowany Stuxnetem chciałby wiedzieć, co złośliwe oprogramowanie zrobiło z jego systemem — także w sytuacji, gdy Symantec już wykrył i usunął szkodliwe pliki. Czy Stuxnet wykradł dane osobowe lub ważne dokumenty? A może zmodyfikował lub usunął istotne dane? O'Murchu uznał, że odkrycie tego jest jego obowiązkiem.

Nie był to jedyny powód, dla którego chciał lepiej zapoznać się z kodem. Po prawdzie Stuxnet był atrakcyjny z powodu adrenaliny, jaką wzbudzało rozwiązywanie tej zagadki. Wykryty wirus był zdecydowanie zbyt złożony jak na narzędzie szpiegowskie i zbyt zaawansowany jak na dzieło przeciętnych cyberprzestępców. O'Murchu zwyczajnie musiał się dowiedzieć, o co w tym chodzi.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

POD KONIEC PIERWSZEGO dnia pracy nad robakiem O'Murchu zapisał notatki obejmujące jego dotychczasowe odkrycia i przesłał je do zespołu Symanteca w Tokio, żałując, że nie miał więcej czasu na zajęcie się kodem.

Zespół w Tokio przez część weekendu pracował, tworząc mapę komponentów Stuxneta i przeprowadzając wysokopoziomową analizę kodu, tak aby każdy mógł zrozumieć, czym firma się zajmuje. W Kalifornii O'Murchu, który ze swoją dziewczyną, Angielką, mieszkał w pobliżu plaży Marina del Rey, bez powodzenia próbował zapomnieć o analizowanym kodzie. Nie potrafił pozbyć się z głowy myśli o skomplikowanym sposobie przechwytywania kontroli nad systemem, aż w końcu zaczął wątpić w swoją ocenę tego, na co natrafił. W celu pozbycia się wątpliwości wrócił do biura, aby ponownie przyjrzeć się kodowi. W końcu przekonał się, że miał rację.

W poniedziałek rano z niecierpliwością czekał na spotkanie ze współpracownikiem, Erikiem Chienem, i podzielenie się swoimi odkryciami. Chien, podobnie jak O'Murchu, został przeniesiony z dublińskiego biura Symantecu do Culver City. Obecnie zajmował stanowisko dyrektora technicznego w zespole reagowania na zagrożenia. Chien zdecydował, że powinni zadzwonić do Nicolasa Falliere'a, młodego wiekiem starszego inżyniera oprogramowania i analityka w paryskim biurze Symantecu, uznawanego za specjalistę od dekonstrukcji skomplikowanego kodu. We trzech opracowali plan rozwiązania problemu.

Stuxnet był bardzo rozbudowany i miał dużo różnych elementów, jednak oczywistym punktem wyjścia były serwery C&C. W czasie gdy Falliere zapoznawał się z elementami Stuxneta, które O'Murchu już odkrył, Chien i O'Murchu skupili się na wspomnianych serwerach.

Stuxnet za każdym razem, gdy zainfekował system, „dzwonił do domu" — do jednej z dwóch domen internetowych udających witryny dla fanów piłki nożnej: mypremierfutbol.com i todaysfutbol.com. Nazwy tych domen, zarejestrowane na fałszywe nazwiska z użyciem fałszywych kart kredytowych, prowadziły do zlokalizowanych w Danii i Malezji serwerów pełniących w ataku funkcję stacji C&C. Po zainfekowaniu maszyny Stuxnet każdorazowo kontaktował się z tymi serwerami, aby powiadomić je o „podboju" i przekazać informacje o najnowszej ofierze. Komunikacja była zaszyfrowana, aby uniemożliwić przypadkowym osobom jej podsłuchanie,

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

napastnicy zastosowali jednak zaskakująco słaby szyfr, który łatwo było złamać. Gdy Chien i O'Murchu poradzili sobie z nim, zobaczyli, że Stuxnet przekazywał napastnikom nazwy komputera i domeny, a także wewnętrzny adres IP, używaną wersję systemu Windows oraz informację o tym, czy na maszynie zainstalowane jest oprogramowanie firmy Siemens[4].

Każdy fragment tych danych zapewne pomagał napastnikom ustalić, czy Stuxnet zbliża się do celu. Było to istotne, ponieważ atak był prowadzony na oślep. Po wypuszczeniu samopowielający się robak, taki jak Stuxnet, zaczyna żyć własnym życiem, a napastnicy nie mają kontroli nad przemieszczaniem się szkodliwego kodu. Dane przesyłane na serwery pomagały w pewnym zakresie śledzić drogę robaka wędrującego w sieci w poszukiwaniu ofiary.

Jednak spośród wszystkich informacji przesyłanych przez Stuxneta do jego właścicieli najważniejsze były dane dotyczące Siemensa. Było tak, ponieważ — jak badacze mieli wkrótce ustalić — gdy Stuxnet stwierdzał, że znajduje się w systemie *bez* zainstalowanego oprogramowania Siemensa, kończył pracę. Nadal szukał innych maszyn do zainfekowania, ale nie uruchamiał ładunku (ang. *payload*) na żadnym komputerze bez oprogramowania Siemensa.

[4] Nazwa domeny i zewnętrzny adres IP maszyny (zewnętrzny adres maszyn podłączonych do internetu) mogą ujawnić nazwę organizacji lub firmy, do której ta maszyna należy. Ustalanie właściciela odbywa się na podstawie tego, do kogo należy blok adresów IP obejmujący adres danej maszyny. Mogło to pomagać napastnikom w ustalaniu, jak szybko i daleko Stuxnet się rozprzestrzenia. Te informacje informowały ich też o tym, że Stuxnet zboczył z drogi i zaczął pojawiać się w obszarach odległych od celu. Wewnętrzne adresy IP to adresy przypisywane przez firmę maszynom na potrzeby ich mapowania i kierowania ruchem w sieci. Te adresy IP mogą być przydatne, jeśli napastnicy posiadają mapę wewnętrznej sieci zainfekowanej firmy lub organizacji (np. wykradzioną z komputera administratora systemu), określającą wewnętrzny adres IP przypisany do każdej maszyny. W takim scenariuszu napastnicy mogli śledzić, jaką drogę pokonywał Stuxnet w sieci, infekując kolejne maszyny i przekazując informacje do serwerów C&C za każdym razem, gdy zainfekował komputer podłączony do internetu. Nazwy komputerów mogły pomagać napastnikom w określeniu, do jakiego pracownika lub do której grupy roboczej należała zainfekowana maszyna. Na przykład jeden z komputerów nosił nazwę GORJI-259E4B69A, a inny PEYMAN-PC. Jednak wiele zainfekowanych systemów miało takie same domyślne nazwy: ADMIN-PC, USER-PC lub laptop-dom, przez co trudniej było odróżnić takie maszyny od siebie.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wszystkie systemy bez takiego oprogramowania były tylko środkiem do celu Stuxneta[5].

O'Murchu skontaktował się z dostawcami usług DNS (ang. *Domain Name System*) w sprawie dwóch domen C&C i poprosił, by ruch był kierowany nie do napastników, ale do kontrolowanego przez Symantec ujścia — komputera przeznaczonego do odbioru danych wysyłanych przez Stuxneta. Dostawcy usług DNS są jak policjanci kierujący ruchem w internecie i dbają o to, by e-maile i przeglądarki docierały do celu. To dzięki nim gdy ktoś wpisze w przeglądarce adres *nytimes.com* lub kliknie odnośnik do witryny, dociera pod odpowiedni adres IP[6]. Przekierowanie ruchu do ujścia pozwoliło badaczom rejestrować w czasie rzeczywistym dane, które Stuxnet, jak dobry żołnierz, miał przekazywać napastnikom. Od wtorkowego poranka 20 lipca te dane trafiały do ujścia Symanteca.

Gdy zgłaszały się kolejne zainfekowane maszyny, O'Murchu i Chien tworzyli mapę domen i państw, z których napływały zgłoszenia, i analizowali dane przesyłane przez Stuxneta, szukając w nich powtarzających się cech. Między innymi chcieli określić liczbę zainfekowanych maszyn z oprogramowaniem Siemensa. Do końca tygodnia z ujściem skontaktowało się ponad 38 tys. zainfekowanych maszyn z dziesiątków państw. Dziennie Stuxnet atakował 9000 maszyn, a liczba ta szybko rosła. Ostatecznie badacze namierzyli ponad 100 tys. infekcji w ponad 100 krajach[7]. Mimo sygnatur dodanych

[5] Aleks Gostiew, główny ekspert ds. złośliwego oprogramowania w rosyjskiej firmie Kaspersky Lab, odkrył, że Stuxnet przesyłał do serwerów C&C plik *Oem6c.pnf*, informujący nie tylko o tym, który program Siemensa jest zainstalowany na komputerze (narzędzie programistyczne Step 7 lub program WinCC używany przez operatorów do monitorowania stanu sterowników PLC), ale też o liście plików projektów narzędzia Step 7 i prowadzących do nich ścieżkach. Pliki projektów narzędzia Step 7 zawierały instrukcje programów dla sterowników PLC. Gostiew podejrzewał, że napastnicy po znalezieniu na maszynie plików projektów mogli przesyłać na nią inne narzędzie w celu wykradzenia tych plików i znalezienia w nich danych konfiguracyjnych. Pozwalało to ustalić, czy Stuxnet znalazł szukane systemy.

[6] Gdy Symantec skontaktował się z dostawcami usług DNS, ci nie kierowali już ruchu do dwóch domen napastników. Zamiast tego przekierowywali go pod adres IP 127.0.0.1, który jest powszechnie używany do zwracania danych do maszyny nadawcy.

[7] Liczba 100 tys. została ustalona przez Symantec w pierwszych sześciu miesiącach od wykrycia Stuxneta. Jednak łączna liczba infekcji, oszacowana na podstawie danych z innych firm antywirusowych dodających mechanizmy wykrywania tego zagrożenia do swoich produktów, ostatecznie wzrosła do ponad 300 tys. (według firmy Kaspersky Lab).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

przez producentów programów antywirusowych w celu powstrzymania ataku Stuxnet wciąż się rozprzestrzeniał. Świadczyło to o tym, że wiele ofiar nie zainstalowało najnowszego oprogramowania antywirusowego. Wśród zainfekowanych maszyn komunikujących się z ujściem zdarzały się też komputery producentów programów antywirusowych. Oznaczało to, że badacze z niektórych konkurencyjnych firm nadal uruchamiali Stuxneta na testowych komputerach.

Gdy O'Murchu i Chien przeanalizowali geograficzne lokalizacje infekcji, dostrzegli nieoczekiwany wzorzec. Spośród 38 tys. namierzonych maszyn ponad 22 tys. znajdowały się w Iranie. Na drugim miejscu, ze znacznie mniejszą liczbą 6700 komputerów, była Indonezja, a na trzecim Indie (3700 komputerów). W Stanach Zjednoczonych odnotowano niecałe 400 infekcji, a w innych państwach jeszcze mniej. Tylko w niewielkiej części zainfekowanych maszyn zainstalowane było oprogramowanie Siemensa. Większość z tych maszyn znajdowała się w Iranie (217). W Stanach Zjednoczonych było ich tylko 16[8].

Liczba infekcji była niezgodna ze wzorcami wcześniejszych ataków, kiedy to Iran nigdy nie zajmował wysokich miejsc (jeśli w ogóle występował na listach). Nawet gdy ataki rozpoczynały się na Bliskim Wschodzie lub w Azji Środkowej, Iran nie pojawiał się wysoko na listach. Było więc oczywiste, że napastnicy chcieli przeprowadzić skoncentrowany atak na tę republikę islamską. Skoro jednak byli zainteresowani przede wszystkim maszynami z oprogramowaniem Siemensa w Iranie, to Stuxnet rozprzestrzenił się znacznie poza docelowy obszar. Ponadto dlaczego rozmnożył się bardziej w Indiach i Indonezji niż w Stanach Zjednoczonych i Europie? Co Iran, Indie i Indonezja miały ze sobą wspólnego, że infekcje skoncentrowały się w tych państwach? Z uwagi na czas i pieniądze, jakie z pewnością były potrzebne do opracowania kodu Stuxneta, badacze wiedzieli, że nie szukają kogoś, kto chce wykraść receptury leków lub sekrety produkcji samochodów. Było to sprzeczne ze spekulacjami Boldewina. Celem napastników musiało być wykradzenie informacji o krytycznych systemach — możliwe, że o strategicznym politycznym znaczeniu dla regionu.

[8] Na przesłuchaniu w senacie Stanów Zjednoczonych w listopadzie 2010 r. Dean Turner, dyrektor globalnej sieci pozyskiwania informacji w firmie Symantec, zeznał, że liczba unikatowych infekcji w Stanach Zjednoczonych doszła do tego czasu do 1600. Spośród tych komputerów na 50 zainstalowane było oprogramowanie WinCC Siemensa.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Oprogramowanie Siemensa szukane przez Stuxneta było używane nie tylko w przemyśle, ale też w krytycznych systemach infrastrukturalnych. Chien poszukał w Google'u informacji o Iranie i Indiach, aby ustalić, co te kraje mają ze sobą wspólnego. Odkrył świeże wiadomości na temat gazociągu budowanego w celu połączenia obu państw. Tak zwany Gazociąg Pokoju miał obejmować liczący ok. 2700 km rurociąg biegnący z pola gazowego South Pars w południowym Iranie przez Pakistan do Indii. Tym planom stanowczo sprzeciwiały się Stany Zjednoczone. Projekt przez lata przechodził różne fazy w zależności od zmian geopolitycznych i problemów z finansowaniem. W 2009 r. Indie wycofały się z niego z powodu presji Stanów Zjednoczonych, jednak w maju 2010 r., dwa miesiące przed wykryciem Stuxneta, ponownie zaangażowały się w projekt. W tym samym miesiącu Iran rozpoczął projektowanie i budowę ostatniego fragmentu gazociągu po swojej stronie granicy.

Jednak w nagłówkach wiadomości dotyczących Iranu dominował inny temat — szybko rozwijany program nuklearny. Iran miał uruchomić reaktor w miejscowości Buszehr na południu kraju, co przez lata było źródłem poważnych napięć między tym krajem a Izraelem i państwami zachodnimi. Jeszcze bardziej kontrowersyjny był zakład wzbogacania uranu w Natanzie, zbudowany w celu zapewnienia paliwa dla wspomnianego reaktora. ONZ przegłosowała nałożenie sankcji na Iran z powodu tego zakładu. Prowadzone były też rozmowy na temat możliwych nalotów na tę jednostkę.

Zaczął pojawiać się obraz związany z sytuacją geopolityczną. Zaawansowany charakter szkodliwego kodu w połączeniu ze skradzionymi certyfikatami i centrum infekcji zlokalizowanym w Iranie sprawiały wrażenie, że Stuxnet mógł być produktem tajnej rządowej misji szpiegowskiej, takiej jednak, która najwyraźniej wymknęła się spod kontroli. Ponieważ celem wydawał się Iran, lista podejrzanych była krótka: Izrael, Chiny, Rosja lub Stany Zjednoczone.

Chien przerwał pracę, aby zastanowić się nad implikacjami. Jeśli Stuxnet *był* produktem rządowej misji szpiegowskiej, zwłaszcza amerykańskiej, to zastosowanie przez badaczy ujścia było zuchwałym posunięciem. Przechwytując dane, które napastnicy spodziewali się uzyskać z zainfekowanych maszyn z Iranu, badacze zostali wplątani w międzynarodowy incydent, a ponadto mogli się przyczynić do sabotażu tajnej operacji. Potencjalne konsekwencje były przytłaczające.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak dla Chiena nie mogło mieć to decydującego znaczenia. Zadaniem Symanteca nie było chronienie tajnych rządowych operacji, i to niezależnie od tego, który kraj je prowadził. Ich misją było zabezpieczanie maszyn klientów. Nie miało znaczenia, kto wypuścił szkodliwy kod lub co było jego celem. Jeśli ten kod zagrażał klientom Symanteca, trzeba było go powstrzymać.

Choć głównym celem wydawały się maszyny w Iranie, gdzie Symantec nie miał klientów, Stuxnet zainfekował także tysiące komputerów w innych krajach i cały czas się rozprzestrzeniał. Badacze wciąż nie wiedzieli, co ma robić szkodliwy ładunek lub czy zawiera on kod, który może wpłynąć na maszyny niebędące celem Stuxneta.

Nie można też było wykluczyć, że Iran był źródłem ataku, a nie jego celem. Możliwe, że irańscy inżynierowie opracowali Stuxneta w celu zaatakowania maszyn w Stanach Zjednoczonych, ale utracili kontrolę nad nim w laboratorium. To tłumaczyłoby infekcje w Iranie. Co się stanie, jeśli teraz Stuxnet rozprzestrzeni się w krytycznych systemach w Stanach Zjednoczonych — w elektrowni, w układach kontroli tam lub w systemach kolejowych?

Chien i O'Murchu zdecydowali, że muszą kontynuować pracę. Ewentualnymi politycznymi skutkami tej decyzji zajmą się w przyszłości.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 3

NATANZ

Gdy Chien i O'Murchu zastanawiali się nad swoją nową rolą w polityce międzynarodowej, tysiące kilometrów dalej, w Iranie, technicy w Natanzie wciąż zmagali się z problemami z wirówkami. Choć w poprzednich miesiącach wymienili ok. 1000 urządzeń, kaskady działały z wydajnością od 45 do 66% i pobierały znacznie mniej uranu (w postaci gazowej), niż potrafiły wzbogacić. Dla inspektorów z MAEA nie było jasne, czy problemy wynikają z naturalnych trudności związanych z „dojrzewaniem" nowego zakładu (w Natanzie wzbogacanie uranu rozpoczęto w 2007 r., jednak technicy wciąż instalowali nowe kaskady i rozwiązywali problemy), czy dzieje się coś złego. To ostatnie nie byłoby zaskoczeniem. Zakład w Natanzie był poddany międzynarodowej kontroli i nie było sekretem, że wielu ludziom bardzo zależy na jego zamknięciu. Próbowano do tego doprowadzić od prawie dziesięciu lat.

STAROŻYTNE MIASTO NATANZ zbudowano ok. 320 km na południe od Teheranu. Znajduje się tam pochodzące z XIII w. mauzoleum sufickiego szejka Abd Al-Samada Esfahaniego. To mauzoleum, z eleganckimi cegłami z terakoty i kobaltowymi płytkami w wyrafinowane wzory, jest modelowym przykładem architektury wczesnej Persji. Choć Natanz leży w cieniu gór Karkas na skraju Wielkiej Pustyni Słonej, to wysoko położone miasto ogrodów posiada ożywiający górski klimat i wiele naturalnych źródeł.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Od dawna było znane z płodnych sadów, przede wszystkim z soczystych gruszek. Jednak od 14 sierpnia 2002 r. stało się słynne z innego powodu. Tego dnia Narodowa Rada Oporu Iranu (ang. *National Council of Resistance of Iran* — NCRI), koalicja irańskich grup opozycyjnych na uchodźstwie, zorganizowała konferencję prasową w hotelu Willard InterContinental w Waszyngtonie (dwie przecznice od Białego Domu), aby ogłosić, że Iran buduje nielegalny obiekt jądrowy w Natanzie.

Ponad 20 dziennikarzy i przedstawicieli organizacji pozarządowych, ekspertów i irańskich obserwatorów zapełniło salę Tafta na drugim piętrze hotelu, aby wysłuchać relacji NCRI. Jednym z słuchaczy była 29-letnia blondynka, Corey Hinderstein, pracująca dla Instytutu Nauki i Bezpieczeństwa Międzynarodowego (ang. *Institute for Science and International Security* — ISIS), organizacji *non profit* dążącej do nierozprzestrzeniania broni jądrowej i obserwującej działalność nuklearną w Iranie oraz innych państwach.

Gdy goście usiedli, a operator kamery z sieci telewizyjnej C-SPAN zajął stanowisko z tyłu sali, Alireza Jafarzadeh, rzecznik NCRI, od razu przeszedł do sedna. „Choć pozornie [irańska] główna działalność nuklearna koncentruje się wokół elektrowni jądrowej w Buszehrze — powiedział do szeregu mikrofonów — w rzeczywistości prowadzonych jest wiele tajnych programów nuklearnych bez wiedzy MAEA. […] Niedługo ujawnię dwie ściśle tajne lokalizacje, które irańskiemu reżimowi do dziś udawało się utrzymać w tajemnicy”[1].

Hinderstein i inni skupili uwagę.

Irański reaktor atomowy w Buszehrze, starożytnym nadbrzeżnym mieście nad Zatoką Perską, budowano z przerwami od 30 lat. Była to jedna z lokalizacji, którą Iran wskazał jako obiekt jądrowy w ramach porozumienia o zabezpieczeniach z MAEA, agencją ONZ-etu monitorującą działalność jądrową na całym świecie w celu zapewnienia, że państwa takie jak Iran nie wykorzystają cywilnych obiektów atomowych do potajemnej produkcji broni jądrowej.

[1] Przemówienie Alirezy Jafarzadeha jest dostępne w bibliotece C-SPAN na stronie: *https://www.c-span.org/video/?172005-1/iran-nuclear-weapons*. Nieoficjalną transkrypcję komentarzy Jafarzadeha znajdziesz na stronie: *http://www.iranwatch.org/library/ncri-new-information-top-secret-nuclear-projects-8-14-02*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Iran przez lata utrzymywał, że program realizowany w Buszehrze (elektrownia miała rozpocząć pracę w 2005 r.) był całkowicie pokojowy[2]. Jednak od dawna mówiono o tajnych obiektach jądrowych w Iranie, w tym o ukrytych zakładach wzbogacania uranu, które mogły służyć do produkcji materiałów do broni jądrowej. W 2001 r. źródła rządowe (amerykańskie i inne) poinformowały współpracowników Hinderstein z ISIS, że tajne obiekty atomowe rzeczywiście istnieją w Iranie, jednak nie podały szczegółów, które mogłyby pomóc w śledztwie. Teraz wyglądało na to, że słabo zorganizowana grupa dysydentów, do której należał Jafarzadeh, może wreszcie zapewnić dowody poszukiwane przez ISIS i inne jednostki.

Jafarzadeh, mężczyzna z grubym ciemnym wąsem zakrywającym górną wargę, ujawnił nazwy dwóch obiektów jądrowych położonych daleko na północ od Buszehru. Jednym z nich był zakład produkcji ciężkiej wody budowany na brzegu rzeki Qara-Chai w pobliżu Araku. „Każdy, kto ma plany dotyczące broni nuklearnej, z pewnością będzie chciał prowadzić projekty związane z ciężką wodą" — powiedział Jafarzadeh[3].

Drugi obiekt to zakład produkujący paliwo nuklearne budowany w pobliżu starej autostrady łączącej Natanz z miastem Kaszan. Był to wspólny projekt Agencji Energii Atomowej Iranu (ang. *Atomic Energy Organization of Iran* — AEOI) i irańskiej Najwyższej Rady Bezpieczeństwa Narodowego. Aby ukryć rzeczywiste przeznaczenie fabryki, założone zostały firmy przykrywki sekretnie zaopatrujące zakład w materiały i technologie. Jedną z nich była Kala Electric (znana też jako Kalaye Electric Company).

---

[2] Choć eksperci od nierozprzestrzeniania broni jądrowej nie przejmowali się tym, że pluton z reaktora lekkowodnego w Buszehrze posłuży do produkcji broni (nie był to dobry materiał do tego celu), z obiektem tym związane były inne problemy. Zastępca asystenta sekretarza obrony Marshall Billingslea 29 lipca 2002 r. poinformował senat o obawach przed tym, że Buszehr jest „pretekstem do zbudowania infrastruktury, która miała pomóc Teheranowi w uzyskaniu broni atomowej". Oznaczało to, że materiały zakupione na potrzeby obiektu w Buszehrze mogły posłużyć do tajnych prac nad bronią nuklearną.

[3] Ciężka woda to woda o wysokiej zawartości deuteru (izotopu wodoru). Ma cywilne zastosowania jako chłodziwo i moderator w elektrowniach. Przydaje się też w reaktorach badawczych do produkcji izotopów medycznych. Jednak zużyte paliwo z elektrowni może zawierać pluton i inne materiały, które po przetworzeniu można wykorzystać do produkcji broni nuklearnej. Reaktory ciężkowodne są lepszym źródłem plutonu niż reaktory lekkowodne (jakie budowano w Buszehrze).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Później pojawiła się w związku ze Stuxnetem jako jedna z firm, które mogły zostać zainfekowane omawianą tu bronią cyfrową[4].

Budowa kompleksu w Natanzie, który według Jafarzadeha zajmował 100 tys. m^2 i kosztował już 300 mln dolarów, została rozpoczęta w 2000 r. i miała trwać trzy miesiące. Wtedy to robotnicy mieli zacząć instalowanie wyposażenia. Przykrywką dla zakładu był projekt eradykacji pustyni. Musiałby to jednak być niezwykle istotny projekt eradykacji, ponieważ były premier Iranu odwiedził zakład wcześniej w tym samym miesiącu jako reprezentant Najwyższej Rady Bezpieczeństwa Narodowego, a szef AEOI co miesiąc gościł w pobliskim Kaszanie, aby śledzić prace. Ponadto robotnicy nie mogli rozmawiać na temat projektu z lokalnymi urzędnikami. Według Jafarzadeha niedawno zaistniał spór między AEOI a biurem gubernatora Kaszanu, ponieważ AEOI nie udostępniała biuru informacji na temat zakładu, a gdy zastępca gubernatora generalnego prowincji chciał odwiedzić plac budowy w Natanzie, nie został wpuszczony.

Gdy Jafarzadeh opowiadał o szczegółach zakładu i pokazywał plansze z siecią firm przykrywek oraz ludzi kierujących projektem, Hinderstein robiła notatki w notebooku. Ogólna lokalizacja obiektów, a także nazwy i adresy firm przykrywek były pierwszymi solidnymi dowodami, które ISIS zdobyła na temat nielegalnego irańskiego programu jądrowego i które można było zweryfikować.

Hinderstein zwróciła też uwagę na moment ujawnienia informacji. Iran był sygnatariuszem Układu o nierozprzestrzenianiu broni jądrowej i zgodnie z porozumieniem o zabezpieczeniach z MAEA był zobowiązany do ujawnienia istnienia każdego nowego obiektu jądrowego 180 dni przed pojawieniem się w danym zakładzie materiałów jądrowych, tak aby inspektorzy mogli rozpocząć monitorowanie go. Jeśli zakład w Natanzie rzeczywiście miał zostać ukończony za 90 dni, grupa Jafarzadeha ujawniła to w ostatnim momencie, w którym inspektorzy MAEA mogli zażądać dostępu do obiektu przed jego otwarciem.

Pojawiły się oczywiste pytania o to, w jaki sposób grupa NCRI zdobyła ściśle tajne informacje, które przez lata najwyraźniej były niedostępne dla najlepszych agencji szpiegowskich świata. Jafarzadeh utrzymywał, że grupa otrzymała dane od osób z Iranu bezpośrednio zaangażowanych w program,

[4] Więcej informacji znajdziesz na s. 105.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

a także dzięki szeroko zakrojonym analizom i badaniom. Jednak bardziej prawdopodobne było to, że uzyskała informacje od agencji wywiadowczych Stanów Zjednoczonych lub Izraela[5]. Izrael już wcześniej ujawniał zdobyte przez wywiad dane poprzez pośredników, aby wpłynąć na opinię publiczną bez podejrzeń o chęć uzyskania korzyści politycznych. Naturalnie miał największe powody do obaw przed uzyskaniem przez Iran broni jądrowej, jednak nagłaśnianie przez Izraelczyków działalności jądrowej innych państw byłoby oczywistą hipokryzją, ponieważ kraj ten przez długi czas prowadził własny tajny program produkcji broni jądrowej, do czego nigdy się publicznie nie przyznał[6]. Z tego powodu oraz z innych przyczyn Izrael prowadził w ukryciu polityczne machinacje, przekazując informacje zachodnim rządom, agencji MAEA i grupom takim jak organizacja Jafarzadeha.

Jeśli informacje rzeczywiście pochodziły od Amerykanów lub Izraelczyków, wybór grupy Jafarzadeha do ich ujawnienia był zaskakujący. NCRI była politycznym ramieniem organizacji Ludowych Mudżahedinów (pers. *Mujahedin-e Khalq* — MEK), irańskiej grupy opozycyjnej znanej niegdyś z antyizraelskich i antyamerykańskich poglądów. Organizacja ta została oskarżona o zamordowanie ośmiu Amerykanów w Iranie w latach 70. ubiegłego wieku, a także o podłożenie w 1981 r. w Iranie bomb, które zabiły ponad 70 osób, w tym irańskiego prezydenta i premiera. Ludowi Mudżahedini od 1997 r. znajdowali się na liście organizacji terrorystycznych Departamentu Stanu USA, jednak od tego czasu starali się poprawić swój wizerunek, by

[5] Jafarzadeh powiedział, że grupa NCRI otrzymała informacje na kilka dni przed opisaną konferencją prasową. Jako ich źródło wskazał działających w Iranie członków ruchu oporu. „Są to ludzie, którzy byli bezpośrednio powiązani z tymi pracami [i] mieli bezpośredni dostęp do informacji o tego rodzaju działaniach — powiedział zgromadzonym reporterom. — Z pewnością są to osoby, które posiadają dostęp do tych danych w ramach reżimu". Zapytany o to, czy grupa udostępniła swoje informacje władzom Stanów Zjednoczonych, Jafarzadeh starannie dobierał słowa. Dane „zostały udost… — zaczął mówić — były dostępne dla właściwych władz tego kraju. Nie wiem na razie, jaka była ich reakcja". Dwa lata później dyrektor CIA George Tenet wypowiedział się na temat tych i innych odkryć grupy NCRI. „Chcę zapewnić, że to, do czego Iran ostatnio przyznał się w sprawie programów nuklearnych, potwierdza dane naszego wywiadu. Błędem jest twierdzenie, że zostaliśmy zaskoczeni zeszłorocznymi raportami irańskiej opozycji". Tenet przemawiał na Georgetown University 5 lutego 2004 r. Transkrypcja jego wypowiedzi jest dostępna na stronie: *https://www.cia.gov/news-information/speeches-testimony/2004/tenet_georgetownspeech_02052004.html*.

[6] Izrael potajemnie dołączył do grupy potęg nuklearnych w 1967 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

skreślono ich z tej listy. Udział w ujawnieniu tajnych obiektów nuklearnych w Iranie z pewnością pomógłby w zdobyciu poparcia w tej kwestii w Kongresie Stanów Zjednoczonych[7].

NCRI w przeszłości wygłaszała prowokacyjne tezy na temat irańskiego programu nuklearnego, ale niektóre z nich okazały się fałszywe. Dlatego pojawiły się wątpliwości co do wiarygodności nowych informacji. Jafarzadeh twierdził, że zakład w Natanzie ma produkować paliwo, jednak dla Hinderstein i jej współpracowników z ISIS nie miało to sensu. Iran już planował budowę zakładu do produkcji paliwa nieopodal Natanzu, dlatego stawianie drugiego w tak niewielkiej odległości wydawało się nielogiczne. Mimo to ISIS była gotowa na razie uznać ujawnione informacje za prawdziwe. Jednak w celu ich weryfikacji Hinderstein postanowiła zdobyć zdjęcia satelitarne i spróbować znaleźć na nich dowody w postaci budowy pasującej do opisu Jafarzadeha.

Hinderstein pracowała dla ISIS od sześciu lat. Trafiła do tej organizacji prosto z uczelni. Z czasem stała się ekspertem od zdjęć satelitarnych — nowego narzędzia, które dopiero od niedawna stało się dostępne dla organizacji takich jak ISIS. Przez dziesięciolecia dostęp do zdjęć satelitarnych — zwłaszcza o wysokiej rozdzielczości — był możliwy wyłącznie dla agencji rządowych i wywiadu. Jedyną możliwość obejrzenia zdjęć z przestrzeni kosmicznej dawało opublikowanie ich przez agencję rządową lub instytut badawczy, co zdarzało się rzadko. Od połowy lat 90. ubiegłego wieku możliwy stał się zakup takich zdjęć, jednak były one nieostre. Dopiero po paru latach dostępne stały się zdjęcia o rozdzielczości 1,6 m, pozwalające dobrze przyjrzeć się szczegółom.

ISIS była jedną z pierwszych organizacji pozarządowych, które zainwestowały w drogie oprogramowanie potrzebne do analizowania takich zdjęć. Szybko zrozumiała istotną rolę takich zdjęć w działaniach na rzecz nierozprzestrzeniania broni jądrowej. Pierwsze doświadczenia w analizowaniu zdjęć satelitarnych Hinderstein zdobyła w 1998 r., po tym jak Pakistan

[7] Lobbing grupy NCRI zadziałał. Z pomocą i wsparciem licznych amerykańskich prawodawców, a także byłych przywódców FBI i CIA grupa doprowadziła w 2012 r. do skreślenia jej z listy organizacji terrorystycznych. Zwolennicy nazwali tę grupę lojalnym sprzymierzeńcem Stanów Zjednoczonych i podkreślali jej rolę w ujawnieniu tajnego irańskiego programu nuklearnego jako jeden z powodów, dla których należy usunąć NCRI ze wspomnianej listy.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

przeprowadził sześć podziemnych testów nuklearnych w reakcji na podziemne próby atomowe w Indiach. Pracując z ekspertem od zdjęć satelitarnych, nauczyła się identyfikować na fotografiach spikselizowane obiekty oraz interpretować cienie i gradacje kolorów w celu określenia głębokości na dwuwymiarowych zdjęciach.

Mniej więcej dwa miesiące po opisanej konferencji prasowej Hinderstein, uzbrojona w informacje od Jafarzadeha i szeroko zakrojone dodatkowe analizy, zalogowała się na swoje konto w serwisie Digital Globe, jednym z dwóch komercyjnych dostawców zdjęć satelitarnych w Stanach Zjednoczonych, aby poszukać dostępnych obrazów w archiwum[8]. Obecnie satelity zarejestrowały prawie wszystkie zakątki Ziemi, a większość zdjęć jest dostępna dla wszystkich za pośrednictwem aplikacji Google Earth. Jednak w 2002 r. znalezienie zdjęcia w archiwum Digital Globe było możliwe tylko, jeśli wcześniej ktoś zlecił jego wykonanie lub jeżeli firma wykonała fotografie danego miejsca z własnej inicjatywy (dotyczyło to np. wodospadu Niagara i Wielkiego Kanionu; firma wiedziała, że takie zdjęcia będą się dobrze sprzedawać). Zlecenie wykonania zdjęcia, które nie znajdowało się w archiwum, kosztowało ok. 10 tys. dolarów. Ale jeśli fotografia była już dostępna, inni mogli ją kupić za jedną trzecią tej ceny.

Używany przez Hinderstein interfejs w serwisie Digital Globe był podobny jak w aplikacji Google Maps. Na sfotografowanych obszarach pojawiały się małe szare pola. Jednak kliknięcie pola prowadziło tylko do wyświetlenia zdjęcia pomocnego przy przeglądaniu zasobów. Była to ogólna fotografia o rozdzielczości 16 m (oznacza to, że każdy piksel reprezentował 16 m powierzchni). Aby zobaczyć więcej szczegółów, należało kupić wersję o rozdzielczości 1,6 m.

Hinderstein nie mogła uwierzyć w swoje szczęście, gdy znalazła w archiwum zdjęcia okolic miast Arak i Natanz. Jafarzadeh nie podał dokładnych współrzędnych dwóch ujawnionych zakładów, dlatego musiała najpierw znaleźć Arak na mapie w serwisie Digital Globe, a następnie powoli przejść poza miasto, przeszukując okolicę w coraz większych okręgach. Wreszcie natrafiła na szare pole. Gdy kliknęła zdjęcie, stało się jasne, że — zgodnie z opisem Jafarzadeha — natrafiła na zakład produkcji ciężkiej wody.

[8] Drugą taką firmą była GeoEye.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ISIS kilka lat wcześniej zidentyfikowała taki zakład w Pakistanie, a obiekt pod Arakiem wyglądał bardzo podobnie.

Gdy Hinderstein przeszukiwała okolice Natanzu, znalazła dwie możliwe lokalizacje pośrodku pustyni, dla których dostępne były zdjęcia. W każdym z tych miejsc znajdowały się po trzy szare pola jedno na drugim. Wyglądało to tak, jakby ktoś pozostawił wielką strzałkę kierującą Hinderstein w te miejsca. Z dat wynikało, że wszystkie zdjęcia zostały wykonane 16 i 26 września, czyli kilka tygodni po konferencji prasowej Jafarzadeha. Było oczywiste, że ktoś szukał tych samych informacji. Hinderstein podejrzewała, że zrobiła to MAEA, która poprzedniego roku uruchomiła laboratorium analizy zdjęć satelitarnych. Zlecenie wykonania tych zdjęć przez MAEA po doniesieniach Jafarzadeha było zrozumiałe[9].

Hinderstein kliknęła szare pola w jednym z dwóch miejsc i szybko wykluczyła je jako lokalizację obiektu jądrowego. Kompleks miał znacznie mniej niż 100 tys. m^2 z opisów Jafarzadeha i wyglądał raczej jak zakład uzdatniania wody lub oczyszczania ścieków niż miejsce produkcji paliwa jądrowego. Jednak drugie miejsce wyglądało bardziej podejrzanie. Kompleks był znacznie większy od pierwszego i nosił oczywiste ślady wykopów na dużą skalę. Mimo rozmazanego obrazu o rozdzielczości 16 m Hinderstein potrafiła dostrzec coś, co wyglądało jak grupa budynków i wielkie sterty ziemi z wykopów za podwójnym płotem. Zauważyła też, że do obiektu prowadzi tylko jedna droga, co wskazywało na to, że dostęp do kompleksu jest ograniczony.

Gdy Hinderstein zakupiła zdjęcie o rozdzielczości 1,6 m i załadowała je do przeglądarki, zobaczyła liczne rury wychodzące z ziemi, a także sterty żwiru do produkcji betonu. Widoczne było też częściowo wyasfaltowane rondo. Po bliższym przyjrzeniu się zdjęciu Hinderstein dostrzegła coś osobliwego. Jafarzadeh stwierdził, że kompleks jest zakładem produkcji paliwa nuklearnego, jednak taka produkcja to proces przemysłowy zwykle wymagający obiektów wznoszących się ponad poziom gruntu, np. wysokich kominów. Jednak w kompleksie nie było widać kominów. Ponadto trzy wielkie budynki połączone tunelem były stawiane pod ziemią. Prace nad nimi osiągnęły końcową fazę. Wzdłuż granic kompleksu dało się też zauważyć wiele okręgów, wskazujących przyszłą lokalizację dział przeciwlotniczych.

[9] Źródło z MAEA potwierdziło, że to ta agencja zleciła wykonanie zdjęć.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Zdjęcia zostały wykonane w idealnym momencie, aby uchwycić irańskich pracowników kładących dachy podziemnych budowli z naprzemiennych warstw ziemi i cementu. Kilka tygodni później budynki byłyby zupełnie niewidoczne z góry i nie byłoby oczywistych śladów ich istnienia. Ktoś starannie zaplanował ujawnienie zakładu w Natanzie — w idealnym momencie, aby można było zarejestrować dowody.

Każdy z dwóch podziemnych budynków miał rozmiar sześciu boisk do futbolu i był solidnie wzmocniony betonowymi ścianami o grubości ok. 2 m. Irańczycy najwyraźniej zabezpieczali zakład przed ewentualnymi atakami z powietrza. Ponadto tunel prowadzący do budynków miał kształt litery U, a nie linii prostej. Jest to typowa strategia zapobiegająca trafieniu wystrzelonej w otwór tunelu rakiety w cel znajdujący się po jego drugiej stronie.

Hinderstein pokazała zdjęcia szefowi, Davidowi Albrightowi, fizykowi, byłemu inspektorowi ds. broni w Iraku i założycielowi ISIS. Wspólnie doszli do przekonania, że kompleks nie jest zakładem produkcji paliwa. Iran nie miał powodów, aby budować taki zakład pod ziemią, ponieważ bombardowanie go nie miało dużego sensu. Uznali więc, że jedynym logicznym wnioskiem, wyjaśniającym podziemne konstrukcje i plany zamontowania dział przeciwlotniczych, było to, iż natrafili na nieuchwytny zakład wzbogacania uranu, którego szukali.

W WIEDNIU DZIEŃ był spokojny, gdy informacje z konferencji prasowej Jafarzadeha trafiły do Ollego Heinonena w znajdującej się nad Dunajem siedzibie głównej MAEA. W sierpniu większość Europy wyjechała na wakacje. Wiedeń nie był pod tym względem wyjątkiem. Przełożony Heinonena, dr Muhammad el-Baradei, dyrektor naczelny MAEA, odpoczywał w Egipcie. Także wielu innych pracowników organizacji znajdowało się poza miastem. Dlatego Heinonen, Fin po pięćdziesiątce, w okularach z drucianą oprawką i chłopięcą burzą rudobrązowych włosów, był w biurze sam, gdy przeczytał wiadomość. Heinonen był szefem działu B w departamencie bezpieczeństwa MAEA, a trzy miesiące później miał dołączyć do grupy zajmującej się Iranem. Wcześniej przez kilka lat był głównym inspektorem agencji w Korei Północnej i innych częściach Azji. Obecne zmiany były dla niego powrotem na znane terytorium, ponieważ już wcześniej (w latach

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

1992 – 1995) zarządzał działaniami MAEA w Iranie. Perski dywan związany z tym okresem wciąż zdobił jego gabinet.

Heinonen był doświadczonym inspektorem nuklearnym. Dołączył do MAEA w 1983 r., przechodząc z fińskiego centrum badań nuklearnych. Dzięki dyplomowi doktora radiochemii z Uniwersytetu Helsińskiego posiadał większą wiedzę niż pierwsze generacje inspektorów MAEA, zwykle mających niewielkie podstawy naukowe. Heinonen miał też reputację człowieka o wyważonej pewności siebie i determinacji, potrafiącego jasno przekazać krajom, w których przeprowadza inspekcję, że nie będzie tolerował kłamstw.

Po zapoznaniu się z informacjami od Jafarzadeha był zaskoczony poziomem ich szczegółowości. Już od pewnego czasu czekał na tego rodzaju informacje. Podobnie jak jego odpowiednicy z ISIS od początku podejrzewał, że zakład w Natanzie nie ma produkować paliwa, tylko wzbogacać uran. Dwa lata wcześniej źródła rządowe poinformowały MAEA, że w latach 80. Iran próbował potajemnie zakupić w Europie części do produkcji wirówek do wzbogacania uranu[10]. Na tej podstawie Heinonen podejrzewał, że w Iranie ukryta jest nielegalna fabryka wirówek, jednak nie znał jej lokalizacji. MAEA nie mogła zażądać od Irańczyków ustosunkowania się do tych wiadomości, nie podając ich źródła. Organizacja wystrzegała się też podejmowania działań na podstawie danych ze źródeł rządowych, od czasu jak agencja wywiadowcza w 1992 r. poinformowała inspektorów o tym, że Iran potajemnie kupował zakazany sprzęt nuklearny. Wywiad nie podał jednak żadnych szczegółów. Gdy MAEA skonfrontowała Iran z tymi oskarżeniami, irańscy urzędnicy wszystkiemu zaprzeczyli i zaprosili inspektorów do wizyty w obiektach nuklearnych w celu ich sprawdzenia. Inspektorzy nie znaleźli żadnych dowodów potwierdzających oskarżenia i zawstydzeni opuścili Iran[11].

Tym razem sytuacja wyglądała inaczej. Informacje zostały ujawnione publiczne, dlatego Heinonen nie musiał ukrywać ich źródła. Dane obejmowały też precyzyjne i konkretne szczegóły włącznie z nazwami i lokalizacjami zakładów.

[10] David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*, Free Press, Nowy Jork 2010, s. 187.

[11] Z wywiadu autorki z Heinonenem z czerwca 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

To oznaczało, że MAEA mogła samodzielnie sprawdzić istnienie obiektów i zażądać od Iranu otwarcia ich w celu inspekcji[12].

Heinonen zadzwonił do swojego przebywającego w Egipcie przełożonego, a ten zgodził się, że agencja powinna natychmiast wysłać list do Alego Akbara Salehiego, irańskiego ambasadora przy MAEA, z żądaniem wyjaśnień na temat prac w Natanzie. Salehi był oburzony oskarżycielskim charakterem listu i stwierdził, że MAEA nie powinna zadawać pytań opartych na niezweryfikowanych twierdzeniach, zwłaszcza tych pochodzących od znanej grupy terrorystycznej. Gholam Reza Aghazadeh, wiceprezydent Iranu i głowa Agencji Energii Atomowej tego kraju, poinformował MAEA, że Iran nie ukrywał zakładu w Natanzie i planował ujawnić jego istnienie w późniejszym czasie[13]. Stwierdził, że jeśli MAEA zachowa cierpliwość, wkrótce wszystkiego się dowie. Na razie mógł powiedzieć tylko tyle, że Iran planuje w ciągu najbliższych 20 lat zbudować kilka elektrowni atomowych i potrzebuje paliwa jądrowego do ich działania. Nie wyjaśnił, czy w Natanzie powstaje zakład wzbogacania uranu potrzebny do produkcji takiego paliwa, ale można było to wywnioskować z jego słów.

MAEA naciskała Iran, aby natychmiast udostępnił obiekt w Natanzie inspektorom. Po krótkiej wymianie listów irańscy urzędnicy w końcu niechętnie zgodzili się na wpuszczenie inspektorów w październiku. Jednak gdy MAEA przygotowała się do kontroli, Iran anulował wizytę, stwierdzając, że data jest nieodpowiednia. Drugą wizytę zaplanowano na grudzień, jednak

[12] Dostępne są sprzeczne raporty na temat tego, o czym MAEA wówczas wiedziała. Według Marka Hibbsa, byłego czołowego dziennikarza ds. energii atomowej, obecnie analityka politycznego, mniej więcej dwa miesiące przed konferencją prasową grupy NCRI Stany Zjednoczone przekazały MAEA współrzędne podejrzanych obiektów w Iranie. Stany Zjednoczone śledziły te kompleksy przynajmniej od początku 2002 r. (Hibbs, *US Briefed Suppliers Group in October on Suspected Iranian Enrichment Plant*, „NuclearFuel", 23 grudnia 2001). Jednak David Albright z ISIS twierdzi, że choć amerykańskie źródła udostępniły MAEA współrzędne obiektów, nie wyjaśniły, że w Natanzie powstaje zakład wzbogacania uranu. Muhammad el-Baradei w swojej książce *The Age of Deception* przyznał, że w połowie 2002 r. MAEA otrzymała dane o kompleksie w Natanzie, nie wyjaśnia jednak, czy agencja wiedziała, że budowany jest tam zakład wzbogacania uranu.

[13] Urzędnicy irańscy utrzymywali później, że jedyną przyczyną prób ukrycia działań w Natanzie było to, iż Zachód próbował utrudniać Iranowi realizowanie cywilnego programu nuklearnego.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

także ona została odwołana. Heinonen podejrzewał, że Iran gra na zwłokę, aby zyskać czas na pozbycie się obciążających dowodów z Natanzu.

Gdy David Albright, założyciel MAEA, dowiedział się, że Iran blokuje kontrolę, zdecydował się przedstawić zdjęcia satelitarne mediom, aby wywrzeć na Irańczyków presję i skłonić ich do wpuszczenia inspektorów do Natanzu. Jedną rzeczą było podważanie przez Iran oskarżeń opozycjonistów mających polityczne motywy, czymś innym było zaś zareagowanie na jednoznaczne zdjęcia tajnych obiektów pokazane na całym świecie przez CNN. Tak więc 12 grudnia stacja CNN wyemitowała reportaż, w którym zostały zaprezentowane zdjęcia satelitarne udostępnione przez MAEA. Stwierdzono w nim, że Iran jest podejrzewany o budowanie w Natanzie tajnego zakładu wzbogacania uranu, który może posłużyć do produkcji materiału rozszczepialnego do broni nuklearnej. Irański ambasador przy ONZ-ecie zaprzeczył prowadzeniu przez Iran programu rozwoju broni nuklearnej i poinformował CNN, że „wszystkie posiadane przez was zdjęcia satelitarne jakichkolwiek obiektów" są związane z pokojowym programem pozyskiwania energii atomowej, a nie z budowaniem broni nuklearnej[14].

Zdjęcia przyniosły jednak oczekiwany efekt. Po emisji reportażu przez stację CNN irańscy urzędnicy zatwierdzili zaplanowaną na luty inspekcję.

CHOĆ OBIEKT W NATANZIE był nowy, Iran prowadził działalność jądrową już od ponad 40 lat. Zapoczątkowano ją w czasach reżimu poprzedniego szacha, Mohammada Rezy Pahlawiego, w okresie gdy Stany Zjednoczone i inne zachodnie państwa w pełni popierały nuklearne aspiracje Iranu.

Iran uruchomił publiczny i akceptowany program nuklearny w 1957 r., przeszło dekadę po tym, jak Stany Zjednoczone zdetonowały pierwsze bomby atomowe w Japonii. W owych czasach inne państwa starały się dołączyć do ekskluzywnego nuklearnego klubu założonego przez Amerykanów. Starając się skierować nuklearne ambicje tych krajów w inną stronę, administracja Dwighta Eisenhowera promowała program Atoms for Peace (czyli „atom dla pokoju"). Polegało to na tym, że inne państwa mogły otrzymać pomoc w rozwijaniu technologii nuklearnych, ale pod warunkiem że wykorzystają je tylko w celach pokojowych. W ramach tego programu Iran

[14] Transkrypcja tego materiału z CNN jest dostępna na stronie: *http://transcripts.cnn.com/TRANSCRIPTS/0212/13/lol.07.html*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

podpisał ze Stanami Zjednoczonymi porozumienie, na mocy którego Amerykanie pomogą zbudować na Uniwersytecie Teherańskim badawczy lekkowodny reaktor nuklearny. Stany Zjednoczone zobowiązały się też dostarczać wzbogacony uran do tego reaktora[15].

Jednak mimo wysiłków Amerykanów na rzecz ograniczenia rozwoju broni nuklearnej czterem innym krajom po wojnie udało się dołączyć do elitarnego klubu nuklearnego. Były to: Związek Radziecki, Wielka Brytania, Francja i Chiny. Aby ograniczyć ten niebezpieczny proces, w latach 60. podpisano Układ o nierozprzestrzenianiu broni jądrowej. Miał on zapobiegać produkcji broni jądrowej w kolejnych państwach i skutkować ograniczeniem arsenału w krajach, które już taką broń posiadały[16].

Układ dzielił świat na państwa posiadające broń jądrową i nieposiadające broni jądrowej. Te ostatnie miały otrzymywać pomoc w rozwijaniu cywilnych programów nuklearnych w zamian za rezygnację z budowy broni jądrowej i zgodę na regularne inspekcje MAEA, która sprawdzała, czy materiały i sprzęt przeznaczone dla programów cywilnych nie są wykorzystywane do produkcji broni. Problem z tym układem był taki, że wiele komponentów i obiektów dla programów cywilnych miało dwojakie zastosowanie i mogło posłużyć także do prac nad bronią. Dlatego trudno było kontrolować działania poszczególnych państw. Hannes Alfvén, szwedzki laureat Nagrody Nobla w dziedzinie fizyki, powiedział kiedyś: „Atom dla pokoju i atom dla wojny to bliźnięta syjamskie".

Iran był jednym z pierwszych sygnatariuszy układu. Podpisał go w 1968 r., a w 1974 założył własną Agencję Energii Atomowej i opracował wielki plan budowy 20 reaktorów nuklearnych ze wsparciem Niemiec, Stanów Zjednoczonych i Francji. Wszystkie te państwa liczyły na zyski ze sprzedaży sprzętu reżimowi szacha. Pierwsze dwa reaktory miały powstać w Buszehrze.

---

[15] Digital National Security Archive, „US Supplied Nuclear Material to Iran", 29 stycznia 1980. Te materiały są dostępne na stronie: *http://nsarchive.chadwyck.com* (wymagana jest rejestracja). Zob. też Dieter Bednarz, Erich Follath, *The Threat Next Door: A Visit to Ahmadinejad's Nuclear Laboratory*, „Spiegel Online", 24 czerwca 2011. Ten tekst jest dostępny pod adresem: *http://www.spiegel.de/international/world/the-threat-next-door-a-visit-to-ahmadinejad-s-nuclear-laboratory-a-770272.html*.

[16] Anne Hessing Cahn, „Determinants of the Nuclear Option: The Case of Iran", [w:] *Nuclear Proliferation in the Near-Nuclear Countries*, red. Onkar Marway, Ann Shulz, Ballinger Publishing Co., Cambridge 1975, s. 186.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 1975 r. niemieccy inżynierowie z Kraftwerk Union, jednostki zależnej Siemensa, rozpoczęli realizację projektu budowlanego, który miał kosztować 4,3 mld dolarów. Zakończenie prac planowano na 1981 r.[17].

W tym czasie pojawiły się obawy o to, że celem Iranu może być budowa broni jądrowej. Sam szach zasugerował, że nuklearne plany Iranu nie są czysto pokojowe. W wywiadzie stwierdził, że Iran „bez wątpliwości […] i to szybciej niż ktokolwiek podejrzewa" może zdobyć broń jądrową, jeśli sytuacja na Bliskim Wschodzie będzie tego wymagać[18]. Jednak przywódcy amerykańscy nie widzieli w tym powodu do niepokoju, ponieważ uważali szacha za sojusznika i nie potrafili sobie wyobrazić, że pewnego dnia on lub jego reżim utracą władzę[19].

Ten dzień szybko nadszedł, gdy w 1979 r. wybuchła rewolucja islamska. W tym czasie kończono właśnie jeden z budynków reaktora w Buszehrze. Rewolucjoniści, którzy obalili szacha i przejęli władzę pod przywództwem ajatollaha Ruhollaha Chomejniego, postrzegali olbrzymie reaktory budowane w Buszehrze jako symbol sojuszu szacha z Zachodem. Stany Zjednoczone, zaalarmowane niestabilną sytuacją polityczną, wycofały wsparcie projektu, a niemiecki rząd wymusił na firmie Kraftwerk Union wycofanie się z kontraktu w Buszehrze[20].

Późniejsza wojna Iranu z Irakiem nie oszczędzała porzuconych reaktorów. W ciągu ośmiu lat walk (1980 – 1988) Irak wielokrotnie bombardował dwie wieże budowli. Pozostały z nich ruiny[21]. W trakcie wojny dowódca

[17] Ali Vaez, *Waiting for Bushehr*, „Foreign Policy", 11 września 2011.

[18] John K. Cooley, *More Fingers on Nuclear Trigger?*, „Christian Science Monitor", 25 czerwca 1974. Później urzędnicy irańscy zaprzeczali, że szach powiedział coś takiego.

[19] Iran omawiał z Izraelem możliwość zaadaptowania rakiet ziemia – ziemia do głowic jądrowych. Zob. Paul Michaud, *Iran Opted for N-bomb Under Shah: Ex-Official*, „Dawn", 23 września 2003. Ponadto Akbar Etemad, szef irańskiej Agencji Energii Atomowej, stwierdził, że powierzono mu zadanie utworzenia specjalnego zespołu do śledzenia najnowszych badań nuklearnych, aby Iran był gotowy do zbudowania bomby, jeśli i kiedy będzie to konieczne. Etemad ujawnił te informacje w wywiadzie udzielonym „Le Figaro" w 2003 r. Zob. Elaine Sciolino, *The World's Nuclear Ambitions Aren't New for Iran*, „New York Times", 22 czerwca 2003.

[20] John Geddes, *German Concern Ends a Contract*, „New York Times", 3 sierpnia 1979. Zob. też Judith Perera, *Nuclear Plants Take Root in the Desert*, „New Scientist", 23 sierpnia 1979.

[21] Vaez, *Waiting for Bushehr*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

gwardii rewolucyjnej nakłaniał ajatollaha Chomejniego do realizacji programu rozwoju broni jądrowej, co miało pozwolić odeprzeć Irakijczyków i ich zachodnich sprzymierzeńców. Jednak Chomejni odmówił. Uważał, że broń jądrowa jest sprzeczna z islamem i narusza podstawowe moralne zasady tej religii. Najwyraźniej jednak zmienił zdanie, gdy Saddam Hussajn użył broni chemicznej przeciw irańskim żołnierzom i cywilom, zabijając ok. 25 tys. osób i raniąc ponad 100 tys. kolejnych. Zirytowany biernością ONZ-etu i zaalarmowany pogłoskami, że Irak sam planuje zbudować broń jądrową, Chomejni zdecydował się wznowić irański program jądrowy. W jego ramach miał być realizowany program wzbogacania uranu[22].

Aby rozpocząć prace nad programem, Iran zwrócił się o pomoc do pakistańskiego metalurga Abdula Qadeera Khana. Khan był bardzo ważną postacią w pakistańskim programie budowy broni jądrowej w połowie lat 70. Wykorzystał w nim technologię wirówek, którą wykradł z Europy. Pracował dla duńskiej firmy, która prowadziła badania nad wirówkami dla konsorcjum Urenco. Konsorcjum zostało założone przez Niemców, Brytyjczyków i Holendrów na potrzeby budowy wirówek dla europejskich elektrowni atomowych. W swojej pracy Khan miał dostęp do poufnych projektów wirówek, które skopiował i przewiózł do Pakistanu. Zdobył też listy dostawców. Wielu z nich było otwartych na potajemną sprzedaż Pakistanowi części i materiałów potrzebnych do produkcji wirówek.

Wirówki to metalowe cylindry z wewnętrznymi wirnikami, które mogą obracać się ponad 100 tys. razy na minutę. Służą do wzbogacania sześciofluorku uranu produkowanego z rud uranu znajdujących się w ziemi i z wody morskiej. Sześciofluorek uranu jest tłoczony do kaskad wirówek — grup wirówek połączonych rurkami i zaworami. W trakcie obracania się wirników siła odśrodkowa oddziela nieco lżejsze izotopy ^{235}U (są to rozszczepialne izotopy potrzebne do uzyskania energii atomowej) od cięższych izotopów ^{238}U. Proces ten przypomina przesiewanie piasku w poszukiwaniu złota[23]. Gaz zawierający cięższe izotopy przepływa bliżej zewnętrznych ścianek,

[22] Institute for Science and International Security, „Excerpts from Internal IAEA Document on Alleged Iranian Nuclear Weaponization", 2 października 2009. Ten raport organizacji ISIS jest oparty na wewnętrznym dokumencie MAEA zatytułowanym *Possible Military Dimensions of Iran's Nuclear Program* (*http://isisnucleariran.org/assets/pdf/IAEA_info_3October2009.pdf*).

[23] Izotop ^{235}U ma o 3 neutrony mniej niż izotop ^{238}U, przez co jest lżejszy.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

natomiast gaz z lżejszymi izotopami znajduje się bliżej środka. Wirówki są otoczone spiralnymi rurkami wypełnionymi gorącą wodą. To sprawia, że w wirówce powstaje różnica temperatur, wprawiająca gaz w ruch pionowy wzdłuż ścianek wirówki. Pozwala to na lepsze rozdzielenie izotopów. Czerpaki przenoszą gaz z lżejszymi izotopami do wirówek na wyższych poziomach kaskady, gdzie następuje dalsza separacja izotopów. Cięższy gaz, zubożony uran, jest przenoszony do drugiego zbioru wirówek na niższych poziomach kaskady, gdzie też jest dalej rozdzielany. Po wyodrębnieniu z tego gazu dodatkowych izotopów ^{235}U są one łączone z resztą gazu tego rodzaju, natomiast zubożony uran trafia do „kosza", na koniec kaskady, gdzie jest usuwany. Proces ten jest powtarzany do momentu uzyskania gazu zawierającego docelowe stężenie izotopów ^{235}U[24].

W 1987 r., gdy Iran wznowił program nuklearny, irańscy urzędnicy skontaktowali się z niemieckim inżynierem, który zaczął działać na czarnym rynku. Ten inżynier był głównym dostawcą sprzętu do nielegalnego pakistańskiego programu jądrowego i pomógł zorganizować w Dubaju tajne spotkanie między przedstawicielami Iranu a innymi dostawcami Khana. Za 10 mln dolarów Irańczycy otrzymali dwie duże walizy i dwie teczki pełne materiałów potrzebnych do uruchomienia programu wzbogacania uranu. Materiały obejmowały techniczne projekty wirówek, kilka rozłożonych na części prototypów tych urządzeń i plany małego zakładu z wirówkami obejmującego sześć kaskad[25]. Jako bonus handlarze dorzucili 15-stronicowy dokument opisujący, jak przekształcić wzbogacony uran w uran metaliczny i jak przetopić go w półkule — podstawowy komponent bomb jądrowych[26].

---

[24] Charles D. Ferguson, *Nuclear Energy: What Everyone Needs to Know*, Oxford University Press, Nowy Jork 2011.

[25] Dennis Frantz, Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets*, Free Press, Nowy Jork 2007, s. 156. Materiały te były wymienione w odręcznie napisanym dokumencie otrzymanym przez MAEA. Został on opisany w raporcie Rady Gubernatorów MAEA „Director General, Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran, GOV/2005/67", 2 września 2005, s. 5.

[26] Według Rady Gubernatorów MAEA w listopadzie 2007 r. Iran przekazał agencji kopie tego 15-stronicowego dokumentu, co opisano w raporcie „Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions 1737 (2006) and 1747 (2007) in the Islamic Republic of Iran", 22 lutego 2008, s. 4. Iran stwierdził, że nie prosił o ten dokument, tylko otrzymał go z inicjatywy handlarzy z czarnego rynku.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Później Khan w pakistańskiej telewizji wyjaśnił, że pomagał Iranowi w programie nuklearnym, ponieważ uważał, że jeśli Pakistan i Iran staną się potęgami nuklearnymi, „zneutralizuje to siłę Izraela" w regionie[27].

Rozłożone wirówki otrzymane przez Irańczyków były zbudowane na podstawie jednego z projektów skradzionych przez Khana z Urenco. W Pakistanie te wirówki nazywano P-1, jednak w Iranie ich nazwa to IR-1. Początkowo Iranowi brakowało pieniędzy, aby cokolwiek zrobić z otrzymanymi planami. Jednak w 1988 r., po zakończeniu wojny irańsko-irackiej i pojawieniu się wolnych środków, kraj zaczął inwestować w program wzbogacania uranu. Zakupił wysoko wytrzymałe aluminium i inne materiały potrzebne do budowy własnych wirówek. Ponadto potajemnie zaimportował z Chin prawie 2 t naturalnego uranu, w tym sześciofluorek uranu[28].

Później Khan w sekrecie udostępnił Iranowi komponenty do budowy 500 wirówek P-1 oraz instrukcje dotyczące zapewniania jakości w procesie produkcji i testowania wirówek. Te instrukcje były bardzo potrzebne, ponieważ Iran miał problemy z wirówkami zbudowanymi na bazie pakistańskich prototypów. Czasem urządzenia zaczynały wirować w niekontrolowany sposób i psuły się. W innych przypadkach w ogóle nie działały[29]. Do 1994 r. Iranowi udało się z powodzeniem uruchomić tylko jedną wirówkę pracującą „z prawie pełną prędkością"[30].

W efekcie Irańczycy oskarżyli Khana o sprzedaż złomu. W 1996 r. Khan przekazał Irańczykom plany pakistańskich wirówek P-2, bardziej zaawansowanego urządzenia opartego na innym skradzionym projekcie z Urenco[31].

---

[27] Erich Follath, Holger Stark, *The Birth of a Bomb: A History of Iran's Nuclear Ambitions*, „Der Spiegel", 17 czerwca 2010.

[28] Raport Rady Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", 10 listopada 2003, s. 5.

[29] W 1992 r. Masud Naraghi, były szef irańskiej Agencji Energii Atomowej, opuścił Iran i przekazał CIA informacje na temat irańskiego programu. W 1987 r. uczestniczył w negocjacjach transakcji między Iranem a A.Q. Khanem, które doprowadziły do uzyskania pierwszych wirówek dla irańskiego programu wzbogacania uranu. Naraghi poinformował CIA m.in. o problemach irańskich naukowców z wirówkami IR-1, które próbowali zbudować na podstawie projektów otrzymanych od Khana. Zob. Frantz, Collins, *Nuclear Jihadist*, s. 202, oraz Albright, *Peddling Peril*, s. 76 – 81.

[30] Frantz, Collins, *Nuclear Jihadist*, s. 213.

[31] Raport Rady Gubernatorów MAEA, „Director General, Implementation of the NPT Safeguards Agreement", 2 września 2005, s. 5.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wirówki P-2 były znacznie wydajniejsze niż IR-1 i potrafiły w tym samym czasie wzbogacić dwa i pół raza więcej uranu. Wykorzystywały wirnik ze stali maraging — materiału odporniejszego niż podatne na pęknięcia aluminium z urządzeń IR-1.

Iran, w sekrecie pracując nad wzbogacaniem uranu, równolegle prowadził publiczny program nuklearny. W 1995 r. Irańczycy podpisali wart 800 mln dolarów kontrakt z Rosją na wznowienie budowy reaktora w Buszehrze. Państwa te prowadziły też rozmowy na temat budowy zakładu wzbogacania uranu na potrzeby produkcji paliwa dla reaktora, jednak administracja Billa Clintona zaczęła interweniować i przekonała Rosjan do wycofania się z tych planów. Iran budował więc tajny zakład wzbogacania uranu samodzielnie[32].

Mniej więcej w tym czasie Europa zaczęła wzmacniać kontrolę nad eksportem sprzętu i komponentów o podwójnym zastosowaniu. To jednak nie zniechęciło Iranu, tylko zmusiło do dokładniejszego zamaskowania tajnego programu. Aby chronić zakłady badawcze i produkcyjne przed wykryciem, urzędnicy zaczęli rozdzielać zadania między różne placówki rozproszone po kraju. Niektóre z nich znajdowały się na chronionych terenach wojskowych, inne były ukryte w niepozornych biurach i magazynach. W ramach tych zmian produkcję wirówek przeniesiono z teherańskiego Centrum Badań Nuklearnych, gdzie program został zapoczątkowany, do znajdujących się w przemysłowej części Teheranu fabryk, należących wcześniej do Kalaye Electric Company, dawnego producenta zegarków, zakupionego przez Agencję Energii Atomowej jako firma przykrywka. O tej samej firmie Jafarzadeh wspomniał w trakcie konferencji prasowej w 2002 r.

[32] Uważa się, że projekty osobnego zakładu przetwarzania uranu w Isfahanie, służącego do przekształcania oczyszczonej rudy uranu w gaz, mogły pochodzić z Chin. W 1997 r. administracja Clintona ogłosiła, że zablokowała transakcję sprzedaży przez Chińczyków zakładu przetwarzania uranu Iranowi. Irańczycy otrzymali jednak od Chińczyków projekty takiego obiektu. Zob. John Pomfret, *U.S. May Certify China on Curbing Nuclear Exports*, „Washington Post", 18 września 1997.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Mniej więcej w 1999 r. Iran przeprowadził pierwsze udane testy wzbogacania uranu w fabryce firmy Kalaye. Zastosowano w nich małe kaskady wirówek i sześciofluorek uranu zakupiony od Chin[33]. Był to wielki przełom, który udowodnił wykonalność programu prowadzonego już od dziesięciu lat. W tym momencie urzędnicy z irańskiej Agencji Energii Atomowej zdecydowali się zwiększyć zakres prac i nakazali produkcję 10 tys. wirówek dla zakładu wzbogacania uranu, który planowali postawić w Natanzie. W tym samym czasie zaczęli intensywnie pracować nad zamówieniami, aby pozyskać części i materiały w Europie oraz z innych źródeł[34]. Mniej więcej w 2000 r. robotnicy rozpoczęli prace nad kompleksem w Natanzie, a Iran znalazł się na drodze do zbudowania broni jądrowej.

[33] Iran przez lata ujawniał fragment po fragmencie szczegóły historii swojego programu nuklearnego. Począwszy od 2004 r., MAEA zamieszczała te dane w raportach. Jednak informacje od Iranu nie zawsze były zgodne z informacjami uzyskanymi przez MAEA i dziennikarzy z innych źródeł.

[34] Albright, *Peddling Peril*, s. 185.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 4

DEKONSTRUKCJA STUXNETA

W pierwszych dniach po pojawieniu się informacji o Stuxnecie nad wstępną analizą kodu pracował prawie tuzin badaczy z Symanteca znajdujących się na trzech kontynentach. Bardzo szybko pozostali tylko Chien, O'Murchu i Falliere. Inni analitycy zajęli się nowymi zagrożeniami. Prawie tydzień po ujawnieniu Stuxneta wspomniana trójka wciąż zmagała się z samym „pociskiem" zastosowanym w ataku i nie zaczęła nawet analizować ładunku.

Większość broni cyfrowej, podobnie jak konwencjonalnej, składa się z dwóch części: „pocisku" (ang. *missile*; jest to system przenoszenia), odpowiedzialnego za rozprzestrzenianie szkodliwego ładunku i instalowanie go na komputerach, oraz samego ładunku, przeprowadzającego atak — np. wykradającego dane lub wykonującego inne operacje na zainfekowanych maszynach. W omawianej sytuacji ładunkiem był szkodliwy kod, który miał na celu zakłócenie oprogramowania i pracy sterowników PLC Siemensa.

Ponieważ rozpracowanie Stuxneta wciąż wymagało bardzo dużo pracy, Chien musiał przekonać menedżerów, że razem z zespołem powinien kontynuować analizowanie kodu, choć nie był on już informacją dnia. Co środę odbywał wideokonferencję z firmowymi menedżerami ds. zagrożeń z całego świata, aby omówić wszystkie ważne infekcje, które w danym momencie badali, i porozmawiać na temat strategii prac. W pierwszą środę po ujawnieniu Stuxneta ten zagadkowy atak znalazł się na czele listy tematów.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Biura Symanteca w Culver City to przestronny budynek w obejmującym ponad 3,5 ha kompleksie biznesowym, w którym rosną palmy i pustynne krzewy. Ta nowoczesna pięciopiętrowa budowla znacznie różniła się od zatłoczonego biura z epoki komunizmu zajmowanego przez firmę VirusBlokAda. Znajdowały się w niej obszerne atrium z wysokim sufitem i podłogi z dużych cementowych płyt, które wydawały odgłos podobny do pustego szkła z powodu położonych pod nimi tuneli mieszczących systemy zasilania i wentylacji. Kompleks Symanteca uzyskał certyfikat LEED Gold dzięki przyjaznej środowisku architekturze z dachem odbijającym bezlitosne południowokalifornijskie słońce. Szklana fasada zapewniała wszystkim pracownikom widok — przynajmniej na to, co działo się w nieciekawym otoczeniu centrów handlowych i autostrady w pobliżu lotniska w Los Angeles.

Sala do wideokonferencji była niewielkim, pozbawionym okien pomieszczeniem zlokalizowanym w zapomnianym obszarze na trzecim piętrze, gdzie można było dotrzeć okrężną drogą przez laboratorium do badania szkodliwego oprogramowania. W tej sali znajdowały się trzy duże ekrany zamontowane na ścianie na poziomie oczu przed rzędem stołów. Sprawiało to wrażenie, że wirtualni rozmówcy siedzą bezpośrednio naprzeciwko Chiena.

Chien przedstawił menedżerom podsumowanie pierwszych odkryć O'Murchu. Zwrócił uwagę na niespotykanie dużą objętość kodu, zaawansowaną technikę ładowania i ukrywania plików oraz tajemniczy ładunek, dla którego celem wydawały się być wyłącznie sterowniki PLC Siemensa. Poinformował też o dziwnym wzorcu lokalizacji, z jakich do ujścia Symanteca napływały dane z zainfekowanych maszyn. Nie wspomniał jednak o możliwych politycznych skutkach ataku.

„Chcemy, aby Nico zajął się tylko tą sprawą — powiedział, mając na myśli Falliere'a, analityka z Francji. — Ponadto uważam, że Liam i ja też powinniśmy kontynuować prace nad tym problemem". Był jednak pewien haczyk. Chien nie wiedział, ile czasu zajmie im dokończenie analizy kodu.

Zespoły badaczy analizowały zwykle ok. 20 szkodliwych plików dziennie. Dlatego przypisanie trzech czołowych analityków na nieokreślony czas do jednego zagrożenia nie miało żadnego sensu biznesowego. Podobna sytuacja zdarzyła się wcześniej tylko raz, gdy w 2008 r. pojawił się robak Conficker. Jednak był to zmieniający kształty robak, który zainfekował

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

miliony maszyn na całym świecie i do tej pory jest zagadką. Nie wiadomo np., po co w ogóle został utworzony[1]. Natomiast Stuxnet zainfekował znacznie mniej komputerów, a celem jego ataku był jeszcze mniejszy podzbiór maszyn ze sterownikami PLC Siemensa. Jednak coś w tym tajemniczym kodzie aż prosiło się o dalsze analizy, a menedżerowie Chiena zgodzili się, że nie należy jeszcze rezygnować z prac. „Ale informujcie nas o tym, co znajdziecie" — powiedzieli, nie wiedząc jeszcze, że ich cotygodniowe spotkania na wiele miesięcy zostaną zdominowane przez rozmowy dotyczące Stuxneta.

Chien ze współpracownikami wykorzystali możliwość zajęcia się kodem i potraktowali to zadanie jak osobistą obsesję. Wkrótce po rozpoczęciu prac zrozumieli, że wkraczają na nieznane terytorium, w którym będą zdani głównie na własne siły.

[1] Choć Conficker rozprzestrzeniał się bardzo szybko i skutecznie, na większości zainfekowanych maszyn nie podejmował żadnych działań. Dlatego motywy jego utworzenia i uruchomienia pozostały tajemnicą. Zdaniem niektórych napastnicy chcieli utworzyć z zainfekowanych maszyn ogromną sieć botów, aby rozsyłać spam lub przeprowadzać ataki DoS na witryny. Późniejsza odmiana Confickera miała straszyć użytkowników, tak aby pobrali szkodliwy program antywirusowy. Inne osoby obawiały się, że Conficker może instalować w zainfekowanych systemach „bombę logiczną", która w przyszłości spowoduje destrukcję danych. Jednak gdy żaden z tych scenariuszy się nie ziścił, niektórzy uznali, że Conficker został wypuszczony w celu przetestowania, jak zareagują na niego rządy i branża zabezpieczeń. Kod wykorzystywany w ataku był kilkakrotnie modyfikowany. Napastnicy zastosowali w nim zaawansowane metody, aby stale wyprzedzać badaczy o kilka kroków i uniemożliwiać im całkowite pozbycie się tego robaka. Zdaniem części osób świadczyło to o tym, że napastnicy testowali zabezpieczenia. Po wykryciu Stuxneta John Bumgarner, dyrektor techniczny w U.S. Cyber Consequences Unit, firmie konsultingowej pracującej głównie dla klientów rządowych, stwierdził, że autorami Confickera i Stuxneta są ci sami napastnicy, a Conficker był „zasłoną dymną" i „taranem", przez co pozwolił umieścić Stuxneta na maszynach w Iranie. Jako dowód wskazał czas obu ataków i to, że w Stuxnecie została wykorzystana jedna z luk, dzięki której rozprzestrzeniał się też Conficker. Jednak badacze z Symanteca i innych firm, którzy przeanalizowali oba ataki, stwierdzili, że nie znaleźli niczego na poparcie słów Bumgarnera. Co więcej, pierwsza wersja Confickera nie infekowała maszyn na Ukrainie, co wskazuje na to, że atak mógł mieć źródło w tym kraju.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

SYMANTEC JEST DUŻĄ międzynarodową firmą, jednak Chien i O'Murchu pracowali w niewielkim oddziale i zmagali się z problemem z niewielką pomocą z zewnątrz. Ich siedzibą było laboratorium analizy zagrożeń w Culver City. To cybernetyczny odpowiednik laboratorium obrony przed atakami biologicznymi. Badacze mogli tu uruchomić złośliwy kod w czerwonej sieci — odizolowanym systemie bez połączenia z siecią biznesową Symanteca — aby obserwować przebieg szkodliwych operacji w kontrolowanym środowisku. By dotrzeć do tego zlokalizowanego na parterze laboratorium, pracownicy musieli przejść przez kilka zabezpieczonych drzwi. Przejście przez każde kolejne z nich wymagało spełnienia coraz bardziej restrykcyjnych warunków. Przez ostatnie drzwi mogła przejść tylko niewielka grupa osób. Za nimi znajdowała się czerwona sieć fizycznie odizolowana od komputerów podłączonych na zewnątrz do internetu. Obowiązywał też zakaz używania przenośnych nośników pamięci. Niedozwolone były płyty DVD i CD oraz pendrive'y. Miało to zapobiegać bezmyślnemu włożeniu nośnika do jednej z zainfekowanych maszyn i przypadkowemu wyjściu z laboratorium z zapisanym szkodliwym kodem.

Określenie „laboratorium analizy zagrożeń" przywodzi na myśl sterylną pracownię z naukowcami w białych kitlach pochylonymi nad mikroskopami i szalkami Petriego. Jednak laboratorium Symanteca było nijakim biurem zapełnionym głównie pustymi boksami. Pracowała w nim grupka osób, które przez cały dzień intensywnie wpatrywały się w monitory, przeważnie nic nie mówiąc, oraz metodycznie wykonywały najwyraźniej żmudną pracę. Nie było tu zdjęć na ścianach, plastikowych karabinów lub innych biurowych gier, w które pracownicy czasem grali, aby rozładować stres. Nie było też roślin, sztucznych lub naturalnych, które nadawałyby temu miejscu domowy charakter. Jedyną zieleń zapewniała szklana ściana wychodząca na trawiaste, pokryte drzewami wzgórze z rodzaju tych, jakie tworzone są w parkach biznesowych w celu zasymulowania natury na potrzeby zamkniętych w biurach pracowników.

Boks O'Murchu był niemal pozbawiony indywidualnego charakteru. Jedynym wyjątkiem było panoramiczne zdjęcie Wielkiego Kanionu skąpanego w różowych i purpurowych odcieniach typowych dla zachodu słońca. To zdjęcie było pamiątką z wycieczki, na jaką O'Murchu rok wcześniej wybrał się ze swoim ojcem. Badacz trzymał na biurku dwa używane do analiz komputery podłączone do czerwonej sieci. Trzeci, przeznaczony do

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

czytania e-maili i surfowania po internecie, składał się tylko z urządzeń peryferyjnych (klawiatury, monitora i myszy) połączonych za pomocą wijących się kabli z dyskiem twardym ukrytym poza laboratorium w szafce serwerowej, bezpiecznie odizolowanej od wrogich sieci.

Boks Chiena, połączony ścianką z miejscem pracy O'Murchu, był tylko trochę bardziej osobisty. Znajdował się tam dziwny zestaw artystycznych pocztówek i flag pirackich, a na lakierowanych drzwiach widniał napis „CHIEN LUNATIQUE", który był grą słowną opartą na nazwisku badacza. W swobodnym tłumaczeniu z francuskiego oznaczało to: „Ostrożnie, pies", jednak Chien wolał bardziej dosłowny przekład: „Wściekły Pies".

Chien miał 39 lat, jednak wyglądał o 10 lat młodziej. Był wysoki, szczupły, nosił druciane okulary i miał szeroki ujmujący uśmiech z dołeczkami, które stawały się wyraźne, gdy badacz się śmiał. Kiedy był podekscytowany tematem dyskusji, mówił bardzo szybko i w przerywany sposób. Chien miał za sobą długą i udaną karierę w branży zabezpieczeń, jednak w tej wysoce konkurencyjnej dziedzinie, w której profesjonaliści często chwalili się swoimi umiejętnościami i doświadczeniem, aby wyróżnić się na tle innych, zachowywał się inaczej niż pozostali. Był skromny i powściągliwy. Wolał skupiać się na analizach niż na budowaniu wizerunku.

Spośród trzech badaczy zajmujących się Stuxnetem Chien pracował w Symantecu najdłużej. Był to jego pierwszy pracodawca po ukończeniu studiów, a Chien trafił do tej firmy zupełnie przypadkowo. Na początku lat 90. studiował na UCLA genetykę, biologię molekularną i inżynierię elektryczną. Podobnie jak O'Murchu był na dobrej drodze do kariery w dziedzinie nauk ścisłych. Po otrzymaniu w 1996 r. dyplomu zatrudnił się wraz z kilkoma znajomymi w Symantecu, zamierzając pozostać tam tylko kilka lat i zarobić pieniądze na studia doktoranckie. Nigdy jednak nie odszedł z tej firmy.

Cyberbezpieczeństwo wciąż należało wtedy do raczkujących dziedzin i łatwo było w nim o pracę bez wykształcenia lub doświadczenia. Chien nic nie wiedział wówczas o wirusach, jednak nauczył się Asemblera x86, języka programowania, w którym pisana jest większość złośliwego oprogramowania. To wystarczyło. Zresztą i tak najlepszymi analitykami nie byli inżynierowie komputerowi. Inżynierowie budowali rzeczy, natomiast pogromcy wirusów rozbierali je na części. Nawet gdy zabezpieczenia komputerów zaczęto traktować jako uznaną profesję z kursami i certyfikatami, Chien

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

faworyzował kandydatów bez doświadczenia, ale z niezaspokojoną ciekawością i intensywnym pragnieniem rozwiązywania zagadek oraz rozkładania rzeczy na części. Łatwo było nauczyć kogoś pisania sygnatur wirusów, jednak nauczenie kogoś ciekawości lub wzbudzenie pasji do dowiadywania się, jak coś działa, było niemożliwe. Najlepsi badacze mieli obsesyjne skłonności, sprawiające, że analizowali fragment kodu do momentu rozgryzienia tajemnicy.

Gdy Chien dołączył do Symanteca, badacze wirusów przypominali mechanika ze znanych w Stanach Zjednoczonych reklam firmy Maytag i często nie mieli nic do roboty. Wirusy pojawiały się rzadko i rozprzestrzeniały powoli za pośrednictwem dyskietek i „sieci trampkowej", przenoszone ręcznie z jednego komputera na drugi. Klienci uważający, że ich sprzęt został zainfekowany wirusem, przesyłali tradycyjną pocztą podejrzane pliki na dyskietkach do Symanteca. Takie dyskietki mogły tygodniami leżeć na biurkach, do czasu aż Chien lub jeden z jego współpracowników podszedł i je zabrał. Zwykle pliki okazywały się nieszkodliwe, ale czasem badacze znajdowali złośliwy kod. Wtedy pisali sygnatury potrzebne do wykrywania go, umieszczali je na innej dyskietce i przesyłali ją pocztą z powrotem do klienta wraz z instrukcjami aktualizacji skanera wirusów.

Jednak szybko nastąpiła ewolucja złośliwego oprogramowania i sytuacja się zmieniła. Wprowadzenie systemu Microsoft Windows 98 i pakietu Office w połączeniu z rosnącą popularnością internetu i e-maili spowodowało pojawienie się szybko rozpowszechniających się wirusów i robaków, które potrafiły w ciągu minut zaatakować miliony komputerów. Jednym z najbardziej znanych był wirus Melissa z 1999 r.[2]. Wypuszczony przez

[2] Wirus Melissa nie był pierwszym tak skutecznym atakiem. Ten zaszczyt należy się robakowi Morrisa, samopowielającemu się programowi utworzonemu przez 23-letniego doktoranta nauk komputerowych, Roberta Morrisa Jr., syna specjalisty od zabezpieczeń komputerowych z NSA. Choć wiele technik w Stuxnecie było nowoczesnych i wyjątkowych, ich korzenie sięgają robaka Morrisa i mają z nim pewne cechy wspólne. Morris wypuścił swojego robaka w 1988 r. w sieci ARPANET. Była to sieć komunikacyjna zbudowana przez agencję ARPA (ang. *Advanced Research Projects Agency*) Departamentu Obrony Stanów Zjednoczonych pod koniec lat 60. Sieć ta była prekursorem internetu. Robak Morrisa, podobnie jak Stuxnet, starał się ukryć za pomocą różnych technik. Między innymi umieszczał pliki w pamięci i usuwał swoje fragmenty, gdy nie były już potrzebne, co pozwalało zmniejszyć ilość zasobów zużywanych w maszynie. Jednak ten robak (znów podobnie jak Stuxnet) miał kilka wad, co spowodowało

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Davida Smitha, 31-letniego programistę z New Jersey, znajdował się w dokumencie Worda zamieszczonym przez Smitha na grupie dyskusyjnej alt.sex.usenet. Smith dobrze znał swoją grupę docelową. Zachęcił użytkowników do otwarcia pliku, twierdząc, że znajdują się w nim nazwy i hasła pozwalające na dostęp do witryn pornograficznych. Po otwarciu pliku wirus Melissa wykorzystywał lukę w funkcji makro w Wordzie i rozsyłał się e-mailem do pierwszych 50 kontaktów z książki adresowej programu Outlook klienta. W ciągu trzech dni ten pierwszy na świecie rozprzestrzeniający się masowo za pomocą e-maili wirus trafił na ponad 100 tys. maszyn. Wówczas był to spektakularny rekord, wypadający jednak blado według dzisiejszych standardów. Oprócz rozprzestrzeniania się za pomocą Outlooka wirus dodawał do dokumentów na zainfekowanych komputerach głupkowaty tekst nawiązujący do gry scrabble: „dwadzieścia dwa plus słowo razy trzy plus pięćdziesiąt punktów za wykorzystanie wszystkich liter. Gra skończona. Spadam". Wirus Melissa był stosunkowo niegroźny, jednak otworzył drogę innym szybko rozpowszechniającym się wirusom i robakom, które na lata zdominowały nagłówki prasowe[3].

Wraz z rozwojem skali zagrożeń Symantec zdał sobie sprawę, że musi szybciej powstrzymywać infekcje, jeszcze zanim wirusy zaczną się rozprzestrzeniać. Gdy firma zaczęła działalność w branży antywirusowej, za dobry czas rozwiązania problemu (od wykrycia wirusa do momentu dostarczenia sygnatur) uznawano okres tygodnia. Jednak celem firmy było skrócenie tego

niekontrolowane rozprzestrzenienie się go na 60 tys. maszyn i wykrycie. Gdy robak natrafiał na już zainfekowany komputer, powinien wstrzymać infekcję i szukać dalej. Jednak Morris obawiał się, że administratorzy wyeliminują robaka, programując komputery w taki sposób, by informowały o tym, że są zainfekowane, nawet jeśli było to nieprawdą. Dlatego robak i tak infekował co siódmą napotkaną maszynę. Morris nie uwzględnił jednak sieci wzajemnych połączeń w ARPANECIE. Robak wielokrotnie docierał więc do tych samych maszyn i niektóre z nich ponownie infekował setki razy, aż przestawały działać z powodu wielu jednocześnie uruchomionych na nich kopii robaka. Na przykład maszyny University of Pennsylvania zostały zaatakowane 210 razy w 12 godz. Zamknięcie lub restart komputera pozwalały usunąć robaka, ale tylko tymczasowo. Dopóki maszyna była podłączona do sieci, zostawała ponownie zainfekowana przez inne komputery.

[3] Samoreplikujące się robaki (Conficker i Stuxnet są tu wyjątkami) zdarzają się znacznie rzadziej niż w przeszłości. Dużo popularniejszą techniką jest obecnie phishing, polegający na tym, że złośliwe oprogramowanie jest przesyłane za pomocą załączników do e-maili lub zamieszczonych w e-mailach odnośników do szkodliwych witryn.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

czasu do mniej niż dnia. Aby to osiągnąć, firma potrzebowała analityków w wielu strefach czasowych, by wykrywali aktywne wirusy od razu, gdy się pojawią, i udostępniali sygnatury amerykańskim klientom, zanim ci się obudzą i zaczną klikać szkodliwe załączniki w e-mailach.

W tym czasie Chien przekroczył już dwuletni okres, jaki planował spędzić w Symantecu. Zaoszczędził wystarczającą ilość pieniędzy na studia doktoranckie i planował przenieść się do Kolorado, aby pojeździć na snowboardzie i rowerze przed złożeniem podania na studia z dziedziny nauk ścisłych. Jednak Symantec przedłożył mu kuszącą ofertę stanowiska w Holandii. Firma miała pod Amsterdamem biuro zajmujące się pomocą techniczną oraz sprzedażą i chciała zatrudnić w nim zespół analityków złośliwego oprogramowania. Chien nie potrafił odmówić. Znalazł się w Holandii niedługo przed tym, jak robak Love Letter zaatakował internet w maju 2000 r. Ten robak został zapoczątkowany jako złośliwy projekt filipińskich studentów, jednak później rozprzestrzenił się na miliony komputerów z całego świata. Była to znakomita okazja do sprawdzenia nowego europejskiego zespołu szybkiego reagowania (nawet jeśli składał się on z tylko jednej osoby). W rekordowym czasie 20 min Chien przeanalizował kod i opracował sygnatury potrzebne do wykrywania robaka. Niestety, jego wyczyn na niewiele się zdał, ponieważ Love Letter zużywał tyle przepustowości łącz internetowych, że klienci nie mogli skontaktować się z serwerami Symanteca w celu pobrania sygnatur. Gdy tylko kryzys minął, Chien zatrudnił czterech dodatkowych badaczy, aby uzupełnić zespół w Amsterdamie. Wszyscy byli gotowi, gdy w następnym roku pojawiło się kolejne poważne zagrożenie — robak Code Red.

Chien na krótko przeprowadził się do Tokio, gdzie otworzył następną jednostkę badawczą. Później, w 2004 r., Symantec przeniósł europejską siedzibę główną z Amsterdamu do Dublina. Wraz z biurem przeniósł się też Chien. Wkrótce potem rozbudował zespół badawczy o kilkunastu nowych pracowników, w tym O'Murchu. W 2008 r. wrócił do Stanów Zjednoczonych razem ze świeżo poślubioną Francuzką pracującą w biurze Symanteca w Holandii. Później w Kalifornii dołączył do niego O'Murchu.

Obecnie ten duet pracował w Culver City i razem z Falliere'em zmagał się z trudnym zadaniem dekonstrukcji Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PIERWSZA PRZESZKODA, na jaką natrafili badacze, pojawiła się przy próbie odszyfrowania całego kodu Stuxneta. O'Murchu odkrył wcześniej, że kod robaka znajduje się w dużym pliku .DLL umieszczanym na komputerach. Obejmował on dziesiątki wielokrotnie zaszyfrowanych mniejszych plików .DLL i komponentów. Wszystkie te szyfry trzeba było złamać i usunąć, aby dotrzeć do kodu. Na szczęście potrzebne klucze znajdowały się w samym kodzie. Za każdym razem, gdy Stuxnet trafiał na komputer z systemem Windows, używał tych kluczy do odszyfrowania i wypakowania wszystkich plików .DLL i komponentów potrzebnych na danej maszynie. Przynajmniej tak powinno to działać. Jednak na maszynie testowej niektóre klucze nie były aktywowane. Chodziło tu o ostatnie klucze, potrzebne do odblokowania ładunku.

O'Murchu analizował kod, próbując znaleźć powód problemu z ostatnimi kluczami. Wtedy natrafił na nawiązania do konkretnych modeli sterowników PLC Siemensa. Stuxnetowi nie chodziło *tylko* o systemy z zainstalowanym oprogramowaniem Siemens Step 7 lub WinCC. To oprogramowanie musiało ponadto korzystać z konkretnej serii sterowników PLC Siemensa — S7-315 lub S7-417. Tylko ta kombinacja oprogramowania i sprzętu aktywowała klucze Stuxneta odblokowujące i uruchamiające ładunek.

Jedyny problem polegał na tym, że Chien i O'Murchu nie mieli ani oprogramowania Siemensa, ani odpowiednich sterowników PLC. Bez tego musieli używać debuggera do wyrywkowego sprawdzania kodu w celu znalezienia kluczy i ręcznego odblokowania ładunku.

Debugger, podstawowe narzędzie w inżynierii odwrotnej, umożliwił im wykonywanie kodu krok po kroku (jak na filmie poklatkowym) w celu wyodrębnienia każdej funkcji i udokumentowania jej działania. Za pomocą tej techniki badacze znaleźli wszystkie sekcje kodu zawierające polecenia odszyfrowania złośliwego oprogramowania i za pomocą tych poleceń odnaleźli klucze. Jednak ustalanie kluczy było tylko połową sukcesu. Gdy już znaleźli je wszystkie, musieli określić algorytm deszyfrujący, w którym były używane poszczególne klucze. Wymagało to kilku dni pracy, jednak po odblokowaniu całego kodu badacze wreszcie ustalili wszystkie kroki wykonywane przez Stuxneta na początkowych etapach infekcji[4].

[4] Gdy „pogromcy wirusów" ustalili klucze i dopasowali je do algorytmów, napisali program deszyfrujący, aby umożliwić szybkie deszyfrowanie innych bloków kodu używających tych samych algorytmów. Dzięki temu po natrafieniu na nowe wersje Stuxneta, a nawet inne złośliwe oprogramowanie napisane przez tych samych autorów lub wykorzystujące te same algorytmy, nie musieli powtarzać żmudnego procesu debugowania całego kodu w celu znalezienia kluczy. Wystarczyło uruchomić program deszyfrujący.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jedna z pierwszych wykonywanych operacji polegała na ustaleniu, czy w komputerze działa 32-, czy 64-bitowa wersja systemu Windows. Stuxnet działał tylko w maszynach 32-bitowych. Robak określał też, czy komputer już jest zainfekowany Stuxnetem. W zainfekowanych maszynach sprawdzał, czy zainstalowane złośliwe oprogramowanie jest aktualne, i zastępował starsze pliki ich najnowszymi wersjami. Jeśli jednak natrafiał na komputer niezainfekowany, rozpoczynał wyrafinowany proces, wykonując szybko sekwencję kroków w celu zapoznania się ze środowiskiem maszyny i ustalenia najlepszej drogi postępowania.

W tym procesie na komputerze szybko umieszczany był jeden z rootkitów, aby ukrywał przed systemem pliki Stuxneta z pendrive'a. W tym celu rootkit zwodził system tak, by nazwy tych plików były niewidoczne dla skanerów wirusów. Można powiedzieć, że pliki te były ukrywane w cieniu skanera. Gdy skaner próbował zbadać zawartość pendrive'a, rootkit przechwytywał polecenia i zwracał zmodyfikowaną listę danych pozbawioną plików Stuxneta. Jednak niektórych skanerów nie można było zwieść w ten sposób. Stuxnet potrafił ustalić, które skanery są zagrożeniem, i odpowiednio dostosowywał do nich metodę działania. Po stwierdzeniu, że w ogóle nie potrafi oszukać danego skanera, wstrzymywał infekcję i kończył pracę.

Jeśli jednak Stuxnet decydował się kontynuować działanie, aktywował drugi sterownik. Wykonywał on dwa zadania. Po pierwsze, przez początkowych 21 dni po zainfekowaniu danej maszyny przez Stuxneta infekował wszystkie podłączane pendrive'y[5]. Drugą, ważniejszą operacją było odszyfrowanie i załadowanie dużego pliku .DLL i różnych komponentów do pamięci maszyny za pomocą nowatorskich technik udokumentowanych przez O'Murchu. Najpierw Stuxnet wypakowywał plik .DLL, aby uzyskać mniejsze, wewnętrzne pliki .DLL, a następnie wczytywał je do pamięci. Ponieważ pliki działały w pamięci, po każdym restarcie maszyny były usuwane, dlatego sterownik musiał wczytywać je przy każdym uruchomieniu komputera.

Po wypakowaniu i wczytaniu do pamięci dużego pliku .DLL i jego zawartości Stuxnet szukał nowych maszyn do zainfekowania oraz komunikował się z serwerami C&C, aby poinformować je o nowym podboju. Jeśli jednak na komputerze nie znajdowało się oprogramowanie Siemens Step 7

[5] W niektórych wersjach Stuxneta napastnicy wydłużyli ten czas do 90 dni.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

lub WinCC, Stuxnet po wykonaniu opisanych kroków przechodził na danej maszynie w stan uśpienia.

Badacze wiedzieli więc, jak Stuxnet się rozprzestrzenia i jak wczytuje plik. Nadal jednak nie rozumieli, po co go utworzono i do jakich zadań został zaprojektowany. Odpowiedzi na te pytania wciąż były ukryte w ładunku.

Gdy O'Murchu zastanawiał się nad tym, co do tej pory odkrył w części kodu pełniącej funkcję „pocisku", nie potrafił powstrzymać się od podziwu dla kunsztu napastników — pomysłowych rozwiązań problemów, jakie spodziewali się napotkać, i licznych scenariuszy, które musieli przetestować przed wypuszczeniem kodu. Nie wszystkie pojedyncze mechanizmy Stuxneta były zaawansowane, ale jako całość atak stanowił poważne zagrożenie.

Oprócz stosowania zaawansowanych metod ładowania plików i radzenia sobie z zabezpieczeniami Stuxnet używał długiej listy kontrolnej do upewnienia się, że wszystkie warunki są spełnione. Dopiero wtedy uruchamiał ładunek. Ponadto starannie śledził zużycie zasobów i zwalniał niepotrzebne już komponenty, aby zmniejszyć moc obliczeniową wykorzystywaną na danej maszynie. Zajęcie przez Stuxneta zbyt wielu zasobów groziło spowolnieniem maszyny i wykryciem ataku. Ponadto robak zastępował treść wielu tworzonych na komputerze plików tymczasowych, gdy nie były już potrzebne. Wszystkie programy generują pliki tymczasowe, natomiast zwykle nie dbają o ich usuwanie, ponieważ takie dane mogą zostać zastąpione plikami tymczasowymi utworzonymi przez inne aplikacje. Napastnicy nie chcieli jednak, by pliki Stuxneta zbyt długo znajdowały się w systemie, ponieważ zwiększało to ryzyko ich odnalezienia.

Jednak mimo wielu dodatkowych starań, jakich napastnicy dołożyli w trakcie przygotowywania kodu, kilka aspektów było zaskakująco niedopracowanych. Nie tylko O'Murchu tak uważał. Gdy badacze z Symanteca w ciągu kilku następnych tygodni opublikowali swoje odkrycia dotyczące Stuxneta, członkowie społeczności zainteresowanej zabezpieczeniami zaczęli wskazywać liczne słabe punkty w kodzie i stwierdzili, że jego autorom daleko jest do czołowych hakerów, za jakich uważano ich po pierwszych doniesieniach o tym robaku. Umiejętności techniczne autorów były niespójne i popełnili oni liczne błędy, które pomogły badaczom zrozumieć działanie Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Na przykład dużo trudniej byłoby odszyfrować Stuxneta, gdyby napastnicy zastosowali lepsze techniki zaciemniania kodu, pomagające powstrzymać narzędzia analityczne badaczy. Autorzy robaka mogli posłużyć się bardziej zaawansowanymi technikami szyfrowania, dzięki którym odblokowanie ładunku byłoby możliwe wyłącznie na docelowych maszynach. W ten sposób można byłoby też ukryć to, że Stuxnet szuka oprogramowania Siemens Step 7 i sterowników PLC. W Stuxnecie zastosowano słabe algorytmy szyfrowania i standardowe protokoły komunikacji z serwerami C&C, zamiast wykorzystać niestandardowe protokoły, które utrudniłyby badaczom utworzenie ujścia i odczytanie danych generowanych przez analizowane złośliwe oprogramowanie.

Komentarze kryptografa Nate'a Lawsona były pełne pogardy. W artykule na blogu napisał on, że autorzy Stuxneta „powinni wstydzić się amatorskich technik ukrywania ładunku" i że stosowali przestarzałe metody, od dawna zarzucone przez hakerów zajmujących się działalnością przestępczą. „Mam szczerą nadzieję, że kod nie został napisany przez Stany Zjednoczone — pisał — ponieważ chcę wierzyć, że nasi najlepsi twórcy cyberbroni wiedzą przynajmniej to, co bułgarscy nastolatkowie robili na początku lat 90."[6]. Inni badacze uznali, że połączenie zaawansowanych technik z zupełnie podstawowymi sprawia, iż Stuxnet wygląda jak Frankenstein złożony z oklepanych metod, a nie jak zaawansowany projekt elitarnej agencji wywiadowczej[7].

Jednak O'Murchu interpretował niespójności w Stuxnecie w odmienny sposób. Uważał, że napastnicy celowo posłużyli się do komunikacji z serwerami słabym szyfrowaniem i standardowymi protokołami, ponieważ chcieli, aby dane przesyłane z zainfekowanych maszyn wyglądały jak zwykła komunikacja i nie wzbudzały podejrzeń. Ponieważ komunikacja tych maszyn z serwerami była bardzo ograniczona (złośliwe oprogramowanie przesyłało tylko niewielką ilość informacji o każdej zainfekowanej maszynie), napastnicy nie potrzebowali bardziej zaawansowanego szyfrowania do jej ukrycia. Jeśli chodzi o lepsze zabezpieczenie ładunku, mogły istnieć

---

[6] Nate Lawson, „Stuxnet Is Embarrassing, Not Amazing", 17 stycznia 2011. Tekst jest dostępny na stronie: *https://rdist.root.org/2011/01/17/stuxnet-is-embarrassing-not-amazing/#comment-6451*.

[7] James P. Farwell, Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, „Survival" 53, nr 1, 2011, s. 25.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ograniczenia uniemożliwiające zastosowanie bardziej zaawansowanych technik — takich jak szyfrowanie danych z użyciem klucza określonego na podstawie konfiguracji docelowej maszyny, co pozwoliłoby odblokować ładunek tylko na tej maszynie[8]. Niewykluczone, że docelowe maszyny były skonfigurowane w odmienny sposób, co utrudniało posłużenie się jednym kluczem do szyfrowania ładunku. Mogły też występować inne problemy. Na przykład konfiguracja na komputerach mogła się zmieniać, przez co klucz stałby się bezużyteczny, a uruchomienie ładunku byłoby niemożliwe.

Wady Stuxneta mogły być też wynikiem ograniczeń czasowych. Możliwe, że coś zmusiło napastników do pospiesznego wypuszczenia kodu i szybkiego wykonania prac, których efekty wydały się krytykom niedbałe i amatorskie.

Jeszcze innym wytłumaczeniem dziwacznego połączenia zastosowanych technik była możliwość, że za Stuxneta odpowiadają różne zespoły programistów o różnych zdolnościach i umiejętnościach. Modułowy charakter tego złośliwego oprogramowania oznaczał, że w rozwijaniu go mogło brać udział kilka zespołów pracujących nad poszczególnymi częściami jednocześnie lub w różnych okresach. O'Murchu oszacował, że w zbudowaniu całego Stuxneta brały udział przynajmniej trzy zespoły: zaawansowany zespół „tygrysów" o wysokich umiejętnościach, który pracował nad ładunkiem dla oprogramowania i sterowników PLC Siemensa, drugi zespół, odpowiedzialny za mechanizmy rozprzestrzeniania i instalacji robaka oraz odblokowywanie ładunku, i trzecia, najsłabsza grupa, która przygotowała serwery C&C oraz szyfrowanie i protokoły używane do komunikacji.

[8] Jedną z metod, wskazaną przez Nate'a Lawsona na jego blogu, jest zebranie szczegółowych danych konfiguracyjnych z docelowej maszyny i wykorzystanie ich do wyznaczenia skrótu kryptograficznego klucza, który odblokowuje ładunek. Taki klucz jest bezużyteczny, dopóki złośliwe oprogramowanie nie natrafi na maszynę o dokładnie takiej samej konfiguracji lub ktoś nie uzyska klucza przez atak siłowy, sprawdzając wszystkie możliwe konfiguracje do czasu uzyskania odpowiedniej. Tę drugą technikę można powstrzymać, generując skrót na podstawie określonego zestawu danych konfiguracyjnych. W Stuxnecie używana była prostsza wersja techniki opisanej przez Lawsona. Robak ten używał podstawowych danych konfiguracyjnych o szukanym sprzęcie, aby odblokować ładunek za pomocą klucza, natomiast sam klucz był niezależny od konfiguracji. Dlatego gdy badacze ustalili klucz, mogli łatwo zastosować go do odblokowania ładunku bez konieczności znajomości konfiguracji. Jednak później badacze z firmy Kaspersky Lab natrafili na złośliwe oprogramowanie wykorzystujące bardziej zaawansowaną technikę ukrywania ładunku. Ten ładunek nigdy nie został odszyfrowany (zob. s. 304 –305).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Możliwe, że podział obowiązków był na tyle ściśle zdefiniowany, a zespoły na tyle odizolowane od siebie, że grupy te nigdy nie komunikowały się ze sobą.

Jednak choć każdy z zespołów miał inny poziom umiejętności i doświadczenia, wszystkie posiadały przynajmniej jedną cechę wspólną: nie pozostawiły w kodzie żadnych wskazówek pozwalających łatwo wyśledzić którąś z tych grup. A przynajmniej tak się wydawało.

PRZYPISYWANIE AUTORSTWA TO stały problem w śledztwach dotyczących ataków hakerów. Ataki na komputery można zainicjować w dowolnym miejscu świata i przekierować przez wiele przejętych maszyn lub serwerów pośredniczących, aby ukryć źródło operacji. Jeśli haker starannie ukrywa swoje poczynania, często niemożliwe jest dotarcie do niego na podstawie samych cyfrowych dowodów.

Jednak zdarza się, że twórcy złośliwego oprogramowania pozostawiają w kodzie pewne poszlaki (celowo lub przypadkiem), które mogą ujawniać, kim napastnik jest i skąd pochodzi, nie identyfikując go bezpośrednio. Dziwne anomalie i ślady pozostawione w pozornie niepowiązanych wirusach lub koniach trojańskich często pomagają śledczym w powiązaniu złośliwego oprogramowania w rodzinę, a nawet dotarciu do jej autora. Podobnie sposób działania seryjnego mordercy łączy go z listą zbrodni.

Kod Stuxneta był bardziej sterylny niż złośliwe oprogramowanie, z jakim Chien i O'Murchu stykali się na co dzień. Zauważalne były w nim jednak dwa aspekty.

Chien przeglądał notatki, jakie pewnego dnia poczynił na temat procesu infekcji stosowanego przez Stuxneta, gdy jego uwagę przykuło coś ciekawego. Był to znacznik infekcji, który zapobiegał instalacji Stuxneta na niektórych maszynach. Za każdym razem, gdy Stuxnet napotkał potencjalną nową ofiarę, przed rozpoczęciem odszyfrowywania i wypakowywania plików szukał w rejestrze systemu Windows „magicznego" łańcucha znaków 0x19790509. Jeśli znalazł ten łańcuch, wycofywał się z maszyny i rezygnował z infekowania jej.

Chien spotykał już wcześniej tego rodzaju „szczepionki". Hakerzy umieszczali je w rejestrach własnych komputerów, tak aby po przepuszczeniu testowego lub rzeczywistego ataku oprogramowanie nie zwróciło się przeciwko nim, infekując maszyny napastników lub inne komputery, które chcieli chronić.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Szczepionką może być jakakolwiek wartość ustalona przez hakera. Zwykle jest nią losowy łańcuch cyfr. Ale tym razem wartość wyglądała na datę 9 maja 1979 r. Najpierw podany był rok, potem miesiąc, a na końcu dzień. Jest to standardowy format dat w oprogramowaniu uniksowym. Inne pojawiające się w Stuxnecie łańcuchy cyfr uznane za badaczy za określone daty miały ten sam format.

Chien poszukał w Google'u informacji o znalezionej dacie. Był tylko częściowo zaskoczony, gdy jeden z wyników wyszukiwania łączył Izrael z Iranem. Wspomniana data z 1979 r. była dniem egzekucji znanego irańskiego biznesmena pochodzenia żydowskiego, Habiba Elghaniana. Został on rozstrzelany przez pluton egzekucyjny po tym, jak nowy rząd zdobył władzę w wyniku rewolucji islamskiej. Elghanian, bogaty filantrop i szanowany lider irańskiej społeczności żydów, został oskarżony o szpiegostwo na rzecz Izraela i stracony. Jego śmierć była punktem zwrotnym w stosunkach między społecznością żydowską a Iranem. Przez prawie 40 lat rządów szacha Mohammada Rezy Pahlawiego irańscy żydzi utrzymywali stosunkowo przyjazne relacje ze swoimi muzułmańskimi sąsiadami — podobnie jak islamski Iran z Izraelem. Jednak egzekucja Elghaniana, przeprowadzona zaledwie trzy miesiące po obaleniu szacha przez rewolucjonistów, była dla wielu perskich żydów niczym noc kryształowa i unaoczniła im, że życie pod nowym reżimem będzie zupełnie inne. To wydarzenie doprowadziło do masowego eksodusu żydów z Iranu do Izraela i rozbudziło utrzymującą się do dziś wrogość między tymi państwami.

Czy majowa data w Stuxnecie była przekazem „pamiętajcie o Alamo" skierowanym przez Izrael do Iranu, podobnym do listów, jakie żołnierze amerykańscy pisali czasem na bombach zrzucanych na wrogie terytoria? A może była to próba zmylenia tropów przez nieizraelskich napastników chcących zasugerować udział Izraela w operacji? A może Chien miał po prostu bujną wyobraźnię i dostrzegał znaczenie tam, gdzie go nie było? Chien mógł tylko zgadywać.

Wtedy jednak zespół z Symanteca znalazł inne informacje, które mogły prowadzić do Izraela, choć tym razem dopatrzenie się powiązań wymagało więcej wysiłku. W jednym z plików sterownika znajdowała się ścieżka ze słowami *myrtus* (czyli mirt) i *guava* (czyli guawa). Ścieżki prowadzą do katalogów komputera, gdzie zapisany jest dany plik lub dokument. Ścieżka do dokumentu „życiorys" zapisanego w katalogu *Dokumenty* na dysku *C:* to

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

c:\Dokumenty\życiorys.doc. Czasem, gdy programiści przetworzą kod źródłowy za pomocą kompilatora (narzędzia tłumaczącego czytelny dla człowieka język programowania na czytelny dla maszyny kod binarny), w skompilowanym pliku binarnym zapisywana jest ścieżka określająca, gdzie programista zapisał kod na swoim komputerze. Większość autorów złośliwego oprogramowania konfiguruje kompilatory tak, aby usuwały ścieżki, jednak twórcy Stuxneta — celowo lub przypadkiem — tego nie zrobili. Ścieżka znaleziona w pliku sterownika wyglądała tak: *b:\myrtus\src\ objfre_w2k_x86\ i386\guava.pdb*. Oznaczało to, że sterownik jest częścią projektu nazwanego przez programistę *guava* i zapisanego w katalogu *myrtus*. Mirt to rodzaj roślin obejmujący kilka gatunków guaw. Chien zastanawiał się, czy autor projektu był miłośnikiem botaniki, czy może chodziło o coś innego.

Poszukał informacji na temat mirtu i odkrył pośredni związek z innym ważnym wydarzeniem w historii żydów — ratunkiem tego narodu w starożytnej Persji przed masakrą w IV w. p.n.e. dzięki pomocy królowej Estery. Wedle legend Estera była Żydówką, która poślubiła perskiego króla Achaszerosza. Król nie znał jednak pochodzenia swojej żony. Gdy Estera dowiedziała się, że najwyższy urzędnik w kraju, Haman, planuje za zgodą króla zabić wszystkich Żydów w imperium perskim, ujawniła przed Achaszeroszem swoje pochodzenie i błagała, by król oszczędził ją i jej lud. Achaszerosz nakazał wtedy egzekucję samego Hamana i pozwolił zamieszkującym imperium Żydom walczyć z wszystkimi wrogami, jakich Haman zgromadził w celu wymordowania tego ludu. Żydzi zwyciężyli, przy czym zginęło 75 tys. ich przeciwników. Święto Purim, celebrowane co roku przez żydowskie społeczności na całym świecie, upamiętnia ten ratunek perskich Żydów przed pewną śmiercią.

Na pozór ta historia nie ma nic wspólnego ze Stuxnetem. Jednak Chien odkrył możliwe powiązanie dzięki hebrajskiemu imieniu Estery. Przed zmianą imienia i zyskaniem tytułu królowej Persji Estera nazywała się Hadassah. Słowo to w hebrajskim oznacza mirt.

W świetle ówczesnych wydarzeń nietrudno było znaleźć analogie między starożytną i współczesną Persją. W 2005 r. w serwisach informacyjnych cytowano wezwanie irańskiego prezydenta Mahmuda Ahmadineżada do wymazania Izraela z map. Choć wedle późniejszych doniesień słowa prezydenta zostały błędnie przetłumaczone, nie było tajemnicą, że Ahmadineżad życzyłby sobie wyeliminowania państwa żydowskiego, podobnie jak

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wiele wieków wcześniej Haman chciał pozbyć się współczesnych mu Żydów[9]. Trzynastego lutego 2010 r., mniej więcej w czasie, gdy twórcy Stuxneta przygotowywali nową wersję ataku na irańskie maszyny, rabin Owadia Josef, wpływowy były naczelny rabin Izraela i polityk, w wygłoszonym przed świętem Purim kazaniu bezpośrednio powiązał starożytną Persję ze współczesnym Iranem. Stwierdził, że Ahmadineżad to „Haman naszego pokolenia".

„Dziś w Persji żyje nowy Haman, grożący nam bronią jądrową" — powiedział Josef. Dodał jednak, że podobnie jak niegdyś Haman i jego poplecznicy, tak Ahmadineżad wraz ze zwolennikami odkryją, iż ich łuki są połamane, a miecze zwrócone przeciwko nim, aby „przebić ich własne serca"[10].

Nic z tego nie było jednak dowodem, że mirt ze sterownika Stuxneta jest nawiązaniem do *Księgi Estery*. Zwłaszcza w kontekście tego, że niektórzy badacze później zasugerowali, iż słowo *myrtus* można zinterpretować w inny sposób — jako *my RTUs*, czyli „moje zdalne moduły RTU". Moduły RTU, podobnie jak sterowniki PLC, to przemysłowe komponenty sterownicze używane do sterowania sprzętem i procesami oraz monitorowania ich. Ponieważ Stuxnet miał atakować sterowniki PLC Siemensa, prawdziwe mogło być drugie znaczenie nazwy *myrtus*[11]. Nie dało się jednak z pewnością tego stwierdzić.

---

[9] Profesor Juan Cole z University of Michigan oraz inni badacze zwrócili uwagę na to, że w języku perskim nie ma idiomu „wymazać z mapy". Ich zdaniem Ahmadineżad w rzeczywistości powiedział, że ma nadzieję, iż żydowscy (syjonistyczni) okupanci Jerozolimy upadną i zostaną wymazani z kart historii.

[10] „Rabbi Yosef: Ahmadinejad a New Haman", Israel National News, 14 lutego 2010. Tekst jest dostępny na stronie: *http://www.israelnationalnews.com/News/Flash.aspx/180521*.

[11] John Bumgarner, dyrektor techniczny w US Cyber Consequences Unit, przychyla się do tej interpretacji. Ponadto jego zdaniem słowo *guava* w ścieżce do sterownika jest związane z cytometrami przepływowymi produkowanymi przez kalifornijską firmę Guava Technologies. Cytometry przepływowe to urządzenia służące do zliczania i badania mikrocząsteczek. Wykorzystuje się je m.in. do pomiarów izotopów uranu. Bumgarner uważa, że urządzenia te mogły być używane w Natanzie do pomiaru poziomu wzbogacenia sześciofluorku uranu w procesie oddzielania izotopów ^{238}U od potrzebnych w reaktorach i bombach nuklearnych izotopów ^{235}U. Guava Technologies produkuje cytometry przepływowe Guava EasyCyte Plus, które można zintegrować ze sterownikami PLC w celu zapewnienia operatorom w czasie rzeczywistym danych o poziomie izotopów uranu. Sprzedaż tych urządzeń jest regulowana. Aby sprzedać je Iranowi, firma musi zarejestrować ten fakt na mocy dokumentu *Trade Sanctions Reform and Export Enhancement Act of 2000*. Zob. John Bumgarner, „A Virus of Biblical Distortions", 6 grudnia 2013. Ten tekst jest dostępny na stronie: *http://www.darkreading.com/attacks-breaches/a-virus-of-biblical-distortions/d/d-id/1141007?*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Badacze z Symanteca starali się nie wyciągać żadnych wniosków na podstawie danych. Zamiast tego w artykule opublikowanym na blogu Chien i jego współpracownicy napisali: „Rozpocznijmy spekulacje”[12].

[12] Patrick Fitzgerald, Eric Chien, „The Hackers Behind Stuxnet”, Symantec, 21 lipca 2010. Ten tekst jest dostępny na stronie: *https://www.symantec.com/connect/blogs/hackers-behind-stuxnet*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 5

WIOSNA AHMADINEŻADA

Sznur czarnych opancerzonych mercedesów wyjechał z Teheranu, kierując się na południe w stronę Natanzu z prędkością 140 km/h. W trzech z tych samochodów siedzieli osobno: Olli Heinonen, jego przełożony, dyrektor MAEA Muhammad el-Baradei, i ich trzeci współpracownik z agencji. Był rześki zimowy poranek pod koniec lutego 2003 r., sześć miesięcy po tym, jak Alireza Jafarzadeh i jego grupa ujawnili tajny zakład w Natanzie. Inspektorzy mieli wreszcie po raz pierwszy przyjrzeć się temu kompleksowi. Z el-Baradeiem jechał elegancki mężczyzna o wyglądzie profesora, siwowłosy i z krótką przystrzyżoną szpakowatą brodą. Był to Gholam Reza Aghazadeh, wiceprezydent Iranu i prezes MAEA.

Dwa tygodnie wcześniej prezydent Iranu Mohammad-Reza Khatami wreszcie przyznał, że Irańczycy budują w Natanzie zakład wzbogacania uranu. Potwierdził to, co ISIS i inne organizacje podejrzewały na temat tego kompleksu. Prezydent w przemówieniu powiedział, że Iran buduje wiele zakładów na potrzeby wszystkich etapów cyklu produkcji paliwa, a kompleks w Natanzie jest tylko jednym z nich. Utrzymywał jednak, że Iran zamierza wykorzystywać atom wyłącznie w celach pokojowych[1]. Dodał, że

[1] Khatami przemawiał w Teheranie 9 lutego 2003 r. w trakcie spotkania między ministerstwem nauki, badań i technologii a rektorami uniwersytetów. Fragmenty przemówienia zostały przytoczone na stronie: *http://www.iranwatch.org/library/government/iran/iran-irna-khatami-right-all-nations-nuclear-energy-2-9-03*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

dzięki wierze, logice i licznym atutom, jakie posiada wielkie państwo takie jak Iran, broń masowego zniszczenia nie jest temu krajowi potrzebna. Nie powiedział jednak, dlaczego — skoro Iran nie ma nic do ukrycia — zakład w Natanzie znajduje się głęboko pod ziemią. Jeśli nie dzieje się tam nic nielegalnego, to po co zabezpieczać go warstwami cementu i gleby? Ponadto po co budować zakład wzbogacania uranu, jeżeli paliwo do irańskich reaktorów nuklearnych można zakupić od innych państw, tak jak robi to większość krajów korzystających z takich reaktorów? Zresztą sam Iran też kupował takie paliwo od Rosji. Te i inne pytania krążyły po głowach urzędników MAEA w drodze do Natanzu.

MAEA znacznie się zmieniła od czasu jej założenia w 1957 r. Została utworzona w celu promocji rozwijania technologii atomowych w celach pokojowych. Jej dodatkowa funkcja strażnika jądrowego, dbającego o to, by kraje nie wykorzystywały tych technologii do budowania broni, była pierwotnie drugorzędna. Jednak w okresie pięciu dziesięcioleci od powstania agencji to drugie zadanie stało się najważniejsze, ponieważ po jednym kryzysie atomowym następował kolejny. Niestety, spełnianie tej funkcji często było utrudnione z powodu ograniczonych uprawnień do kontrolowania lub karania państw naruszających porozumienia o zabezpieczeniach.

Ponieważ agencja nie posiadała wydziału wywiadowczego do badania podejrzanych działań, musiała polegać na danych od wywiadów 35 stowarzyszonych państw, takich jak np. Stany Zjednoczone, przez co narażała się na manipulacje ze strony tych krajów. Innym źródłem były informacje, jakie inspektorzy mogli wywnioskować na podstawie odwiedzin w obiektach jądrowych. Jednak ponieważ przeważnie odwiedzali tylko zakłady wymienione na zadeklarowanej liście obiektów jądrowych, nieuczciwe państwa mogły swobodnie prowadzić nielegalne prace w niezgłoszonych kompleksach. Nawet po zdobyciu dowodów na to, że dany kraj narusza porozumienia, MAEA nie mogła wiele zrobić, aby wymusić zmiany. Mogła jedynie zgłosić naruszające przepisy państwo Radzie Bezpieczeństwa ONZ-etu, która mogła przegłosować nałożenie sankcji na dany kraj[2].

[2] Przedstawiciele 35 państw członkowskich z Rady Gubernatorów MAEA mogą przegłosować rozpoczęcie śledztwa lub zażądać nałożenia sankcji na kraj przez Radę Bezpieczeństwa ONZ-etu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Te słabości stały się oczywiste w 1991 r., po zakończeniu pierwszej wojny w Zatoce Perskiej, gdy inspektorzy wkroczyli do powojennego Iraku, aby zbadać ruiny, i odkryli, że Saddam Husajn realizował zaawansowany program budowy broni jądrowej tuż pod ich nosem. Przed wojną MAEA zaświadczyła, że współpraca Husajna z agencją była „wzorowa"[3]. Dlatego inspektorzy byli zaskoczeni dokonanym po wojnie odkryciem, że zostali oszukani. Według niektórych szacunków Irakowi brakowało tylko roku do uzyskania ilości materiałów rozszczepialnych wystarczającej do zbudowania bomby atomowej i tylko dwóch – trzech lat do momentu wyprodukowania arsenału broni jądrowej[4]. Jeszcze bardziej szokujące było to, że nielegalne działania prowadzono w pomieszczeniach i budynkach w bezpośrednim pobliżu zgłoszonych zakładów sprawdzanych przez inspektorów. Jednak zgodnie z regułami inspektorzy nie mogli z własnej inicjatywy kontrolować tych niezgłoszonych miejsc[5].

Rozsierdzona dwulicowością Irakijczyków MAEA opracowała protokół dodatkowy, rozszerzający porozumienie o zabezpieczeniach. Ten protokół zwiększał zakres działań, jakie muszą być zgłaszane do MAEA. Ponadto agencja zyskiwała możliwość zadawania bardziej dociekliwych pytań oraz żądania dostępu do ewidencji zakupów sprzętu i materiałów. Łatwiejsza stawała się też inspekcja zakładów podejrzanych o nielegalną działalność. Z protokołem dodatkowym związany był tylko jeden haczyk. Dotyczył on tylko państw, które go ratyfikowały. W 2003 r., gdy inspektorzy kontrolowali Natanz, Iran nie był jednym z nich. Dlatego zakres żądań inspektorów wobec Iranu był ograniczony[6].

---

[3] Przed wojną zastępca dyrektora MAEA odpowiedzialny za przestrzeganie umów poinformował Leonarda Weissa, dyrektora Senackiej Komisji Administracji, że współpraca Iraku z MAEA nie tylko jest wzorowa, ale też że MAEA nie otrzymała żadnych informacji o tym, że Irak może robić coś niewłaściwego. Zob. Leonard Weiss, *Tighten Up on Nuclear Cheaters*, „Bulletin of Atomic Scientists" 47, maj 1991, s. 11.

[4] David Albright, Mark Hibbs, *Iraq's Nuclear Hide and Seek*, „Bulletin of Atomic Scientists" 47, wrzesień 1991, s. 27.

[5] Douglas Frantz, Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets*, Free Press, Nowy Jork 2007, s. 188.

[6] W 2004 r. Iran zgodził się podpisać protokół dodatkowy, ale go nie ratyfikował. Później, w 2006 r., gdy MAEA zgłosiła Radzie Bezpieczeństwa ONZ-etu, że Iran nie przestrzega porozumień o zabezpieczeniach, Iran w odpowiedzi ogłosił, że nie będzie stosował się do wspomnianego protokołu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PO TRZYGODZINNEJ JEŹDZIE z Teheranu do Natanzu inspektorzy dotarli do celu w późnych godzinach porannych wspomnianego wcześniej lutowego dnia. Po drodze minęli po lewej stronie Hoz-e-Soltan, słone jezioro, które w lecie wyparowywało, a w zimie było głębokim do kolan akwenem ze słonawą wodą. Po prawej widzieli miejscowość Kom — ośrodek nauk szyitów i jedno z najświętszych miast islamu.

Po minięciu Komu 100 km jechali przez niekończące się piaski i autostradę, aż dotarli do miejscowości Kaszan. Po dalszych 20 km, w dzikiej okolicy z odcieniami brązu i beżu, na horyzoncie, niczym wyrastające z pustyni, pojawiły się budynki.

Kiedy dotarli do Natanzu, Heinonen był zdumiony tym, że budowa rozrastającego się kompleksu jest zaawansowana znacznie bardziej niż sądził. Oprócz podziemnych hal gotowy był już labirynt naziemnych budowli, w tym grupa pięciu struktur z prefabrykatów z aluminiową elewacją. Budynki te stały na planie krzyża. Zbudowano też dużą elektryczną stację rozdzielczą do zasilania budynków i wirówek. Jedną z pięciu struktur okazał się pilotażowy zakład wzbogacania uranu. Była to jednostka badawcza, w której technicy mogli testować nowe modele wirówek i kaskady przed zainstalowaniem ich w podziemnych halach produkcyjnych. Po zainstalowaniu w halach wirówki miały kręcić się latami, dlatego zakład pilotażowy był niezbędny do wcześniejszego zweryfikowania, czy zastosowana technologia i proces wzbogacania działają.

Choć do rozpoczęcia produkcji w podziemnych halach potrzeba było jeszcze dużo czasu, technicy uruchomili już w zakładzie pilotażowym ok. 160 wirówek. Gotowe były też komponenty do budowy setek kolejnych urządzeń tego typu[7]. Zakład pilotażowy miał rozpocząć pracę w czerwcu, czyli cztery miesiące po wizycie inspektorów, a Iran do końca roku chciał zainstalować 1000 wirówek. Pierwsza partia nisko wzbogaconego uranu miała być gotowa sześć miesięcy później.

Gdy Aghazadeh oprowadzał inspektorów po obiekcie, przekonywał ich, że do Natanzu nie sprowadzono jeszcze sześciofluorku uranu, dlatego nie zostały przeprowadzone testy wzbogacania z użyciem tego gazu. Stwierdził, że testy przeprowadzano tylko na poziomie symulacji komputerowych.

[7] David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*, Free Press, Nowy Jork 2010, s. 192.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Było to ważne, ponieważ wzbogacanie uranu bez zgłoszenia tego do MAEA oznaczałoby naruszenie przez Iran porozumienia o zabezpieczeniach. Heinonen nie wierzył jednak zapewnieniom Irańczyków. Utrzymywanie, że Iran wydał 300 mln dolarów na budowę zakładu wzbogacania uranu bez wcześniejszego przetestowania kaskad z użyciem gazu i upewnienia się, że proces wzbogacania działa, było bardzo naciągane.

Z zakładu pilotażowego inspektorów zaprowadzono do sali pokazowej, gdzie Irańczycy starannie rozłożyli komponenty wirówek IR-1 (jak w zaawansowanym projekcie szkolnym), a także zaprezentowali kilka zmontowanych urządzeń tego typu. Aghazadeh poinformował inspektorów, że Iran wyprodukował wirówki IR-1 na podstawie własnego projektu. Jednak gdy Heinonen bliżej przyjrzał się tym urządzeniom, zauważył, że przypominają one maszyny Urenco pierwszych generacji, produkowane wiele lat wcześniej przez to konsorcjum w Europie. Inspektor nie wiedział jeszcze, że Iran zakupił skradziony projekt od A.Q. Khana, ale z podejrzliwością traktował historyjki Aghazadeha.

Po wizycie w sali pokazowej inspektorzy zostali skierowani do tunelu w kształcie litery U, który Corey Hinderstein dostrzegła na zdjęciach satelitarnych. Po przejściu tunelu zobaczyli dwie przestronne hale zlokalizowane ponad 20 m pod ziemią. Iran planował zacząć zapełnianie hal wirówkami dopiero w 2005 r. Hale miały powierzchnię 32 tys. m^2 każda i mogły pomieścić ok. 47 tys. wirówek[8]. Na razie jednak były puste.

W trakcie wizyty kontakty inspektorów z irańskimi urzędnikami były serdeczne. Sytuacja stała się bardziej napięta, gdy popołudniem karawana wróciła do Teheranu i Heinonen poprosił swoich gospodarzy o pokazanie tajnych magazynów uranu. Aghazadeh był zaskoczony pytaniem i udawał niewiedzę. Heinonen posiadał jednak otrzymane od rządów państw zachodnich dane, wedle których w 1991 r. Iran potajemnie zakupił od Chin uran, w tym sześciofluorek uranu[9]. Przedstawił list od urzędników chińskich potwierdzający tę transakcję. Gdy Irańczycy później ujawnili zapasy uranu,

[8] David Albright, Corey Hinderstein, „The Iranian Gas Centrifuge Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images", ISIS, 14 marca 2003. Ten tekst jest dostępny na stronie: *http://isis-online.org/publications/iran/natanz03_02.html*. Zob. też raport Rady Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", 6 czerwca 2003, s. 6.

[9] Transakcja dotyczyła sześciofluorku uranu, tetrafluorku uranu i tlenku uranu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

twierdząc, że o nich zapomnieli, Heinonen i jego współpracownicy zauważyli, że kontenery były lżejsze niż oczekiwali. Ponadto wyglądało na to, że brakuje części sześciofluorku uranu. Irańczycy stwierdzili, że musiał wyparować przez luki w kontenerach, Heinonen podejrzewał jednak, że gaz zastosowano w tajnych testach wirówek.

To wtedy Heinonen zażądał wizyty w fabryce zegarków firmy Kalaye Electric. W trakcie sierpniowej konferencji prasowej NCRI wskazała Kala Electric (z nieco odmienną pisownią) jako jedną z firm przykrywek, które Iran wykorzystywał w ramach tajnego programu jądrowego. NCRI nie określiła wcześniej roli tej firmy w programie. Jednak krótko po przyjeździe inspektorów z MAEA do Iranu w celu wizyty w Natanzie NCRI, w dogodnym dla MAEA momencie, ogłosiła, że zakłady firmy Kalaye są wykorzystywane do badań nad wirówkami i produkcji tych urządzeń. To, w połączeniu z nieujawnionymi zasobami uranu, dało Heinonenowi potrzebne argumenty do zażądania zaplanowanej w ostatniej chwili wizyty w fabryce.

Irańczycy niechętnie zaprowadzili inspektorów do biur firmy Kalaye, które w większości okazały się puste. Utrzymywali jednak, że nie potrafią znaleźć kluczy, by otworzyć samą fabrykę. Inspektorzy mieli wyjechać z Iranu następnego dnia, dlatego wymogli obietnicę, że zobaczą fabrykę w trakcie następnej wizyty. Niestety, do momentu ich powrotu do Iranu minął ponad miesiąc i Irańczycy mieli mnóstwo czasu na przeprowadzenie porządków. Inspektorzy w jednym z budynków fabrycznych dostrzegli oczywiste ślady malowania ścian, a także wymiany drzwi i fugowania płytek podłogowych. Podejrzewając, że Irańczycy próbowali coś ukryć, inspektorzy chcieli pobrać z budynków próbki w celu przetestowania ich pod kątem śladów wzbogaconego uranu[10]. Zbieranie próbek było czynnością, jaką MAEA dodała do swojego repertuaru środków po nieudanych próbach wykrycia nielegalnego irackiego programu jądrowego. Inspektorzy za pomocą specjalnych bawełnianych płatków i patyczków zbierali kurz ze ścian i powierzchni, a następnie sprawdzali go w celu wykrycia cząsteczek uranu nawet rzędu pikograma. Określali przy tym, jakiego rodzaju uran znajdował się w danym miejscu, a nawet mierzyli, czy był

[10] Amerykanie na zdjęciach satelitarnych uchwycili ciężarówki w opisywanym obiekcie, co wskazywało na to, że Irańczycy przed przyjazdem inspektorów pozbyli się dowodów. Zob. Frantz, Collins, *Nuclear Jihadist*, s. 293.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wzbogacony i do jakiego stopnia[11]. Irańczycy nie pozwolili jednak na zbieranie żadnych próbek.

Wiele miesięcy później, gdy Iran zezwolił na zebranie próbek z fabryki, a także z pilotażowego zakładu wzbogacania uranu w Natanzie, inspektorzy znaleźli cząsteczki nisko i wysoko wzbogaconego uranu, który nie znajdował się na liście materiałów zadeklarowanych przez Irańczyków[12]. Skonfrontowani z dowodami oszustw urzędnicy przyznali wreszcie, że w fabrykach firmy Kalaye znajdował się wzbogacony uran. Stanowiło to naruszenie porozumienia o zabezpieczeniach, jakie Iran podpisał z MAEA. Irańczycy utrzymywali jednak, że gaz był wzbogacany wyłącznie w celu testowania wirówek i został wzbogacony tylko do poziomu 1,2%. Było to jednak niezgodne z cząsteczkami zebranymi przez MAEA, wzbogaconymi na poziomie od 36 do 70%[13].

Uran w stanie naturalnym zawiera mniej niż 1% potrzebnego w reaktorach i bombach izotopu ^{235}U. Większość reaktorów nuklearnych wymaga uranu wzbogaconego na poziomie tylko 3 – 5%. Wysoko wzbogacony uran jest wzbogacany do poziomu 20% i więcej. Choć uran wzbogacony na poziomie 20% można stosować w prostych urządzeniach nuklearnych i niektórych reaktorach, uran do broni jądrowej jest wzbogacany do poziomu 90% i więcej.

Irańscy urzędnicy twierdzili, że cząsteczki wysoko wzbogaconego uranu musiały pochodzić z resztek pozostawionych w wirówkach zakupionych przez Iran. Oznaczało to przyznanie, że Iran nie wyprodukował wirówek według własnego projektu, jak wcześniej utrzymywał, ale skorzystał z pomocy innego państwa. Nagle obawy dotyczące irańskiego programu nuklearnego znacznie wzrosły.

Próbki nie były dowodem na to, że Iran pracuje nad tajnym programem budowy broni jądrowej, ale wskazywały na to, iż inspektorzy mają przed sobą

[11] MAEA, „Tools for Nuclear Inspection". Jest to opublikowana przez dział informacji publicznych agencji dwustronicowa broszurka opisująca proces pobierania próbek środowiskowych. Dokument jest dostępny na stronie: *https://www.iaea.org/sites/default/files/inspectors.pdf*.

[12] Raport Rady Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", 10 listopada 2003, s. 6 – 7.

[13] Sharon Squassoni, „Iran's Nuclear Program: Recent Developments", raport CRS dla Kongresu, 23 listopada 2005, s. 3.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

dużo pracy, jeśli chcą ustalić zakres irańskiego programu nuklearnego. Świadczyły też o tym, że nie można wierzyć w nic, co mówią irańscy urzędnicy. Był to początek długiej i męczącej przeprawy, którą zajmowała się MAEA przez resztę dekady. W tym okresie inspektorzy starali się zrozumieć historię irańskiego programu nuklearnego i ustalić możliwości tego kraju w zakresie produkcji broni atomowej.

W czasie gdy MAEA zaczynała tę przeprawę, NCRI w maju 2003 r. ogłosiła, że posiada dowody na istnienie innych tajnych obiektów nuklearnych w Iranie, w tym zakładu w wiosce Lashkar Abad. Iran przyznał, że zbudował tam następny pilotażowy zakład do eksperymentów nad laserowym wzbogacaniem uranu (jest to inna metoda wzbogacania tego materiału)[14]. Po kilku miesiącach NCRI poinformowała o istnieniu dwóch kolejnych obiektów nuklearnych, w tym jednego w zlokalizowanych bezpośrednio pod Teheranem magazynach, otoczonych w celu ich ukrycia złomowiskami samochodów. Zdaniem NCRI znajdował się tam tajny pilotażowy zakład wzbogacania uranu, który Iran otworzył po lutowej wizycie MAEA w Natanzie. Zakład ten miał umożliwić technikom potajemne prowadzenie eksperymentów z dala od oczu ciekawskich inspektorów[15].

Tak duża liczba publicznie ujawnionych informacji w tak krótkim czasie oznaczała, że ktoś próbował wywierać presję na irańskich urzędników. Jednak te rewelacje wymagały też dodatkowej pracy od inspektorów MAEA, którzy teraz musieli dodać do listy monitorowanych lokalizacji nowe obiekty. Do znajdujących się już na liście Buszehru i dwóch reaktorów MAEA dodała pilotażowy i komercyjny zakład wzbogacania uranu w Natanzie, planowany reaktor w Araku i zakład przetwarzania uranu w Isfahanie ok. 160 km od Natanzu, gdzie Iran planował przetwarzać uran w gaz wzbogacany w Natanzie.

[14] Organizacja ISIS udostępnia stronę ze szczegółowym opisem irańskiego projektu wzbogacania uranu z użyciem lasera. Adres tej strony to: *http://isisnuclearіran.org/sites/by-type/category/laser-enrichment*.

[15] Te informacje pochodzą z transkrypcji oświadczenia wydanego przez rzecznika NCRI Alirezę Jafarzadeha, „Iran-Nuclear: Iranian Regime's New Nuclear Sites" (*http://www.ncr-iran.org/en/news/nuclear/568-iran-nuclear-iranian-regimes-new-nuclear-sites*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

GDY POJAWIAŁY SIĘ pytania dotyczące programu nuklearnego, Iran zdecydowanie realizował plany wzbogacania uranu. W czerwcu pracownicy w Natanzie zaczęli umieszczać pierwszą porcję sześciofluorku uranu w wirówkach w zakładzie pilotażowym, co dodatkowo zaalarmowało inne kraje. Ministrowie państw zagranicznych grupy EU3 (Francji, Niemiec i Wielkiej Brytanii) nalegali, by Iran wstrzymał wzbogacanie uranu do czasu, gdy MAEA ustali więcej faktów na temat programu nuklearnego w tym kraju. Rozpoczęły się negocjacje i w październiku Iran zdecydował się tymczasowo wstrzymać wzbogacanie. Zgodził się też udostępnić szczegółową historię programu nuklearnego, aby wyeliminować „wszelkie wieloznaczności i wątpliwości dotyczącego jego czysto pokojowego charakteru"[16]. Iran w pewnym stopniu zrealizował tę obietnicę, jednak choć urzędnicy przekazali tę historię MAEA, przyznając, że prace nad wirówkami trwały z przerwami od 18 lat, w raporcie zostało pominiętych wiele ważnych szczegółów[17]. MAEA dowiedziała się o tym tylko dlatego, że gdy próbowała uzyskać dane od irańskich urzędników, otrzymała też dodatkowe informacje o tajnym programie nuklearnym od CIA.

Kilka lat wcześniej CIA przeniknęła do nuklearnej sieci dostawców A.Q. Khana i zapewniła sobie współpracę kilku jego kluczowych europejskich kontrahentów, którzy stali się wtyczkami CIA. Od nich dowiedziała się, że Khan sprzedał Irańczykom projekty pakistańskich wirówek P-1, czyli projekty wykradzione z Urenco. Ustalili też, że Khan dostarczył Libii prototypy bardziej zaawansowanych wirówek P-2. Heinonen wywnioskował, że skoro Khan sprzedał projekty wirówek P-2 Libijczykom, musiał dostarczyć je także Iranowi. Iran nie wspominał o nich w swojej szczegółowej historii, jeśli jednak rzeczywiście miał do nich dostęp, to irański program wzbogacania uranu mógł być dużo bardziej zaawansowany, niż podejrzewał Heinonen. MAEA naciskała na Iran, aby ujawnił, czy produkuje wirówki P-2. Urzędnicy przyznali, że rzeczywiście otrzymali w 1996 r. projekt takich wirówek. Zdaniem urzędników konstruktorzy próbowali w okolicach 2002 r. zbudować wirówki na podstawie tego projektu, jednak

[16] Są to słowa Rezy Aghazadeha, wiceprezydenta Iranu, pochodzące z listu do MAEA z 21 października 2003 r. i przytoczone w raporcie Rady Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", 10 listopada 2003, s. 4.

[17] *Ibid*., s. 8.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

szybko zaprzestali tych prac, ponieważ natrafili na problemy z wirnikami. Irańczycy utrzymywali, że nie starali się ukryć prac nad wirówkami P-2, tylko zamierzali ujawnić je później.

W następnych miesiącach sytuacja jeszcze się pogorszyła, ponieważ pojawiły się pytania dotyczące kolejnego tajnego obiektu w Iranie, w teherańskim Centrum Badań Fizycznych[18]. Jednak zanim inspektorzy uzyskali pozwolenie na zbadanie tego budynku, został on wyburzony, a wierzchnią warstwę gleby wywieziono. Dlatego zebranie próbek do testów okazało się niemożliwe[19]. W kwietniu Iran ogłosił plany przeprowadzenia w Isfahanie prób przetworzenia oczyszczonej rudy uranu (żółtego uranu) w sześciofluorek uranu. Grupa EU3 uznała to za naruszenie podpisanego z Iranem porozumienia o tymczasowym wstrzymaniu prac, ponieważ przetwarzanie rudy na gaz było wstępem do wzbogacania uranu. Europejczycy nie naciskali jednak w tej kwestii z obawy o to, że Iran całkowicie zerwie i tak już słabe porozumienie.

W maju MAEA nieoczekiwanie otrzymała duży zbiór dokumentów nieznanego pochodzenia, które wzbudziły kolejne zastrzeżenia co do irańskiego programu nuklearnego.

Zaczęło się od tego, że Heinonen odebrał telefon od kobiety z amerykańskim akcentem, która przedstawiła się jako Jackie. Podejrzewał, że była to pracownica CIA, ale o to nie pytał. Jackie znała szczegóły dochodzenia dotyczącego irańskiego programu nuklearnego i stwierdziła, że posiada informacje, które mogą zainteresować Heinonena. Fin obawiał się, że CIA chce manipulować MAEA, ale zgodził się spotkać z kobietą w Starbucksie[20].

---

[18] NCRI ujawniła ten obiekt w 2003 r., jednak wówczas stwierdziła, że realizowany jest tam program budowy broni biologicznej. Z informacji uzyskanych przez MAEA, ISIS i inne agencje w 2004 r. wynika jednak, że prowadzona była tam działalność nuklearna, wskutek czego MAEA zażądała prawa do inspekcji.

[19] Iran stwierdził, że obiekt został wyburzony na początku grudnia 2003 r. z powodu sporu o własność ziemi toczonego między ministerstwem obrony a miastem Teheran. Budynki zburzono, aby móc zwrócić ziemię miastu. Zob. ISIS, „The Physics Research Center and Iran's Parallel Military Nuclear Program", 23 lutego 2012 (*http://isis-online.org/uploads/isis-reports/documents/PHRC_report_23February2012.pdf*).

[20] Informacje o spotkaniu i dokumentach pochodzą z wywiadu z Heinonenem przeprowadzonym przez autorkę w grudniu 2011 r. Zob. też Catherine Collins, Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking*, Free Press, Nowy Jork 2011, s. 112, oraz Erich Follath, Holger Stark, *The Birth of a Bomb: A History of Iran's Nuclear Ambitions*, „Der Spiegel", 17 czerwca 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W kawiarni czekała na niego młoda Azjatka. Powiedziała, że może zorganizować spotkanie z dwiema wtyczkami CIA z sieci dostawców Khana. Osoby te miały wprowadzić Heinonena w interesy Khana z Iranem. Kobieta powiedziała też, że ma stos dokumentów dotyczących irańskiego programu nuklearnego, które chce mu pokazać. Te dokumenty pochodziły od pracującego dla rządu teherańskiego biznesmena z branży produkcji stali i betonu. Ta działalność doprowadziła biznesmena do Natanzu i Isfahanu oraz umożliwiła mu kontakty z ludźmi stojącymi za irańskim programem nuklearnym. Biznesmen zdołał pozyskać bogaty zbiór wysoce poufnych dokumentów dotyczących tego programu i chciał przekazać je niemieckiej agencji wywiadowczej BND. „Delfin", jak nazwała biznesmena BND, planował posłużyć się tymi dokumentami w celu uzyskania azylu dla siebie i rodziny na Zachodzie. Jednak zanim zdążył zrealizować swój plan, irańscy agenci wywiadu aresztowali go. Jego żona i rodzina zdołali zbiec do Turcji, zabierając ze sobą dokumenty.

Gdy Heinonen czytał otrzymane dokumenty, nie mógł uwierzyć własnym oczom. W danych od „Delfina" bardzo spójnie opisana była seria projektów, które razem tworzyły celowo opracowany tajny program budowy broni atomowej. Obejmował on ambitne plany produkcji własnego paliwa nuklearnego z rudy uranu wydobywanej w kopalni w południowym Iranie, przetwarzania jej na koncentrat uranu (żółty uran) i przekształcania go w tetrafluorek i sześciofluorek uranu. Tetrafluorek uranu można wykorzystać do produkcji uranu metalicznego, który ma zastosowania cywilne, ale może też posłużyć do budowy bomb[21].

Samo w sobie nie było to dowodem na program budowy broni jądrowej. Jednak najbardziej alarmujące w materiałach od „Delfina" były dokumenty opisujące testy precyzji detonacji substancji silnie wybuchowych. Kobieta dostarczyła też szkice i instrukcje budowy pojazdów powrotnych dla irańskich pocisków Shahab-3, które mieściły ciężki okrągły obiekt podejrzanie podobny do głowic atomowych. Ponadto materiały obejmowały trzyminutowe nagranie przedstawiające symulowaną eksplozję głowicy na wysokości 600 m z rozbrzmiewającą w tle oklepaną ścieżką dźwiękową

[21] Broń nuklearna powstaje w wyniku uformowania uranu metalicznego w dwie półkule i umieszczenia ich w ładunku wybuchowym z detonatorami. Detonatory powinny spowodować równomierną i jednoczesną eksplozję, aby doprowadzić do zderzenia obu półkul i wywołania reakcji łańcuchowej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Vangelisa z filmu *Rydwany ognia*[22]. Heinonen stwierdził, że detonacja broni chemicznej lub biologicznej na tak dużej wysokości nie miała sensu, dlatego projektowana głowica musiała być przeznaczona do konstrukcji broni nuklearnej[23].

Czy przekazane dokumenty były autentyczne? Heinonen nie miał co do tego pewności, jednak materiały były zgodne z otrzymanymi przez MAEA od państw członkowskich innymi informacjami na temat poczynań Iranu. Jeśli Fin prawidłowo zinterpretował te dokumenty, były one najbardziej obciążającym z dotychczasowych dowodów na to, że Iran rzeczywiście prowadzi program budowy broni nuklearnej.

Później MAEA poinformowała irańskich urzędników o otrzymanych dokumentach i zażądała wyjaśnień. Urzędnicy stwierdzili jednak, że dokumenty opisujące testy materiałów wybuchowych mogą dotyczyć głowic konwencjonalnych. Ponadto zaprzeczyli projektowi produkcji tetrafluorku uranu. Oskarżyli MAEA o sfabrykowanie dokumentów w celu przeforsowania sankcji przeciw Iranowi i uzasadnienia nalotów Stanów Zjednoczonych i Izraela na zakłady w Natanzie[24].

Gdy wydawało się, że napięcie związane z programem nuklearnym nie może już bardziej wzrosnąć, Iran pod koniec 2004 r. zgodził się zawiesić plany przetwarzania uranu w Isfahanie i inne działania związane ze wzbogacaniem uranu oraz wznowić formalne rozmowy na temat programu nuklearnego. Porozumienie o wstrzymaniu prac szybko jednak zostało zerwane. W czerwcu 2005 r. Mahmud Ahmadineżad, burmistrz Teheranu,

---

[22] Iran w 1998 r. zbudował rakietę o zasięgu ok. 1450 km i w maju 2002 r. przeprowadził jej udane testy. Irańczycy pracowali też nad rakietą o zasięgu ok. 1900 km.

[23] Follath, Stark, *The Birth of a Bomb*.

[24] El-Baradei sprzeciwiał się upublicznieniu tych dokumentów, ponieważ MAEA nie mogła zweryfikować ich autentyczności, a w agencji wciąż pamiętano o wykorzystaniu przez Stany Zjednoczone nieprawdziwych dokumentów do uzasadnienia inwazji na Irak. Mimo to w kolejnych latach MAEA wielokrotnie naciskała na Irańczyków, by udostępnili opisane w dokumentach informacje o prowadzonych programach. W odpowiedzi na to Iran udostępniał niekompletne informacje lub w ogóle ich nie podawał. Niektóre informacje z opisywanych dokumentów trafiły później do ISIS. Zob. David Albright, Jacqueline Shire, Paul Brannan, „May 26, 2008 IAEA Safeguards Report on Iran: Centrifuge Operation Improving and Cooperation Lacking on Weaponization Issues", 29 maja 2008 (*http://isis-online.org/uploads/isis-reports/documents/ISIS_Iran_IAEA_Report_29May2008.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

został wybrany na prezydenta Iranu, a poparcie rządu dla wstrzymania prac i rozpoczęcia rozmów zaczęło maleć. Irański program nuklearny stał się kwestią dumy narodowej, a fundamentaliści w rządzie uznawali wstrzymanie go i rozmowy za kapitulację wobec Zachodu. Uważali, że żadne próby ugłaskania Zachodu nie wystarczą, ponieważ rzeczywistym — ich zdaniem — celem Izraela i Stanów Zjednoczonych jest obalenie irańskiego reżimu.

Gdy wojna w Iraku przeciągała się i Amerykanie tracili przewagę, irańscy przywódcy zaczęli otwarcie przeciwstawiać się ograniczeniom. W sierpniu 2005 r., zaledwie dwa miesiące po wyborze Ahmadineżada, w międzynarodowych rozmowach dotyczących programu nastąpił impas, a Iran ogłosił zerwanie porozumienia o wstrzymaniu prac[25]. Irańczycy bezzwłocznie zniszczyli plomby, które MAEA założyła na sprzęcie w Isfahanie na czas wstrzymania prac, i wznowili projekt przetwarzania tlenku uranu w sześciofluorek uranu. Sytuacja zmieniła się ze złej na jeszcze gorszą w grudniu, kiedy to Ahmadineżad wywołał burzę, publicznie stwierdzając, że Holocaust to mit[26].

Sprawy wymykały się spod kontroli. Sąsiedzi Iranu na Bliskim Wschodzie byli tak przestraszeni rosnącym napięciem między Iranem a Izraelem, że kuwejcki minister zdrowia zdecydował się zainstalować wzdłuż granic i w głębi kraju 15 systemów wykrywania promieniowania, aby móc uzyskać wczesne sygnały o aktywności nuklearnej w regionie[27]. Trudno było jednak ocenić, jak dużo brakuje Iranowi do zbudowania bomby. Nikt nie znał dokładnie stanu tajnego irańskiego programu. Iran nie musiał nawet budować broni atomowej, aby stać się zagrożeniem. Wystarczyło, by Irańczycy opanowali proces wzbogacania uranu i wyprodukowali ilość nisko wzbogaconego uranu wystarczającą do zbudowania bomby. Po dojściu do tego przełomowego poziomu Iran mógł pozostawać na nim w nieskończoność

[25] Muhammad el-Baradei przedstawił w swoich wspomnieniach obszerny opis tych negocjacji i wyjaśnił, dlaczego Irańczycy czuli się oszukani i jak uzasadnili zerwanie rozmów. Zob. *The Age of Deception: Nuclear Diplomacy in Treacherous Times*, Metropolitan Books, Nowy Jork 2011, s. 141 – 147.

[26] Karl Vick, *Iran's President Calls Holocaust „Myth" in Latest Assault on Jews*, „Washington Post", Foreign Service, 15 grudnia 2005.

[27] „06Kuwait71, Kuwait's Country Wide Radiation Monitoring System", depesza z ambasady amerykańskiej w Kuwejcie do Departamentu Stanu w Waszyngtonie, styczeń 2006. Opublikowane w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/06KUWAIT71_a.html*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i zgodnie z prawdą twierdzić, że nie posiada broni atomowej — aż do dnia, w którym zdecydowałby się przetworzyć wzbogacony uran na materiał zdatny do wykorzystania w broni i zbudować bombę. Pojawiły się różne szacunki co do tego, ile czasu zajmie Iranowi dotarcie do tego poziomu. W raporcie NIE z 2005 r. znalazły się szacunki, wedle których uzyskanie materiałów wystarczających do zbudowania bomby zajmie Irańczykom od sześciu do dziesięciu lat. Izrael oceniał sytuację mniej optymistycznie. Przedstawiciele tego kraju szacowali ten czas na pięć lat[28].

Wzbogacanie uranu to jeden z najtrudniejszych procesów w drodze do wyprodukowania broni jądrowej. Jest to skomplikowane i podatne na błędy przedsięwzięcie, a Iran miał w tym obszarze niewielkie doświadczenie. Jeśli dodać do tego trudności związane z produkcją działających wirówek, łatwo było zrozumieć, dlaczego dotarcie do obecnego etapu w irańskim programie zajęło tak dużo czasu. Wyglądało na to, że technicy w Natanzie wciąż mają problemy z wirówkami, o czym Ariel Levite, zastępca dyrektora naczelnego Izraelskiej Komisji Energii Atomowej, poinformował Stany Zjednoczone na początku 2006 r. Później okazało się, że niektóre problemy były efektem sabotażu komponentów pozyskanych przez Iran od Turcji[29].

Mimo przeszkód na początku 2006 r. Iran wznowił wzbogacanie uranu w pilotażowym zakładzie w Natanzie. To posunięcie sprawiło, że urzędnicy izraelscy zrewidowali wcześniejsze szacunki i stwierdzili, że Irańczycy będą gotowi do budowy broni jądrowej za dwa – cztery lata[30]. Ostrzegali Amerykanów, że Iranowi nie można pozwolić na opanowanie procesu wzbogacania uranu, inaczej będzie to „początek końca". Iran po opracowaniu

[28] Autorem tych szacunków był Ariel (Eli) Levite, zastępca dyrektora generalnego Izraelskiej Komisji Energii Atomowej. Znalazły się one w depeszy Departamentu Stanu USA przesłanej z ambasady w Tel Awiwie we wrześniu 2005 r. Dokument został opublikowany w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/05TELAVIV5705_a.html*.

[29] „06TelAviv293, Iran: Congressman Ackerman's January 5 Meeting at", depesza Departamentu Stanu USA z ambasady amerykańskiej w Tel Awiwie, styczeń 2006. Dokument został opublikowany w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/06TELAVIV293_a.html*. Wyjaśnienie problemów znajdziesz na s. 209 tej książki.

[30] W prywatnych rozmowach Izraelczycy i Rosjanie poinformowali Amerykanów, że ich zdaniem Iran może przezwyciężyć problemy ze wzbogacaniem uranu w sześć miesięcy. Zob. „06Cairo601, Iran; Centrifuge Briefing to Egyptian MFA", depesza Departamentu Stanu USA, luty 2006. Dokument został opublikowany w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/06CAIRO601_a.html*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

tego procesu mógł wzbogacać uran w tajnych zakładach w dowolnym miejscu kraju[31]. Zakłady z wirówkami, w odróżnieniu od obiektów związanych z innymi etapami produkcji paliwa, nie wymagały specjalnych kompleksów. Dlatego technicy po rozwiązaniu wszystkich problemów w procesie mogli ukryć kaskady wirówek w dowolnym miejscu, nawet w przekształconych budynkach biurowych. „Wiemy, że Iran obecnie przenosi lokalizację programu" — ostrzegał Amerykanów na początku 2006 r. Gideon Frank, dyrektor naczelny Izraelskiej Komisji Energii Atomowej[32]. Stwierdził, że fabryki do produkcji części wirówek już znajdują się „w wielu miejscach", a inne prace związane z programem nuklearnym są realizowane w mocno ufortyfikowanych kompleksach wojskowych, których inspektorzy MAEA nie mogą kontrolować. Niektóre kompleksy były ukryte pod ziemią, dlatego ataki z powietrza byłyby wobec nich nieskuteczne.

W maju irańscy urzędnicy ogłosili, że technicy w pilotażowym zakładzie wzbogacania w Natanzie z sukcesem wzbogacili pierwszą porcję uranu do 3,5%, wykorzystując kompletną kaskadę obejmującą 164 wirówki. W kolejnym komunikacie poinformowano, że technicy wreszcie rozpoczęli instalowanie pierwszych 3000 wirówek w jednej z dużych podziemnych hal. Wydawało się, że Irańczycy w końcu przezwyciężyli trudności i że nic oprócz nalotów nie zdoła ich powstrzymać.

MAEA, zaniepokojona nagłymi trudnościami z kontrolą irańskiego programu nuklearnego, ogłosiła, że Iran nie przestrzega porozumień o zabezpieczeniach. Stany Zjednoczone nalegały na wydanie takiego ogłoszenia od lat. Rada Bezpieczeństwa ONZ-etu w lipcu 2006 r. przyjęła rezolucję, w której pod groźbą sankcji domagała się od Iranu wstrzymania wzbogacania uranu z końcem sierpnia. Ahmadineżad odmówił. „Ci, którzy myślą, że mogą posługiwać się wobec Iranu językiem gróźb i siły, są w błędzie — powiedział. — Jeśli jeszcze nie zdają sobie z tego sprawy, pewnego dnia przekonają się o tym w dotkliwy sposób"[33].

Wywiad państw zachodnich zauważył, że Irańczycy zintensyfikowali próby potajemnego zakupu komponentów do wirówek w Europie i na innych

[31] „06TelAviv688, Iran-IAEA: Israeli Atomic Energy Commission", depesza Departamentu Stanu USA, luty 2006. Dokument został opublikowany w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/06TELAVIV688_a.html*.

[32] *Ibid.*

[33] „Iran Defiant on Nuclear Deadline", BBC News, 1 sierpnia 2006. Ten tekst jest dostępny na stronie: *http://news.bbc.co.uk/2/hi/5236010.stm*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

rynkach, korzystając z sieci zagranicznych i lokalnych firm przykrywek[34]. „Chcieli kupować jak szaleni" — wspomina David Albright z ISIS. Interesowały ich zawory, rurki, sprzęt próżniowy, a także komponenty, które można wykorzystać do produkcji pocisków[35].

Pojawiły się plotki na temat nalotów, jednak w prywatnej rozmowie sekretarz stanu Condoleezza Rice poinformowała el-Baradeia z MAEA, że jej zdaniem do tego nie dojdzie. Uważała, że Iran z pewnością się ugnie. Jednak Iran tego nie robił.

Pod koniec 2006 r. Rada Bezpieczeństwa ONZ-etu nie miała innego wyboru jak zrealizować swoje groźby. Przyjęła rezolucję nakładającą sankcje na Iran, zakazującą sprzedaży temu państwu materiałów i technologii związanych z energią atomową. Kilka miesięcy później przegłosowano dalsze sankcje, aby zamrozić zasoby ludzi i organizacji podejrzanych o zaangażowanie w program nuklearny[36]. Mimo to Iran pozostawał nieugięty.

W lutym 2007 r. irańscy urzędnicy poinformowali MAEA, że technicy w Natanzie rozpoczęli instalowanie pierwszych wirówek w jednej z podziemnych hal. Dojście do tego etapu zajęło Irańczykom ponad dziesięć lat, jednak ostatecznie pokonali wszystkie przeszkody (technologiczne i będące dziełem człowieka), które stały im na drodze. Teraz już nic nie utrudniało technikom zainstalowania dwóch kaskad w jednej z podziemnych hal do końca miesiąca. Dwie dalsze kaskady były też prawie gotowe. Ponadto Iran przetransportował do hal 9 t sześciofluorku uranu w celu rozpoczęcia wzbogacania[37].

---

[34] „07Berlin1450, Treasury Under Secretary Levey Discusses Next", depesza Departamentu Stanu USA z ambasady w Berlinie, lipiec 2007. Ten dokument został opublikowany w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/07BERLIN1450_a.html*. W depeszy wymienionych jest przynajmniej 30 irańskich firm przykrywek utworzonych w celu zakupów komponentów. Innym źródłem tych danych jest wywiad autorki z Davidem Albrightem ze stycznia 2012 r.

[35] Albright, *Peddling Peril*, s. 200 – 201.

[36] Rada Bezpieczeństwa ONZ-etu nałożyła sankcje ekonomiczne na Iran w grudniu 2006 r. W marcu 2007 r. rada jednogłośnie przegłosowała zamrożenie środków finansowych 28 Irańczyków powiązanych z programami nuklearnymi i wojskowymi.

[37] Gdy sytuacja w Iranie była najbardziej napięta, Korea Północna przeprowadziła test urządzenia nuklearnego. Pogarszające się na wielu frontach bezpieczeństwo atomowe spowodowało, że 17 stycznia 2007 r. organizacja Bulletin of Atomic Scientists przesunęła wskazówkę minutową jej słynnego zegara zagłady o dwie minuty bliżej północy (z siedmiu minut przed północą na pięć).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Do czerwca 2007 r. w Natanzie zostało zainstalowanych 1400 wirówek, które zaczęły wzbogacać uran. Wszystkie te wirówki były typu IR-1, jednak technicy zaczęli także produkcję modelu IR-2, bardziej zaawansowanych urządzeń opartych na projekcie pakistańskich P-2. Iran wznowił prace nad modelem IR-2 po początkowych niepowodzeniach w produkcji wirników[38]. Próbował też zbudować jeszcze bardziej zaawansowane wirówki IR-4[39].

Napięcie między Stanami Zjednoczonymi a Izraelem rosło. Izrael oskarżał Amerykanów o brak zdecydowanych kroków w kwestii irańskiego programu nuklearnego oraz zbytnią ufność w sankcje i działania dyplomatyczne. Ehud Olmert, premier Izraela, publicznie ostrzegł, że jeśli irański program nie zostanie zatrzymany, Izrael sam podejmie odpowiednie kroki. „Każdy, kto nam zagraża, kto zagraża naszemu istnieniu, musi wiedzieć, że mamy determinację i środki potrzebne do tego, by się obronić — powiedział. — Mamy prawo do podjęcia wszelkich działań w obronie naszych żywotnych interesów i nie zawahamy się z niego skorzystać"[40].

Jednak w grudniu 2007 r. wydarzyło się coś, co zaszkodziło nie tylko dyplomatycznym działaniom Stanów Zjednoczonych, ale też izraelskim planom ataku. Tego miesiąca pojawił się raport NIE z zaskakującymi informacjami na temat irańskiego programu nuklearnego. Stwierdzono z „dużą pewnością", że Iran w przeszłości prowadził już program budowy broni nuklearnej, jednak wstrzymał go jesienią 2003 r. po przeprowadzonej pod dowództwem Amerykanów inwazji na Irak. To wskazywało na to, że Iran był „w mniejszym stopniu zdeterminowany w kwestii budowy broni nuklearnej", niż wcześniej uważano. Raporty NIE, koordynowane przez biuro dyrektora Wywiadu Narodowego, są oparte na informacjach otrzymanych od wywiadów amerykańskiego i z innych krajów. Najnowsze informacje były jednak sprzeczne z tym, co adm. Michael McConnell, dyrektor Wywiadu Narodowego, mówił komisji senackiej zaledwie kilka miesięcy wcześniej.

---

[38] Z powodu kontroli eksportu i innych trudności z produkcją wirników ze stali maraging, czego wymagał projekt wirówek, Iran w 2002 r. zrezygnował z produkcji modelu IR-2. Jednak irańscy naukowcy zmodyfikowali projekt, wprowadzając wirniki z włókna węglowego, i po 2004 r. wznowili prace nad tym modelem.

[39] Collins, Frantz, *Fallout*, s. 259.

[40] „Prime Minister Ehud Olmert's Address at the 2007 Herzliya Conference", 24 stycznia 2007. Angielskie tłumaczenie jest dostępne na stronie: *http://pmo.gov.il/English/MediaCenter/Speeches/Pages/speechher240107.aspx*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Oceniamy, że Teheran dąży do zbudowania broni nuklearnej i jest bardziej zainteresowany zerwaniem negocjacji niż dojściem do akceptowalnego rozwiązania dyplomatycznego" — powiedział Senackiej Komisji Sił Zbrojnych w lutym 2007 r.[41].

Choć w raporcie NIE napisano też, że Iran może w każdej chwili wznowić program budowy broni, a w utajnionej wersji dokumentu znalazły się nieobecne w upublicznionych informacjach dowody (wedle których w Iranie nadal mogło działać kilkanaście tajnych obiektów jądrowych prowadzących niedozwolone prace nad wzbogacaniem uranu i budową broni), raport zmniejszał przesłanki do nakładania sankcji przeciw Iranowi i podejmowania akcji militarnych[42]. Robert Gates, sekretarz obrony Stanów Zjednoczonych, sprzeciwiał się nalotom, jednak zakwestionował wnioski płynące z raportu. W trakcie prowadzonej w Kongresie dyskusji nad raportem ostrzegł, że Iran jest zaangażowany w podejrzane transakcje wskazujące na to, że plany tego kraju są dużo bardziej uporządkowane i ukierunkowane, niż wynika to z raportu NIE. Gates nie był jedyną osobą niezgadzającą się z wnioskami z raportu. W prywatnych rozmowach urzędnicy niemieccy poinformowali Stany Zjednoczone, że według wywiadu niemieckiego Iran nadal realizuje program budowy broni jądrowej. Z kolei izraelscy oficjele donieśli, że wedle ich informacji Iran wprawdzie wstrzymał program w 2003 r., ale wznowił go w 2005[43].

---

[41] *McConnell Fears Iran Nukes by 2015*, „Washington Times", 27 lutego 2007.

[42] Oto słowa z gazety „New York Times": „Rzadko, jeśli kiedykolwiek, zdarza się, że jeden raport wywiadu tak całkowicie, nagle i niespodziewanie zmienia przebieg dyskusji w obszarze polityki zagranicznej". Stwierdzono, że raport „z pewnością zmniejszy międzynarodowe poparcie na rzecz zaostrzenia sankcji przeciw Iranowi, […] i ponownie wzbudzi wątpliwości co do wiarygodności krytykowanych amerykańskich agencji wywiadowczych". Steven Lee Myers, *An Assessment Jars a Foreign Policy Debate About Iran*, „New York Times", 4 grudnia 2007.

[43] Rolf Nikel, zastępca doradcy ds. bezpieczeństwa narodowego Niemiec, na początku 2008 r. poinformował urzędników amerykańskich, że opisywany tu raport NIE skomplikował próby przekonania niemieckiej opinii publicznej i niemieckich firm do zasadności sankcji przeciw Iranowi (według depeszy Departamentu Stanu USA z lutego 2008 r., opublikowanej w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/08BERLIN180_a.html*; zob. też *https://wikileaks.org/plusd/cables/07BERLIN2157_a.html*). Jeśli chodzi o komentarze Izraela, to według depeszy Departamentu Stanu USA opublikowanej w serwisie WikiLeaks w maju 2009 r. szef wywiadu Sił Obronnych Izraela, gen. Amos Yadlin,

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Pod koniec 2007 r. w Natanzie zainstalowanych było 3000 wirówek. W następnym roku Iran planował podwoić tę liczbę. Eksperci szacowali, że już 3000 wirówek P-1 w niecały rok wyprodukuje ilość nisko wzbogaconego uranu wystarczającą do budowy bomby, jeśli Iran zdecyduje się dodatkowo wzbogacić uzyskany materiał[44].

Wyglądało na to, że nie da się nic zrobić, aby powstrzymać program wzbogacania uranu bez ryzykowania wojny.

A może jednak?

Gdy napięcie związane z programem wzbogacania uranu dochodziło do niebezpiecznego poziomu, w sekrecie realizowany był nowy plan. Irańscy technicy gratulowali sobie postępów poczynionych w Natanzie i przygotowywali się do rozszerzenia działań, gdy tymczasem po cichu uruchomiono wycelowaną w komputery z zakładu cyfrową broń z jasno określoną misją. Na jej celowniku znajdowały się setki szybko obracających się wirówek. Ta precyzyjna broń ukradkiem, ale zdecydowanie zmierzała prosto do celu.

przekazał je w rozmowie z kongresmenem Robertem Wexlerem. Opisany raport NIE miał też inne skutki. Niemiecko-irański handlarz Mohsen Vanaki był sądzony w Niemczech za przemyt do Iranu sprzętu o podwójnych zastosowaniach. Vanaki został oskarżony w czerwcu 2008 r. na mocy ustawy o kontroli broni i ustawy o handlu zagranicznym. Jednak oskarżony w swojej obronie powiedział, że nie mógł dostarczać Iranowi sprzętu do programu budowy broni nuklearnej, ponieważ według raportu NIE Iran nie prowadził takich prac. Wszystkie zarzuty przeciw Vanakiemu zostały odrzucone, w dużej części z powodu raportu NIE z 2007 r. Prokuratorzy wnieśli jednak odwołanie i w 2009 r. odrzucenie zarzutów zostało oddalone. Później Vanaki został skazany, w dużej mierze na podstawie informacji wywiadu BND o podejrzanych transakcjach dokonanych przez jednostki powiązane z irańskim wojskiem.

[44] International Institute for Strategic Studies, *Iran's Strategic Weapons Programmes: A Net Assessment*, Routledge, Londyn 2005, s. 33.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 6

W POSZUKIWANIU EKSPLOITÓW TYPU ZERO-DAY

Był piątkowy wieczór pod koniec sierpnia. Liam O'Murchu świętował swoje 33. urodziny w eleganckim barze na dachu w Venice w stanie Kalifornia. Zarezerwował część mającego kształt litery U baru pod gołym niebem na dachu hotelu Erwin. Rozpościerał się stamtąd widok na Pacyfik. Badacz razem ze swoją dziewczyną, kilkunastoma przyjaciółmi oraz przybyłymi z Irlandii siostrą i szwagrem raczyli się piwem i koktajlami. Jak to często zdarza się w południowej Kalifornii, ekipa *reality show* filmowała siedzącą nieopodal parę, przechodzącą niezręczne chwile na „prywatnej" randce.

Goście O'Murchu znajdowali się w barze już od trzech godzin, gdy ok. dziewiątej wieczorem pojawił się Eric Chien. Nie w głowie mu jednak były imprezy. Nie mógł się doczekać, by pokazać przyjacielowi i współpracownikom e-mail, jaki wcześniej tego dnia pojawił się na liście dyskusyjnej dotyczącej zabezpieczeń. Miał jednak wątpliwości, czy od razu dzielić się informacjami. Wiedział, że gdy O'Murchu zobaczy ten list, nie będzie mógł przestać o nim myśleć. „Coś ci pokażę — powiedział Chien do O'Murchu. — Ale przez resztę wieczoru nie będziemy o tym rozmawiać, zgoda?". O'Murchu potaknął.

Chien wyciągnął telefon BlackBerry i wyświetlił e-mail z uwagami od badacza z innej firmy antywirusowej. Badacz sugerował, że w Stuxnecie mogą być ukryte inne eksploity typu zero-day. O'Murchu spojrzał na Chiena.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Pracowali nad Stuxnetem od tygodni, próbując za pomocą inżynierii odwrotnej otrzymać komponenty robaka. Natrafili na kilka wskazówek sugerujących, że w kodzie mogą być schowane inne eksploity typu zero-day, jednak nie mieli czasu się nimi zająć. Wskazówki znajdowały się w „pocisku" odpowiedzialnym za rozprzestrzenianie Stuxneta, natomiast badacze koncentrowali się na ładunku, czyli na części kodu atakującej oprogramowanie i sterowniki PLC Siemensa.

Wspomniany e-mail był mało szczegółowy. Nie było jasne, czy jego autor *znalazł* nowe eksploity typu zero-day w Stuxnecie, czy tylko natrafił na te same wskazówki, które odkryli badacze z Symanteca. Niezależnie od tego obudziło to w O'Murchu ducha rywalizacji. „Wystarczy — powiedział do Chiena. — Dziś więcej nie piję". Następnego ranka, w sobotę, O'Murchu wrócił do biura i do analizowania Stuxneta.

Biuro było opustoszałe, dlatego nikt nie zakłócał O'Murchu pracy. Zespół z Symanteca przed zajęciem się ładunkiem przeanalizował już większość „pocisku" Stuxneta, dlatego teraz wystarczyło starannie przejrzeć kod pod kątem eksploitów. Nie było to jednak proste. Eksploity typu zero-day nie są czymś, co można łatwo znaleźć w kodzie szkodliwego pliku. Trzeba sprawdzić w kodzie wszystkie referencje prowadzące do systemu operacyjnego lub innych aplikacji, aby wykryć podejrzane interakcje. Czy Stuxnet wymuszał na jakiejś aplikacji wykonywanie niedozwolonych operacji? A może przeskakiwał bariery ochronne lub obchodził uprawnienia systemowe? Po zastosowaniu inżynierii odwrotnej badacze otrzymali „pocisk" składający się z tysięcy wierszy kodu, z których każdy trzeba było przeanalizować pod kątem podejrzanych operacji.

Stuxnet nie miał struktury liniowej, co utrudniało próby prześledzenia jego działania. Kod pomijał niektóre polecenia i przeskakiwał do innych, a O'Murchu musiał obserwować wszystkie te kroki.

Jednak po mniej więcej godzinie badacz był prawie pewien, że dotarł do drugiego eksploita. Przeszukał archiwum, aby ustalić, czy dana luka została już wcześniej wykorzystana. Nie znalazł takich przypadków. Następnie przetestował eksploit na maszynie z zainstalowaną najnowszą wersją systemu Windows, by się upewnić, że się nie pomylił. Rzeczywiście, Stuxnet wykorzystywał lukę typu zero-day w pliku klawiatury systemu Windows, aby uzyskać na komputerze podwyższone uprawnienia.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Eksploity typu zero-day są cenne, a wykorzystanie ich dwóch w jednym ataku i ryzykowanie, że oba zostaną wykryte, wydawało się O'Murchu dziwnym marnotrawstwem zasobów. Nie zaprzestał jednak analiz. Udokumentował swoje odkrycia i wrócił do kodu.

Po kilku godzinach uznał, że znalazł jeszcze jeden eksploit. W kodzie widoczne były oznaki, że Stuxnet wykorzystuje lukę w programie drukującym w systemie Windows, aby rozprzestrzeniać się między maszynami współużytkującymi drukarkę. O'Murchu jeszcze raz przetestował eksploit w komputerze i bez powodzenia próbował znaleźć w archiwum dowody na to, że luka została już wcześniej wykorzystana. Ponownie poczuł mrowienie, które pojawiło się tygodnie wcześniej. Udokumentował odkrycia i wrócił do kodu, aby kontynuować poszukiwania.

Gdy po południu Chien przyjechał do biura, aby sprawdzić, jak idzie praca O'Murchu, ten miał mętne spojrzenie i potrzebował przerwy. Irlandczyk przekazał swoje odkrycia Chienowi, który kontynuował analizowanie kodu do wieczora. Obaj badacze pracowali nad kodem także w niedzielę i do końca tygodnia, ku swemu zaskoczeniu, odkryli trzy eksploity typu zero-day. To, w połączeniu ze znalezionym wcześniej eksploitem luki związanej z plikami .LNK, dawało cztery eksploity typu zero-day zastosowane w jednym ataku[1].

Badacze uważali, że to szaleństwo. Już jeden eksploit typu zero-day był wystarczająco niebezpieczny. Dwa były przesadą. Ale cztery? Kto mógł zrobić coś takiego? I po co? Oznaczało to zmarnowanie cennych eksploitów. Zaawansowany błąd i eksploit typu zero-day można było sprzedać za 50 tys. dolarów lub więcej przestępcom na czarnym rynku i za nawet dwukrotność tej kwoty rządowym cyberarmiom i szpiegom na szarym rynku. Albo napastnicy mieli do dyspozycji nieograniczoną liczbę eksploitów typu zero-day i nie przejmowali się utratą kilku z nich, albo byli zdesperowani

[1] Czwarty z wykrytych eksploitów atakował lukę w harmonogramie zadań w systemie Windows. Ten eksploit, w połączeniu z eksploitem związanym z klawiaturą, służył do zapewnienia Stuxnetowi wyższych uprawnień w maszynie. Gdy konto użytkownika miało ograniczone uprawnienia, uniemożliwiające Stuxnetowi instalację plików lub wykonanie innych operacji, dwa wymienione eksploity zdobywały uprawnienia systemowe (administracyjne). Dzięki temu Stuxnet mógł wykonywać dowolne zadania, a system nie wyświetlał ostrzeżeń ani nie pytał rzeczywistego administratora o zgodę.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i mieli naprawdę dobre powody do tego, by zapewnić swojemu złośliwemu oprogramowaniu możliwości gwarantujące dotarcie do celu. Chien i O'Murchu podejrzewali, że oba te wyjaśnienia mogą być prawdziwe.

Chien skontaktował się z Microsoftem, aby zgłosić nowe eksploity typu zero-day, ale dowiedział się, że rosyjska firma Kaspersky Lab zrobiła to wcześniej. Wkrótce po pojawieniu się informacji o Stuxnecie firma Kaspersky utworzyła dziesięcioosobowy zespół w celu przeanalizowania „pocisku". Po kilku dniach badacze znaleźli drugi eksploit typu zero-day, a tydzień później trzeci i czwarty. Wtedy zgłosili luki Microsoftowi, który aktualnie pracował nad łatkami. Zgodnie z regułami odpowiedzialnego ujawniania informacji firma Kaspersky nie mogła upublicznić swoich odkryć do czasu załatania przez Microsoft luk w oprogramowaniu[2].

Cztery eksploity typu zero-day w Stuxnecie były zdumiewające, ale nie był to jeszcze koniec historii. W trakcie weekendowego maratonu z kodem Chien i O'Murchu znaleźli cztery dodatkowe sposoby rozprzestrzeniania się Stuxneta (bez użycia luk typu zero-day), co dawało w sumie osiem różnych metod powielania się robaka. Kod użyty do ataku zawierał „szwajcarski scyzoryk" z różnymi narzędziami pozwalającymi Stuxnetowi dostawać się do systemów i rozprzestrzeniać.

Najważniejsza technika polegała na infekowaniu plików projektów w narzędziu Step 7 używanym przez programistów do programowania sterowników PLC. Stuxnet wykorzystywał nazwę użytkownika (*winccconnect*) i hasło (*2WSXcder*) zapisane przez firmę Siemens na stałe w tym narzędziu[3]. System Step 7 stosował te dane do uzyskiwania automatycznego dostępu do używanej na zapleczu bazy danych, gdzie napastnicy wstrzykiwali kod w celu zainfekowania maszyny przechowującej tę bazę. Była to współużytkowana baza, z której mogli korzystać wszyscy programiści pracujący nad

[2] Firmy Microsoft i Kaspersky Lab zaczęły publikować informacje o trzech innych lukach typu zero-day w połowie września.

[3] Zapisane na stałe hasło jest umieszczane przez producenta oprogramowania w kodzie, tak aby system mógł wykonywać niektóre operacje automatycznie, bez konieczności wprowadzania hasła przez użytkownika. Zmiana takiego hasła często skutkuje problemami w systemie. Jednak zapisane na stałe hasła są zagrożeniem dla bezpieczeństwa, ponieważ oznaczają, że w każdym systemie używane jest to samo hasło, a napastnik może je ustalić, czytając kod.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

projektami w narzędziu Step 7. Stuxnet mógł więc zainfekować maszynę dowolnego programisty, który używał tej bazy. Ta technika infekcji zwiększała prawdopodobieństwo, że Stuxnet dotrze do sterownika PLC, gdy programista podłączy laptopa do maszyny zawierającej taki sterownik lub włoży do niej pendrive'a. Napastnicy wykorzystali lukę w rzadko używanej funkcji systemu Step 7, aby zainfekować pliki projektów w tym narzędziu. Wskazywało to, że dobrze znali system stosowany przez nieliczne osoby. Była to następna oznaka wysokich umiejętności napastników[4].

Oprócz mechanizmów rozprzestrzeniania kodu Stuxnet obejmował komponent P2P, który umożliwiał aktualizowanie starszych wersji robaka nowymi. Dzięki temu można było aktualizować Stuxneta zdalnie na komputerach, które nie były bezpośrednio podłączone do internetu, ale łączyły się z innymi maszynami w sieci lokalnej. Na potrzeby rozsyłania aktualizacji Stuxnet na każdej zainfekowanej maszynie instalował serwer wymiany plików i klienta. Maszyny z tej samej sieci lokalnej mogły kontaktować się ze sobą w celu porównywania wersji Stuxneta. Jeśli na jednej z maszyn znajdowała się nowsza wersja, aktualizowała ona pozostałe. W celu zaktualizowania wszystkich komputerów z sieci lokalnej napastnicy musieli przesłać aktualizację tylko na jedną z nich, a pozostałe pobierały nową wersję.

Zestaw metod zastosowanych do rozsyłania Stuxneta dowodził, że napastnikom bardzo zależało na rozprzestrzenieniu ich złośliwego oprogramowania. Jednak, w odróżnieniu od większości złośliwego oprogramowania, rozprzestrzeniającego się za pomocą e-maili lub szkodliwych witryn na tysiące maszyn jednocześnie, żaden z eksploitów ze Stuxneta nie

[4] Chien i O'Murchu dowiedzieli się więcej o tej mało znanej luce z systemu Step 7 dzięki konsultacjom z ekspertami od systemów kontroli (jednym z nich był Eric Byres z Tofino Security, posiadający bogatą wiedzę na temat oprogramowania Siemensa). Ta luka wynikała z tego, że pliki miały umożliwiać programistom dodawanie do plików projektów Siemensa czegoś więcej niż prostych danych. Technicznie nie była to luka, tylko funkcja, ponieważ Siemens celowo dodał tę możliwość do projektu plików. Jednak Stuxnet wykorzystał ją do umieszczania w plikach własnych bibliotek .DLL. Samo to nie wystarczało jednak, aby mógł zainfekować system po otwarciu pliku projektu. Stuxnet musiał też modyfikować ważne fragmenty pliku projektu, w tym dane konfiguracyjne, aby mieć pewność, że biblioteka .DLL zostanie załadowana w maszynie, w której taki plik zostanie otwarty.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

korzystał z internetu[5]. Zamiast tego napastnicy liczyli na to, że ktoś przeniesie robaka z jednego komputera na inny za pomocą pendrive'a lub że Stuxnet, po zainfekowaniu jednej maszyny, będzie rozprzestrzeniał się w sieci lokalnej. Na tej podstawie można było wywnioskować, że chcieli dotrzeć do systemów, o których wiedzieli, że nie są podłączone do internetu. Niespotykana liczba zastosowanych eksploitów typu zero-day wskazywała na to, że cel był ważny i dobrze zabezpieczony.

Jednak ta pośrednia próba dotarcia do celu była skomplikowaną i nieprecyzyjną techniką ataku. To tak, jakby ktoś zaraził jedną z żon Osamy bin Ladena śmiertelnym wirusem w nadziei, że przeniesie go ona na byłego lidera Al-Kaidy. Wirus z pewnością zainfekowałby też inne osoby, co zwiększało ryzyko ujawnienia akcji. Właśnie to stało się ze Stuxnetem. Znalazł się on na tak wielu przypadkowych maszynach, że wystąpienie problemów i wykrycie go było tylko kwestią czasu.

Gdy Chien przeglądał długą listę metod i eksploitów zastosowanych przez napastników, zauważył, że użyte techniki były nieprzypadkowe. Każda realizowała inne zadanie i przezwyciężała inne przeszkody, które napastnicy musieli pokonać, aby osiągnąć cel. Wyglądało to tak, jakby ktoś opracował „listę zakupów" z eksploitami potrzebnymi do ataku (coś do zwiększania uprawnień, coś do rozprzestrzeniania się w sieci ofiary, coś do umieszczania ładunku w sterownikach PLC), a następnie zlecił komuś

[5] Siódma metoda rozprzestrzeniania Stuxneta wykorzystywała udziały sieciowe. Robak infekował zasoby i pliki współużytkowane przez wiele komputerów w sieci lokalnej. Ósmą metodą był eksploit atakujący dwuletnią lukę w systemie Windows, którą Microsoft już wyeliminował. Była to luka, którą wcześniej, w listopadzie 2008 r., wykorzystał Conficker. Microsoft usunął ją w październiku 2008 r., po tym jak chińscy hakerzy po raz pierwszy zastosowali ją do rozprzestrzeniania konia trojańskiego. Microsoft udostępnił rzadką, ponadplanową łatkę dla tej luki, gdy okazało się, że problem można łatwo wykorzystać do rozprzestrzeniania się robaka (ponadplanowe łatki są wypuszczane z wyprzedzeniem względem standardowego harmonogramu udostępniania poprawek; dzieje się tak, gdy luka jest poważna). Niestety, twórcy Confickera mieli tego świadomość i nie marnując czasu, wypuścili swojego robaka w następnym miesiącu. Choć Microsoft udostępniał już wtedy potrzebną łatkę, twórcy Confickera założyli, że wielu użytkowników nie zaktualizuje komputerów. Było to słuszne założenie. Mniej więcej jedna trzecia komputerów z systemem Windows nie miała zainstalowanej łatki, a do kwietnia 2009 r. Conficker zainfekował miliony takich maszyn. Gdy dwa miesiące później wypuszczony został Stuxnet, napastnicy przyjęli to samo założenie. Jednak w Stuxnecie ten eksploit był używany tylko w określonych warunkach. Nie była to podstawowa metoda rozprzestrzeniania tego robaka.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

zakup lub zbudowanie ich. Był to następny dowód na to, jak starannych planów i organizacji wymagał atak.

Spośród wszystkich eksploitów i metod zastosowanych przez hakerów najważniejsze dla ataku były eksploit luki związanej z plikami .LNK i infekowanie plików projektów w narzędziu Step 7. To te elementy zwiększały prawdopodobieństwo dotarcia Stuxneta do ostatecznego celu — sterowników PLC Siemensa. Programiści sterowników PLC często piszą kod na stacjach roboczych podłączonych do internetu, ale bez połączenia z siecią produkcyjną lub sterownikami PLC w hali fabrycznej. Aby przenieść kod do sterownika PLC, ktoś musi przesłać dane za pomocą laptopa podłączonego kablem bezpośrednio do sterownika lub podłączyć pendrive'a do programatora Field PG (jest to laptop z systemem Windows używany jako kontroler przemysłowy). Programatory Field PG nie są podłączone do internetu, ale są połączone z siecią produkcyjną i sterownikami PLC. Dzięki zainfekowaniu plików projektów w narzędziu Step 7 i umożliwieniu Stuxnetowi przeskakiwania między maszynami w pendrive'ach napastnicy sprawili, że każdy inżynier stał się potencjalnym nośnikiem ich broni.

Gdy Chien i O'Murchu udokumentowali wszystkie eksploity i luki używane przez Stuxneta do rozpowszechniania się, zwrócili uwagę na jeszcze jedną kwestię. Kilka technik zostało zastosowanych już wcześniej. Choć firma VirusBlokAda uznała, że do tej pory nikt nie wykorzystał luki związanej z plikami .LNK, Microsoft odkrył inny atak z użyciem podobnego eksploita w październiku 2008 r. Ten eksploit został zastosowany przez przestępców w celu instalowania jednej z wersji konia trojańskiego Zlob na maszynach ofiar[6]. Choć różne skanery antywirusowe potrafiły wykryć tego trojana, nie reagowały na powiązany z nim eksploit typu zero-day. Dzięki

[6] Zlob wyświetlał na zainfekowanych maszynach okno dialogowe wyglądające jak prawdziwy alert Microsoftu. W oknie ostrzegał, że maszyna została zainfekowana, i zachęcał do kliknięcia odnośnika do programu antywirusowego. Jednak pobrany program był złośliwym oprogramowaniem typu backdoor (czyli „tylna furtka"), które umożliwiało napastnikowi wykonywanie na zainfekowanych maszynach różnych operacji. Eksploit wykorzystujący pliki .LNK był pomysłowy, ale mało przydatny twórcom Zloba i innym cyberprzestępcom, których celem było zainfekowanie jak największej liczby maszyn w krótkim czasie. Ten eksploit rozprzestrzeniał złośliwe oprogramowanie powoli, ponieważ wymagał przeniesienia pendrive'a z jednej maszyny do drugiej. Dla twórców Zloba lepszym rozwiązaniem było użycie eksploita, który może zainfekować tysiące maszyn przez internet.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

temu Stuxnet mógł wykorzystać tę samą lukę. Także eksploit programu drukującego pojawił się już wcześniej, opisany w kwietniu 2009 r. w polskim magazynie poświęconym zabezpieczeniom. W artykule przedstawione zostały luka i kod źródłowy potrzebny do jej wykorzystania[7]. Informacje o tej luce nie dotarły wówczas do Microsoftu, dlatego firma nie rozwiązała problemu. Również zapisane na stałe hasło Siemensa zostało już ujawnione, gdy ktoś opublikował je w internecie na forum użytkowników produktów tej firmy w kwietniu 2008 r.[8].

Chien i O'Murchu zastanawiali się, czy zespół ludzi śledził fora hakerów i witryny poświęcone zabezpieczeniom pod kątem informacji o lukach i eksploitach, które twórcy Stuxneta mogliby zastosować w ataku, czy też może napastnicy zakupili gotowe eksploity od pośredników.

Co dziwne, spośród wszystkich eksploitów zastosowanych w Stuxnecie tylko ten wykorzystujący program drukujący pojawił się w pierwszej wersji ataku (z 2009 r.). Pozostałe po raz pierwszy zostały użyte w ataku z marca 2010 r., który wymknął się spod kontroli[9]. Wersja Stuxneta z 2009 r. rozprzestrzeniała się za pomocą pendrive'ów i wykorzystywała sztuczkę z mechanizmem automatycznego uruchamiania w systemie Windows[10]. Wcześniej zostało wyjaśnione, że mechanizm ten można wyłączyć, aby zablokować złośliwe oprogramowanie. Dlatego gdy w marcu 2010 r. pojawiła się następna

---

[7] Carsten Kohler, *Print Your Shell*, „Hakin9", 1 kwietnia 2009.

[8] To hasło zostało podane w kwietniu 2008 r. przez osobę o pseudonimie Cyber, gdy inny użytkownik narzekał, że jego system Siemensa przestał działać po zmianie zapisanego na stałe domyślnego hasła. Użytkownik nie mógł przypomnieć sobie oryginalnego hasła, dlatego Cyber zamieścił je w internecie. Hasło zostało później usunięte z forum Siemensa, gdy ktoś zaatakował Cybera za podanie go. Jednak to samo hasło zostało podane przez Cybera też na rosyjskojęzycznym forum Siemensa i wciąż było dostępne w momencie odkrycia Stuxneta (choć strona, na której je zamieszczono, została później przeniesiona lub usunięta). Angielskojęzyczne forum, na którym hasło zostało podane, to: *http://automation.siemens.com/forum/guests/PostShow.aspx?PostID=161*
↪27&16127&Language=en&PageIndex=3.

[9] We wszystkich trzech wersjach Stuxneta (z czerwca 2009 r. oraz z marca i kwietnia 2010 r.) modyfikowany był tylko pocisk, czyli kod z mechanizmem rozprzestrzeniania robaka. Ładunek atakujący sterowniki PLC pozostał taki sam.

[10] Sztuczka z mechanizmem automatycznego uruchamiania nie jest uznawana za lukę typu zero-day, ponieważ jest to funkcja systemu Windows, a napastnicy odkryli jedynie, że pomaga ona rozprzestrzeniać złośliwe oprogramowanie. Omówienie tej kwestii znajdziesz w przypisach 7. i 8. w rozdziale 1.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wersja Stuxneta, napastnicy zastąpili kod wykorzystujący mechanizm automatycznego uruchamiania eksploitem typu zero-day wykorzystującym pliki .LNK.

Napastnicy do wersji Stuxneta z 2010 r. dodali też inną ważną funkcję — certyfikat firmy RealTek używany do podpisywania sterowników[11].

Analizując zmiany wprowadzone przez napastników między wersjami z 2009 i 2010 r., Chien i O'Murchu stwierdzili, że metody ataku zostały celowo zmodyfikowane na bardziej agresywne. Atak został zapoczątkowany w konserwatywny sposób w 2009 r., a następnie nasilony w 2010 r. poprzez dodanie nowych mechanizmów rozprzestrzeniania robaka. Możliwe, że był to desperacki krok w celu szybszego dotarcia do celu lub zainfekowania innych maszyn niż w trakcie pierwszej próby. Zastosowany w 2010 r. eksploit wykorzystujący pliki .LNK był znacznie wydajniejszą metodą rozprzestrzeniania robaka niż użyty w 2009 r. eksploit związany z mechanizmem automatycznego uruchamiania[12]. Jednak choć nowy eksploit zwiększał prawdopodobieństwo dotarcia Stuxneta do celu, jednocześnie wzrosło ryzyko zainfekowania innych maszyn. Z powodu dodania tego i innych eksploitów w wersji z marca 2010 r. złośliwe oprogramowanie znalazło się na ponad 100 tys. maszyn w Iranie i w innych krajach[13]. Te dodatkowe infekcje

[11] Napastnicy musieli dodać certyfikat do wersji Stuxneta z 2010 r., ponieważ pod koniec 2009 r. Microsoft udostępnił nową wersję systemu operacyjnego, Windows 7, która (co zostało opisane na s. 17) obejmowała nowe zabezpieczenia, zapobiegające instalacji sterowników niepodpisanych cyfrowo z użyciem poprawnego certyfikatu.

[12] Wcześniej wspomniano, że wiele firm wyłącza automatyczne uruchamianie, ponieważ mechanizm ten zagraża bezpieczeństwu. Obsługi plików .LNK nie można w ten sposób wyłączyć, a ponieważ ta luka występowała we wszystkich wersjach systemu Windows od edycji 2000, umożliwiała przeprowadzenie ataku na większą liczbę maszyn.

[13] Założenie o szybszym rozprzestrzenianiu się wersji z 2010 r. w porównaniu z wersją z 2009 r. związane jest z pewnym zastrzeżeniem. Chien i O'Murchu sprawdzili 3280 kopii Stuxneta znalezionych w zainfekowanych maszynach przez różne firmy antywirusowe. Wersja z czerwca 2009 r. była zainstalowana tylko na 2% tych komputerów. Pozostałymi kopiami były wersje z marca i kwietnia 2010 r. Przyjęto, że mała liczba znalezionych kopii z 2009 r. to efekt wolniejszego rozprzestrzeniania się tej wersji i zainfekowania przez nią mniejszej liczby maszyn poza Iranem. Jednak możliwe, że wersja z 2009 r. została zastąpiona na zainfekowanych maszynach wersją z marca 2010 r. Stuxnet po napotkaniu maszyny sprawdzał, czy nie znajduje się już na niej jego starsza wersja. Gdy tak było, zastępował ją nowszą. Mogło to prowadzić do znalezienia przez badaczy mniejszej liczby kopii z 2009 r. Jednak mała liczba wystąpień tej wersji mogła wynikać także z ograniczonych metod jej rozprzestrzeniania.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

nie pomagały napastnikom osiągnąć celu, a jedynie zwiększały ryzyko wykrycia ataku[14]. Napastnicy musieli mieć świadomość ryzyka, jakie podejmowali, znacznie zwiększając możliwości Stuxneta w zakresie rozprzestrzeniania się. I najwyraźniej byli gotowi je ponieść.

Badaczom łatwo było dokładnie prześledzić drogę rozprzestrzeniania się Stuxneta. W każdej kopii robaka znaleźli skarb, który pomógł im zbadać pokonaną trasę. Tym skarbem był niewielki plik dziennika z danymi o wszystkich zainfekowanych maszynach. Gdy robak w poszukiwaniu celu przemierzał drogę między kolejnymi maszynami, zapisywał adresy IP i nazwy domen wszystkich ofiar, a także czas infekcji (mierzony według wewnętrznego zegara poszczególnych komputerów). Te dane zajmowały ok. 100 B (bajtów) i były przechowywane w pliku dziennika rozrastającym się, gdy robak przechodził z jednej maszyny do następnej. Każda kopia Stuxneta pobrana z zaatakowanego komputera zawierała więc historię wszystkich zainfekowanych do tego miejsca maszyn. Powstawała w ten sposób cyfrowa ścieżka powrotu, na podstawie której Chien i O'Murchu mogli dotrzeć do pierwszych ofiar. Dziennik został zaprojektowany tak, aby pomóc *napastnikom* śledzić ścieżkę pokonywaną przez Stuxneta. Zapewne nie zakładali oni, że ktoś inny wykorzysta dziennik w tym samym celu[15].

[14] To, że Stuxnet rozprzestrzeniał się za pośrednictwem pendrive'ów i sieci lokalnej, a nie przez internet, powinno zapobiec tak dużej liczbie infekcji, tak się jednak nie stało. Powodem było zapewne to, że niektóre zainfekowane irańskie firmy posiadały biura poza Iranem lub współpracowały ze zleceniobiorcami, którzy mieli klientów w innych krajach i rozprzestrzeniali infekcję za każdym razem, gdy podłączali zainfekowanego laptopa do sieci nowego klienta lub używali pendrive'a w różnych miejscach. Po wykryciu Stuxneta badacze z Symanteca przeszukali swoje archiwa pod kątem jego kopii, które mogły zostać znalezione i oznaczone jako podejrzane przez automatyczny system raportowania przed natrafieniem na robaka przez firmę VirusBlokAda w czerwcu 2010 r. Znaleźli jedną kopię wersji z marca 2010 r. na komputerze klienta z Australii. Została ona oznaczona przez system raportowania jako podejrzana w miesiącu pojawienia się tej wersji Stuxneta. To pokazywało, jak daleko to złośliwe oprogramowanie dotarło w tak krótkim czasie i jak nieuniknione było to, że w końcu zostanie wykryte.

[15] Napastnicy mogli zdalnie pobrać pliki dziennika z zainfekowanego systemu kontaktującego się z serwerami C&C.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Chien i O'Murchu przeanalizowali 3280 kopii Stuxneta zebranych z zainfekowanych maszyn przez różne firmy antywirusowe. Z danych z dzienników wynikało, że napastnicy uruchomili atak w pięciu irańskich firmach, wybranych zapewne dlatego, że mogły pozwolić Stuxnetowi na dotarcie do celu. Każda z tych firm została zaatakowana przynajmniej jedną z wersji Stuxneta z lipca 2009 r., marca 2010 r. lub kwietnia 2010 r. Symantec wykrył w tych pięciu organizacjach 12 tys. infekcji. Z tych początkowych ofiar Stuxnet rozprzestrzenił się na ponad 100 tys. maszyn w przeszło 100 krajach.

Symantec nigdy nie upublicznił nazw tych firm (z powodu obowiązującej w firmie polityki niewskazywania ofiar). W publicznych opracowaniach nazywał je domenami A, B, C, D i E. Jednak firmy te pojawiły się w plikach dziennika. Były to: Foolad Technique, Behpajooh, Kala, Neda Industrial Group i organizacja opisana w pliku jako CGJ, którą zapewne była Control Gostar Jahed. Uważano, że Kala to ta sama firma Kala Electric (lub Kalaye Electric), którą irańska grupa opozycyjna NCRI wskazała w trakcie konferencji prasowej z 2002 r. jako przykrywkę dla irańskiego programu wzbogacania uranu.

Choć w niektórych firmach atak był powtarzany, nie zawsze dotknięte były nim te same maszyny. Sugerowało to, że napastnicy mogli za każdym razem szukać maszyn znajdujących się w dogodniejszej lokalizacji lub otwierających nowe drogi do celu, co zwiększało prawdopodobieństwo sukcesu. Tylko jedna z tych firm, Behpajooh, została zaatakowana aż trzykrotnie. Była to wskazówka, że mogła ona stanowić najlepszą drogę do docelowych maszyn. Ta sama firma była też źródłem największej liczby przypadkowych infekcji. Tylko ona została zaatakowana w marcu 2010 r., kiedy to Stuxnet wymknął się spod kontroli. Spośród 12 tys. infekcji wykrytych w pięciu wymienionych firmach 69% dotyczyło właśnie organizacji Behpajooh.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 7

RYNEK EKSPLOITÓW TYPU ZERO-DAY

Eksploity typu zero-day ze Stuxneta wzbudziły wiele niepokojących pytań o rosnącą rolę rządów w tajnych transakcjach i zastosowaniach takich narzędzi. Kwestie te muszą dopiero zostać przeanalizowane przez Kongres Stanów Zjednoczonych lub w ramach debaty publicznej, jednak istnieją dowody, że praktyka ta zagraża korporacjom, kluczowej infrastrukturze i indywidualnym użytkownikom komputerów.

Choć rynek luk i eksploitów typu zero-day istnieje od ponad dziesięciu lat, do niedawna był stosunkowo niewielki i ograniczał się do zamkniętego, podziemnego świata hakerów i przestępców. Jednak w kilku ostatnich latach nastąpiła komercjalizacja tego obszaru. Liczba kupujących i sprzedających znacznie wzrosła (podobnie jak ceny), a podejrzane niegdyś transakcje zostały uprawomocnione rządowymi dolarami, co spowodowało powstanie nieregulowanego rynku cyberbroni.

Jedna z pierwszych oznak komercjalizacji wolnego rynku eksploitów typu zero-day pojawiła się w grudniu 2005 r., kiedy to sprzedawca o nicku fearwall wystawił lukę typu zero-day na sprzedaż w serwisie eBay. Wzbudziło to obawy, że praworządni badacze zabezpieczeń i łowcy błędów staną się najemnikami i zaczną sprzedawać swoje umiejętności oraz towary klientom, którzy najwięcej zapłacą, zamiast przekazywać informacje o lukach w oprogramowaniu producentom w celu wyeliminowania problemu. Przed wystawieniem

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

luki typu zero-day z programu Excel na aukcji fearwall ujawnił informacje na jej temat Microsoftowi, tak jak powinni robić to „odpowiedzialni" badacze. Jednak ów gigant z branży oprogramowania nie zaangażował się w rozwiązanie problemu. Microsoft nie prowadził wówczas programu nagród dla badaczy zgłaszających wykryte błędy. Dlatego fearwall zdecydował się sprzedać lukę na otwartym rynku, aby zawstydzić giganta i wymusić na nim szybsze załatanie luki. Cena doszła tylko do 60 dolarów, zanim eBay zamknął aukcję. Jednak zablokowana transakcja była zapowiedzią przyszłych wydarzeń.

Dziś funkcjonuje wiele rynków luk i eksploitów typu zero-day — od prowadzonych przez producentów oprogramowania i właścicieli witryn oficjalnych programów dla łowców błędów, przez kwitnący podziemny czarny rynek zarządzany przez przestępców, po tajne szare rynki zaspokajające nienasycone potrzeby wymiaru sprawiedliwości i agencji wywiadowczych z całego świata.

W oficjalnych programach Google, Microsoft i inne firmy płacą za informacje o lukach w zabezpieczeniach w ich oprogramowaniu. Producenci zaczęli też szybciej eliminować problemy. Niezależne firmy z branży zabezpieczeń, np. HP TippingPoint, też płacą za luki typu zero-day wykorzystywane w testach zabezpieczeń sieci klienckich. Pozwala to lepiej chronić klientów przed atakami. Firma TippingPoint prywatnie ujawnia luki producentom oprogramowania, aby umożliwić rozwiązanie problemu, jednak przygotowywanie łatek może trwać tygodniami lub miesiącami. W tym czasie TippingPoint może uzyskać przewagę nad konkurencją, ponieważ potrafi chronić klientów przed nieznanymi jeszcze atakami.

Na kwitnącym podziemnym czarnym rynku, skierowanym do oszustów i szpiegów korporacyjnych, sprzedawane są nie tylko luki i eksploity typu zero-day, ale też ładunki pozwalające „uzbroić" te eksploity. Te ładunki to konie trojańskie, pakiety szpiegowskie i inne szkodliwe narzędzia zaprojektowane na potrzeby wykradania internetowych danych uwierzytelniających do kont bankowych i firmowych sekretów. Narzędzia te pozwalają też budować armie komputerów zombie tworzących botnety. Luki sprzedawane na tym rynku są ujawniane publicznie i przesyłane producentom oprogramowania dopiero po wykryciu wykorzystujących je ataków. Nieraz może stać się to dopiero po latach, czego dowodem jest czas potrzebny badaczom do wykrycia eksploita plików .LNK wykorzystanego w Stuxnecie i wcześniej w koniu trojańskim Zlob.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak przestępcze podziemie, choć problematyczne, szybko traci na znaczeniu na rzecz najnowszego rynku luk i eksploitów typu zero-day, który, zdaniem analityków, wkrótce będzie wywierał znacznie poważniejszy wpływ na bezpieczeństwo niż rynek przestępczy. Jest to rosnący szary rynek handlarzy bronią cyfrową — dostawców dla przemysłu obronnego i prywatnych przedsiębiorców. Ich klientami są rządy, które windują cenę eksploitów typu zero-day. W efekcie badacze, zamiast brać nagrody w programach umożliwiających wyeliminowanie luk, są popychani w ramiona ludzi chcących je wykorzystać.

Jest to „szary" rynek, ponieważ kupujących i sprzedających można uznać za dobrych ludzi, działających na rzecz bezpieczeństwa publicznego i ochrony kraju. Jednak to, co dla jednego zapewnia bezpieczeństwo narodowe, dla drugiego może być narzędziem opresji. Nie ma też gwarancji, że rząd kupujący eksploity typu zero-day nie wykorzysta ich do szpiegowania przeciwników politycznych i aktywistów lub nie przekaże tej „broni" innym rządom. Nawet jeśli agencja rządowa wykorzystuje eksploity w uzasadnionym celu zapewniania bezpieczeństwa, luki sprzedawane na szarym rynku nie są ujawniane producentom, co pozwoliłoby na wyeliminowanie problemu. Dlatego wszyscy nieświadomi danej luki (w tym inne agencje rządowe i właściciele krytycznej infrastruktury w kraju nabywcy) są podatni na ataki ze strony zagranicznych przeciwników lub niezależnych hakerów, którzy odkryją te same słabe punkty w zabezpieczeniach i je wykorzystają.

Sprzedaż eksploitów jest legalna i w dużym stopniu nieregulowana. Choć kontrola eksportu w Stanach Zjednoczonych dotycząca zwykłego oprogramowania uniemożliwia sprzedaż eksploitów krajom takim jak Iran i Korea Północna, w eksploitach nie występują informacje o prawach autorskich określających producenta lub kraj pochodzenia. Dlatego jednostki sprzedające produkty na tym rynku nie narażają się na wykrycie.

Ceny eksploitów i luk typu zero-day są bardzo zróżnicowane. Zależą od rzadkości luki (w systemach trudniejszych do złamania znajduje się mniej luk), czasu i poziomu trudności związanych ze znalezieniem luki i opracowaniem wykorzystującego ją eksploita, popularności atakowanego oprogramowania i tego, czy kupujący jest jedynym nabywcą danego eksploita lub luki. Eksploity wymagające więcej niż jednej luki do zapewnienia napastnikowi dostępu do maszyny na poziomie administratora są droższe, podobnie jak te omijające antywirusy i inne zabezpieczenia systemu bez

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wywoływania efektów ubocznych (takich jak awaria przeglądarki lub komputera albo inne oznaki ostrzegające właściciela komputera o problemach).

Eksploit typu zero-day atakujący program Adobe Reader może kosztować od 5000 do 30 tys. dolarów. Eksploit systemu Mac OS może być wart 50 tys. dolarów. Jednak eksploit technologii Flash lub systemu Windows może kosztować od 100 tys. dolarów w górę, co wynika z powszechności tego oprogramowania. Eksploit systemu iOS firmy Apple też może kosztować 100 tys. dolarów, ponieważ trudniej jest złamać zabezpieczenia iPhone'ów niż telefonów konkurencji. Eksploity przeglądarek takich jak Firefox, Internet Explorer lub Chrome mogą kosztować od 60 tys. do ponad 200 tys. dolarów w zależności od tego, czy potrafią obejść zabezpieczenia umieszczone przez producentów w oprogramowaniu[1].

Niezależnie jednak od dokładnych cen na szarym rynku są one znacznie wyższe niż kwoty, jakie sprzedawca może uzyskać na białym rynku programów dla łowców błędów. Na przykład organizacja Mozilla Foundation płaci tylko 3000 dolarów za błędy znalezione w przeglądarce Firefox i programie pocztowym Thunderbird, natomiast Microsoft, przez lata krytykowany za brak programu dla łowców błędów, początkowo (w 2013 r.) oferował tylko 11 tys. dolarów za błędy znalezione w wersji *preview* nowej wówczas przeglądarki Internet Explorer 11. Obecnie firma ta płaci 100 tys. dolarów za luki, które mogą pomóc napastnikowi obejść zabezpieczenia w oprogramowaniu, i dodatkowo 50 tys. dolarów za rozwiązanie problemu. Google zwykle płaci tylko od 500 do 20 tys. dolarów za błędy znalezione w przeglądarce Chrome i narzędziach internetowych (takich jak Gmail i YouTube), przy czym w trakcie corocznego sponsorowanego przez tę firmę konkursu oferuje 60 tys. dolarów za luki określonego typu znalezione we wspomnianej przeglądarce. Choć niektóre firmy próbują konkurować z czarnym rynkiem, zwykle nie są w stanie płacić tyle co niektóre rządy na

[1] Zob. Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, „Forbes", 23 marca 2012. W ostatnich latach znajdowanie luk typu zero-day stało się trudniejsze, ponieważ producenci niektórych z najczęściej atakowanych programów wprowadzili zabezpieczające je mechanizmy. Na przykład Google i inne firmy wbudowały w przeglądarki tzw. izolowane środowiska (ang. *sandbox*), aby utworzyć ochronną barierę powstrzymującą szkodliwy kod przed wydostaniem się z przeglądarki do systemu operacyjnego lub do innych aplikacji z danej maszyny. W efekcie cenne stały się eksploity umożliwiające napastnikowi wyjście poza izolowane środowisko.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

szarym rynku. Ponadto firmy Apple i Adobe nadal nie prowadzą żadnych programów dla łowców błędów, w których płaciłyby za luki wykryte w oprogramowaniu używanym przez miliony osób.

Szary rynek eksploitów i luk typu zero-day istnieje od jakichś dziesięciu lat, jednak dopiero od niedawna funkcjonuje w obecnej, stabilnej postaci. Przez wiele lat transakcje były zawierane wyłącznie po cichu, w ramach prywatnych spotkań między firmami zajmującymi się zabezpieczeniami, badaczami i osobami kontaktowymi z rządu. Gdy ktoś chciał sprzedać eksploit, ale nie miał kontaktów w rządzie, trudno było znaleźć nabywcę.

Na początku 2006 r. jedna z firm zajmujących się zabezpieczeniami sprzedała kilka eksploitów typu zero-day osobie kontaktowej z dużej amerykańskiej firmy z sektora obronności, o czym poinformował były pracownik tej ostatniej. Każdy z tych eksploitów (atakowały one luki w przeglądarkach Safari, Firefox i Internet Explorer) kosztował ok. 100 tys. dolarów. Sprzedawca otrzymał z góry po 50 tys. dolarów za każdy eksploit, a później po 10 tys. miesięcznie do momentu spłacenia całej kwoty. Rozłożenie płatności w czasie miało zniechęcić do sprzedaży eksploitów innym nabywcom lub ujawnienia luk producentom, którzy mogliby wtedy przygotować łatki.

Jedną z pierwszych osób, które otwarcie przyznały się do sprzedaży eksploitów rządowi, był Charlie Miller, badacz z dziedziny zabezpieczeń i były haker z agencji NSA, zrekrutowany do niej w 2000 r. po uzyskaniu tytułu doktora matematyki na University of Notre Dame. Miller pracował dla tej agencji wywiadowczej ok. pięciu lat. Początkowo łamał kod, później zajął się włamaniami do komputerów. Przeprowadzał skanowanie rozpoznawcze na potrzeby analizy obcych sieci i dokonywania „penetracji sieci komputerowych obcych celów", jak napisał w ocenzurowanym przez NSA życiorysie. Penetracja sieci komputerowych (ang. *Computer Network Exploitation* — CNE) to w żargonie szpiegowskim włamania do systemów i sieci w celu wykradzenia danych i informacji. Po odejściu z NSA Miller zdobył w zajmującej się zabezpieczeniami społeczności uznanie za wykrywanie luk typu zero-day i tworzenie eksploitów (nie wszystkie z nich sprzedawał rządowi). Jako pierwszy wraz ze współpracownikiem złamał zabezpieczenia iPhone'a po wprowadzeniu tego urządzenia na rynek w 2007 r. Czterokrotnie wygrywał też Pwn2Own, coroczny konkurs sponsorowany przez firmę HP TippingPoint, w którym uczestnicy otrzymują nagrody za luki typu zero-day znalezione w określonym oprogramowaniu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2006 r. Miller pracował dla małej firmy z branży zabezpieczeń, a prywatnie zajmował się wykrywaniem błędów. Wtedy to sprzedał za 50 tys. dolarów eksploit typu zero-day firmie pracującej dla rządu Stanów Zjednoczonych. Miller dostarczył eksploit osobie znanej z czasów pracy w NSA, stwierdził jednak, że nie wie, gdzie kod trafił po transakcji i jak został wykorzystany. W podpisywanych przez badacza kontraktach dotyczących tego i innych eksploitów nie było zapisów określających, w jaki sposób nabywca może wykorzystać kod. „Nie wiem, czy kupiec zrobił z kodem coś dobrego, czy złego. Wiem jednak, że pracował dla rządu Stanów Zjednoczonych — powiedział Miller. — Kupili ode mnie własność intelektualną. Mogą zrobić z nią wszystko, co zechcą".

W 2007 r. Miller wywołał poruszenie, gdy opublikował artykuł o rynku luk i eksploitów typu zero-day oraz publicznie przyznał, że sprzedawał eksploity rządowi[2]. Napisał ten tekst, ponieważ chciał, aby ludzie wiedzieli o takich praktykach. Ponadto chciał pomóc innym badaczom w uniknięciu związanych z takimi transakcjami pułapek, z którymi się zetknął. W owych czasach sprzedaż eksploitów była wstydliwym sekretem branży zabezpieczeń. Badacze czasem rozmawiali na ten temat między sobą, jednak nikt nie chciał mówić o tym otwarcie. Miller szybko zrozumiał, dlaczego tak było. Koledzy ze społeczności zajmującej się zabezpieczeniami oskarżyli go o narażanie użytkowników na zagrożenia. Niektórzy domagali się odebrania Millerowi certyfikatu CISSP (ang. *Certified Information Systems Security Professional*) za naruszenie kodeksu etycznego. „Powiedziałem o tym […] i dostałem za swoje. Więcej o tym nie mówię" — stwierdził Miller[3].

Jednak z perspektywy Millera nieodpłatne ujawnianie błędów producentom nie miało sensu. Prowadzonych było wówczas tylko kilka programów dla łowców błędów, a producenci płacili za błędy i eksploity niewielkie kwoty. Ponadto rzadziej dziękowali badaczom za ujawnienie luki, a częściej grozili pozwami i śledztwami za analizowanie systemów lub oprogramowania w celu wykrycia problemów.

---

[2] Charlie Miller, „The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales", Independent Security Evaluators, 6 maja 2007 (*http://www.econinfosec.org/archive/weis2007/papers/29.pdf*).

[3] Z wywiadu przeprowadzonego przez autorkę z Charliem Millerem we wrześniu 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Miller lata temu zrezygnował z handlu eksploitami typu zero-day (obecnie pracuje w zespole zabezpieczeń Twittera), jednak nadal nie widzi nic złego w sprzedaży ich rządowi. Irytują go ludzie mówiący o etycznych aspektach takich transakcji. „Nikt się nie wścieka, gdy firmy sprzedają rządowi działa i czołgi" — powiedział, dodając, że nie tylko w Stanach Zjednoczonych badacze sprzedają eksploity typu zero-day swojemu rządowi — chińscy i rosyjscy hakerzy robią to samo. Dlatego lepiej, aby to Stany Zjednoczone oferowały najwyższą cenę za eksploity, niż żeby miały one trafić w ręce wroga.

„Moim zdaniem nie ma nic szokującego w tym, że badacze sprzedają eksploity rządowi — powiedział mi Miller. — Uważam jednak, że ludzie powinni […] wiedzieć, że takie rzeczy się zdarzają. Akceptuję to, że rząd robi to otwarcie […]. Nie rozumiem, dlaczego nie uruchomią oficjalnego programu, mówiąc: znajdźcie lukę typu zero-day, a my ją kupimy"[4].

Jednak od czasów, gdy Miller był łowcą błędów, popyt na eksploity typu zero-day na szarym rynku znacznie wzrósł. Dowodem na to jest fakt, że podczas gdy kiedyś sprzedaż eksploitów zajmowała miesiące, obecnie wystarczą na to dni lub tygodnie. Powstał rozwijający się ekosystem, aby zaspokoić to zapotrzebowanie. Pojawiły się w nim niewielkie firmy, których głównym zajęciem jest wyszukiwanie błędów. Ponadto duzi dostawcy i wykonawcy wojskowi zatrudniają zespoły profesjonalnych hakerów odpowiedzialne za tworzenie eksploitów dla rządów. Działa też większa liczba pośredników oferujących eksploity opracowane przez niezależnych sprzedawców.

Jednym z takich pośredników jest pochodzący z Republiki Południowej Afryki badacz mieszkający obecnie w Tajlandii. W społeczności zajmującej się zabezpieczeniami znany jest pod hakerskim pseudonimem The Grugq. Pośredniczy w sprzedaży eksploitów między znajomymi hakerami a osobami kontaktowymi z rządu, pobierając 15% prowizji. Pośrednik rozpoczął swój biznes w 2011 r., a już w 2012 sprzedaż szła tak dobrze, że poinformował reporterów, iż spodziewa się zarobić milion dolarów z tytułu prowizji. Na opublikowanym zdjęciu The Grugq siedzi w barze w Bangkoku z walizką z pieniędzmi pod nogami — zapłatą od jednego ze sprzedawców. Później stwierdził jednak, że zdjęcie było żartem[5].

---

[4] *Ibid.*

[5] Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

The Grugq powiedział „Forbesowi", że większość eksploitów sprzedanych przez niego trafiła do rządów Stanów Zjednoczonych i państw europejskich, ponieważ są one gotowe zapłacić więcej niż inni. Jeden z eksploitów systemu iOS Apple'a został sprzedany dostawcy dla rządu Stanów Zjednoczonych za 250 tys. dolarów. The Grugq dodał, że zażądał zbyt niskiej kwoty, ponieważ nabywca był za bardzo zadowolony z zakupu. Za przyczynę sukcesu pośrednik uważa profesjonalizm, z jakim zajmuje się marketingiem eksploitów, a także wsparcie zapewniane klientom. „W zasadzie polega to na sprzedaży komercyjnego oprogramowania takiego jak każde inne — powiedział „Forbesowi". — Musi być ono dopracowane i obejmować dokumentację".

Jednak naprawdę duże transakcje eksploitów nie są obecnie dokonywane przez pośredników lub indywidualnych sprzedawców takich jak Mille i The Grugq, ale przez firmy z branży zabezpieczeń i przez dostawców wojskowych, którzy uczynili z pisania i sprzedawania eksploitów dla rządów nową gałąź przemysłu wojskowego.

Choć rządy nadal piszą swoje eksploity (agencja NSA zatrudnia w tym celu zespoły programistów), zlecają te prace także firmom zewnętrznym. Dzieje się tak, ponieważ popyt na eksploity wzrósł, podobnie jak koszty ich tworzenia. Dwa – trzy lata temu wystarczyła jedna luka, by uzyskać dostęp do maszyny na poziomie administratora. Dziś potrzebnych jest kilka luk, aby obejść zabezpieczenia i uzyskać ten sam efekt.

Większość firm uczestniczących w opisanych transakcjach nie ujawnia informacji o pracach w tym obszarze — nie tylko dlatego, że takie operacje są poufne, ale też dlatego, by nie stać się celem dla aktywistów protestujących przeciwko takiej działalności lub przeciwników, którzy mogliby włamać się i wykraść eksploity. Ponieważ luki typu zero-day można wykorzystać zarówno do ochrony systemów, jak i ich atakowania, wiele firm ukrywa też ofensywne prace pod przykrywką działań defensywnych. Amerykańskie firmy takie jak Endgame Systems, Harris, Raytheon, Northrop Grumman, SAIC, Booz Allen Hamilton i Lockheed Martin na różne sposoby działają w branży eksploitów. W Europie są to np. niewielkie firmy ReVuln z Malty (tworząca eksploity systemów kontroli procesów przemysłowych) i VUPEN z Francji (sprzedająca eksploity dla wymiaru sprawiedliwości i agencji wywiadowczych). Organizacje Hacking Team z Włoch i Gamma Group z Wielkiej Brytanii sprzedają wymiarowi sprawiedliwości

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i agencjom wywiadowczym narzędzia do inwigilacji, które instalują się przy użyciu eksploitów typu zero-day.

Prace nad eksploitami typu zero-day w zlokalizowanej w stanie Georgia firmie Endgame Systems od lat były słabo skrywanym sekretem w społeczności zajmującej się zabezpieczeniami, jednak poza tym gronem stały się powszechnie znane w 2011 r., kiedy to hakerzy z grupy Anonymous włamali się na serwery innej organizacji, HBGary Federal, i udostępnili tysiące przechowywanych tam e-maili, w tym korespondencję z kierownictwem firmy Endgame. Te e-maile dotyczyły pracy firmy Endgame nad eksploitami, a także starań, by zgodnie z życzeniem rządowych odbiorców „zachować jak największą dyskrecję". W e-mailach znajdowały się też prezentacje w PowerPoincie skierowane do potencjalnych klientów firmy Endgame i opis misji firmy: zwiększanie „możliwości wywiadu i organizacji wojskowych Stanów Zjednoczonych w zakresie operacji informatycznych". Prezes rady nadzorczej firmy Endgame jest jednocześnie dyrektorem naczelnym w In-Q-Tel, należącej do CIA firmie z finansowaniem *venture capital*.

Oficjalnie firma Endgame oferowała usługi ochrony klientów przed wirusami i botnetami, jednak potajemnie sprzedawała pakiety luk i eksploitów obejmujące informacje, które mogły „być przydatne w atakach na sieci komputerowe". Ataki na sieci komputerowe (ang. *Computer Network Attacks* — CNA) to wojskowe określenie operacji hakerskich polegających na manipulowaniu danymi lub systemami, uszkadzaniu ich albo spowalnianiu lub zatrzymywaniu pracy systemów. Firma powstała w 2008 r. i była na tyle obiecująca, że po dwóch latach pozyskała 30 mln dolarów finansowania *venture capital*, a w kolejnej turze dodatkowo 23 mln. W 2011 r. Christopher Rouland, CEO Endgame, powiedział lokalnej gazecie z Atlanty, że przychody firmy „co roku rosną więcej niż dwukrotnie"[6].

W wykradzionych e-mailach opisane były trzy różne pakiety oferowane przez firmę Endgame: Maui, Cayman i Corsica. Kosztujący 2,5 mln dolarów rocznie pakiet Maui oferował nabywcy zestaw 25 eksploitów typu zero-day. Pakiet Cayman kosztował 1,5 mln dolarów i zapewniał informacje o milionach podatnych na ataki maszyn z całego świata już zainfekowanych

[6] Tonya Layman, *Rouland's Tech Security Firm Growing Fast*, „Atlanta Business Chronicle", 11 czerwca 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

robakami tworzącymi botnety (takimi jak Conficker) lub innym złośliwym oprogramowaniem. Przykładowa mapa z e-maili przedstawiała lokalizację podatnych na atak komputerów w Rosji i listę zainfekowanych systemów w najważniejszych biurach rządowych i obiektach infrastruktury krytycznej. Lista obejmowała adres IP każdej maszyny i używany w niej system operacyjny. Na liście znajdowało się 249 zainfekowanych maszyn w Centralnym Banku Rosji i grupa komputerów z ministerstwa finansów, banku rezerwy narodowej, elektrowni jądrowej w Nowoworonieżu i rafinerii ropy naftowej w Achińsku. Firma Endgame zebrała te dane m.in. za pomocą ujść komunikujących się z maszynami zainfekowanymi Confickerem. Gdy to złośliwe oprogramowanie kontaktowało się z ujściami, Endgame rejestrowała dane na temat zaatakowanych komputerów. Podobna mapa Wenezueli przedstawiała lokalizację serwerów WWW z tego kraju i używanego na nich oprogramowania. Serwery WWW, jeśli są źle skonfigurowane i umożliwiają włamanie, często zapewniają napastnikom dostęp do systemów i baz danych używanych na zapleczu. Systemy z tej listy obejmowały serwery Corporación Andina de Fomento (banku rozwoju finansującego 18 krajów członkowskich z Ameryki Łacińskiej, Karaibów i Europy), a także komputer z biura budżetu centralnego Wenezueli, gabinetu prezydenta, ministerstwa obrony narodowej i ministerstwa spraw zagranicznych. Po tym włamaniu firma Endgame w 2012 r. poinformowała reporterów, że zamierza wycofać się z branży sprzedaży eksploitów, a na początku 2014 r. formalnie ogłosiła, że to robi.

Choć Endgame starała się ukrywać swoje poczynania w branży sprzedaży eksploitów, inna organizacja otwarcie chwaliła się rolą, jaką odgrywa w transakcjach eksploitami typu zero-day. Jest to firma VUPEN Security z Montpellier we Francji. VUPEN określa samą siebie jako małą firmę z branży zabezpieczeń tworzącą i sprzedającą eksploity dla agencji wywiadowczych i wymiaru sprawiedliwości na potrzeby ofensywnych operacji w obszarze cyberzabezpieczeń i legalnych misji przechwytywania danych. Została założona w 2008 r. w celu zabezpieczania klientów rządowych przed atakami na luki typu zero-day. Dwa lata później zaczęła tworzyć eksploity na potrzeby operacji ofensywnych. W 2011 r. zarobiła 1,2 mln dolarów, a 90% tej sumy pochodziło z eksportu. W 2013 r. firma ogłosiła otwarcie biura w Stanach Zjednoczonych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Założyciel i CEO firmy VUPEN, Chaouki Bekrar, to bezpośredni i nieco bezczelny człowiek, który lubi irytować na Twitterze krytyków uważających, że dostarczanie eksploitów rządom jest nieetyczne. Bekrar często zachęca działających potajemnie konkurentów do tego, aby otwarcie przyznali się do handlu eksploitami. „Jesteśmy jedyną firmą na świecie, która jasno przyznaje, że się tym zajmuje — mówi. — W Stanach Zjednoczonych i Europie działają firmy, które też się tym zajmują, jednak robią to w ukryciu. Natomiast my zdecydowaliśmy się funkcjonować otwarcie, ponieważ chcemy być w pełni transparentni"[7].

Podczas gdy Endgame i inne firmy starają się działać dyskretnie, Bekrar i jego badacze regularnie uczestniczą w poświęconym zabezpieczeniom konferencjach i konkursach takich jak Pwn2Own, aby zwiększyć rozpoznawalność organizacji. Na konferencji CanSecWest (odbywającej się w Kanadzie dorocznej konferencji z dziedziny zabezpieczeń komputerowych) w 2012 r., gdzie przeprowadzony został konkurs Pwn2Own, Bekrar i czteroosobowy zespół badaczy zajęli pierwsze miejsce. Ubrani byli w czarne bluzy z kapturem i nazwą firmy na plecach.

Jednak transparentność firmy VUPEN ma pewne granice. Bekrar nie opisuje swoich doświadczeń i nie odpowiada na pytania o sprawy osobiste. Zamiast tego kieruje uwagę na firmę. „Jestem tylko aktorem i chcę rozmawiać o filmie" — mówi. Jeśli chodzi o firmę, jest równie dyskretny. Nie informuje, ilu pracowników zatrudnia (ogranicza się do stwierdzenia, że firma jest mała), i nie podaje ich nazwisk.

Badacze w VUPEN cały czas poświęcają na wyszukiwanie luk typu zero-day i tworzenie eksploitów — zarówno dla znanych już luk, jak i dla luk typu zero-day. Bekrar nie podaje, ile eksploitów firma sprzedała od czasu rozpoczęcia ich tworzenia. Twierdzi jednak, że wykrywa setki luk typu zero-day rocznie. „Mamy luki typu zero-day do wszystkiego — mówi. — Mamy niemal dowolne narzędzia dla każdego systemu operacyjnego, dla każdej przeglądarki, dla każdej aplikacji, o jakiej pomyślisz".

Trudno stwierdzić, na ile przechwałki Bekrara są prawdziwe, a na ile jest to tylko marketing, ale jego strategia wydaje się sprawdzać. W 2012 r., kilka miesięcy po wygraniu przez zespół Bekrara konkursu Pwn2Own,

[7] Te i inne słowa Bekrara w tym rozdziale pochodzą z wywiadu przeprowadzonego przez autorkę w marcu 2012 r. (chyba że podane jest inaczej).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

agencja NSA zakupiła od firmy VUPEN roczną subskrypcję usługi BAE (ang. *binary analysis and exploits*). Kontrakt, ujawniony na mocy wniosku o wgląd w dokumenty publiczne, został mocno ocenzurowany i nie obejmuje ceny za tę usługę. Jednak firma konsultingowa, która przyznała firmie VUPEN tytuł przedsiębiorcy roku 2011, zasugerowała, że koszt takiej usługi to ok. 100 tys. dolarów rocznie. Według witryny firmy VUPEN usługa BAE zapewnia „zaawansowane techniczne raporty na temat najważniejszych krytycznych luk, pozwalające zrozumieć ich podstawowe przyczyny, techniki wykorzystywania i łagodzenia problemu, a także wykrywania ataków opartych na eksploitach i lukach”[8].

VUPEN oferuje też program ochrony przed zagrożeniami. W jego ramach firma zapewnia szczegółowe analizy na temat luk wykrytych przez jej badaczy, co pozwala klientom „zmniejszyć zagrożenie atakami na luki typu zero-day”. Te informacje pochodzą z firmowej broszurki, która wyciekła w serwisie WikiLeaks[9]. Oba te programy są opisane w taki sposób, jakby miały pomagać klientom w ochronie przed atakami (eksploity typu zero-day mogą posłużyć do testowania systemu pod kątem jego podatności na zagrożenia), jednak udostępniane informacje można też wykorzystać do ataków na niezabezpieczone systemy. Pakiet ochrony przed zagrożeniami zapewnia klientom nawet gotowe eksploity przeznaczone do ataku na ujawniane luki. VUPEN oferuje też trzecią usługę dla wymiaru sprawiedliwości i agencji wywiadowczych, zaprojektowaną specjalnie na potrzeby potajemnego atakowania docelowych maszyn w celu uzyskania zdalnego dostępu do nich. W broszurze przytaczane są słowa Bekrara: „Agencje wymiaru sprawiedliwości potrzebują najbardziej zaawansowanych badań z zakresu włamań do systemów informatycznych i najbardziej niezawodnych narzędzi do ataku, aby móc niejawnie uzyskać zdalny dostęp do systemów komputerowych. Zastosowanie nieznanych wcześniej luk w oprogramowaniu i eksploitów omijających produkty antywirusowe i zabezpieczenia nowoczesnych systemów operacyjnych […] może pomóc śledczym w skutecznym wykonaniu tego zadania”.

[8] Z notatki prasowej „VUPEN Gets Entrepreneurial Company of the Year Award in the Vulnerability Research Market”, 1 czerwca 2006 (*https://www.frost.com/prod/servlet/press-release.pag?docid=234804194*).

[9] Broszura jest dostępna na stronie: *https://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Narzędzia do włamań są oferowane tylko policji i agencjom wywiadowczym z organizacji NATO, ANZUS i ASEAN, a także z krajów partnerskich tych organizacji. Bekrar pisze, że jest to „ograniczona liczba państw".

„To bardzo delikatna kwestia, dlatego zależy nam na tym, by liczba klientów była niewielka" — mówi. Jednak NATO zrzesza 28 państw, w tym Rumunię i Turcję, a ok. 40 kolejnych krajów (w tym Izrael, Białoruś, Pakistan i Rosja) jest uważanych za partnerów. Bekrar utrzymuje jednak, że VUPEN nie wszystkim krajom z tej listy oferuje swoje produkty.

Firma sprzedaje eksploity atakujące wszystkie najpopularniejsze komercyjne produkty korporacji Microsoft, Apple, Adobe i innych, a także korporacyjne systemy bazodanowe i serwery produkowane przez firmy takie jak Oracle. Jednak najbardziej pożądane są eksploity przeglądarek, a Bekrar twierdzi, że jego firma posiada eksploity dla wszystkich programów tego rodzaju. Firma sprzedaje tylko eksploity i coś, co Bekrar nazywa pośrednim ładunkiem, umożliwiającym klientom ukrycie się w sieci. Klient sam musi uzbroić eksploit docelowym ładunkiem.

Po wykryciu Stuxneta VUPEN zainteresowała się też systemami kontroli, gdy klienci zaczęli dopytywać o atakujące je eksploity. Eksploity w Stuxnecie, które zespół Bekrara przeanalizował po ujawnieniu ataku, robiły duże wrażenie. „Same luki były naprawdę ciekawe, a wykorzystujący je eksploit jeszcze bardziej interesujący — powiedział Bekrar. — Niełatwo było wykorzystać te luki". Jednak opracowanie ataków na systemy kontroli procesów przemysłowych wymaga dostępu do specjalistycznego sprzętu i obiektów. „Nie mamy takich rzeczy i nie chcemy ich mieć" — oświadcza Bekrar.

Subskrybenci usługi zapewniającej eksploity mogą korzystać z portalu, gdzie dostępne jest menu gotowych eksploitów typu zero-day. Można też zamawiać eksploity dla konkretnych systemów operacyjnych i aplikacji. Według broszury eksploity są podzielone na cztery kategorie w różnych cenach. Subskrybenci wykupują określoną liczbę kredytów, które można wykorzystać do zakupu eksploitów wartych 1, 2, 3 lub 4 kredyty. Obok każdego eksploita podane są poziom jego niezawodności i atakowane oprogramowanie. Klienci mogą też otrzymywać w czasie rzeczywistym alerty o odkryciu nowych luk i powstaniu nowych eksploitów. VUPEN śledzi ogłoszenia Microsoftu i innych producentów, aby dowiadywać się o wykryciu lub załataniu luk wykorzystywanych przez jeden z eksploitów firmy. Gdy tak się stanie, informuje klientów o tym, że błąd i eksploit zostały „spalone" (czasem robi to za pomocą wiadomości na Twitterze).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bekrar mówi, że jego firma nie sprzedaje eksploitów na wyłączność, tylko oferuje te same eksploity wielu odbiorcom. Jednak im częściej dany eksploit jest stosowany, tym większe prawdopodobieństwo jego wykrycia, przez co staje się on mniej atrakcyjny dla agencji takich jak NSA, dla których tajność to priorytetowa kwestia. Bekrar utrzymuje, że VUPEN współpracuje tylko z ograniczoną liczbą rządów. Mówi też, że klienci firmy nie wykorzystują eksploitów w „operacjach na masową skalę", dlatego „jest prawie niemożliwe", aby te eksploity były powszechnie stosowane.

Bekrar, podobnie jak Miller, ma niewiele zrozumienia dla osób krytykujących sprzedaż eksploitów. Powiedział kiedyś, że to producenci oprogramowania spowodowali powstanie rynku rządowego, najpierw w ogóle unikając płacenia badaczom za wykryte przez nich luki, a później odmawiając odpowiednio wysokich nagród. Badacze nie mieli więc innego wyboru jak skierować się do innych nabywców, aby uzyskać zapłatę za swoją pracę. Bekrar twierdzi też, że powodem, dla którego handluje eksploitami, nie są pieniądze. „Nie jesteśmy biznesmenami, nie dbamy o poziom sprzedaży. Ważne są dla nas przede wszystkim bezpieczeństwo i etyka" — mówi.

W trakcie konkursu Pwn2Own firma Google zaoferowała 60 tys. dolarów za informacje o eksploicie i luce wykorzystanych przez zespół firmy VUPEN do ataku na przeglądarkę Chrome tej firmy. Bekrar odmówił jednak przekazania informacji[10]. Zażartował, że mógłby się zastanowić, gdyby firma Google zaproponowała milion dolarów. Jednak później w prywatnej rozmowie stwierdził, że nie odda eksploita nawet za tę kwotę, ponieważ woli zatrzymać go dla swoich klientów. Zapytany, czy klienci firmy VUPEN mają tak duże środki, roześmiał się i powiedział: „Nie, nie, nie. Bez szans […]. Nie mają takiego budżetu".

[10] Firma VUPEN wygrała już w konkursie 60 tys. dolarów od HP TippingPoint, jednak firma Google oferowała dodatkowe 60 tys. dolarów za informacje o luce, by móc ją załatać. Konkurs Pwn2Own zwykle wymaga od uczestników przekazania eksploita i informacji o luce, co pozwala ją wyeliminować. Nie dotyczy to jednak eksploitów do wychodzenia poza bezpieczne izolowane środowisko, a firma VUPEN stwierdziła, że zastosowała właśnie takie narzędzie. Pracownik Google'a oskarżył VUPEN o popisywanie się kosztem użytkowników. Oto, co powiedział: „Staramy się uzyskać od kogoś informacje, żebyśmy mogli rozwiązać problem [… Bez tych informacji] nie chodzi tu już o ochronę użytkowników, tylko o popisywanie się. To dobre, by połechtać swoje ego, ale internet nie stanie się dzięki temu bezpieczniejszy".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bekrar utrzymywał, że współpracuje z rządami nie tylko z powodu pieniędzy: „Współpracujemy głównie z rządami, które zmagają się z problemami bezpieczeństwa narodowego […] pomagamy im chronić demokrację i ratować życie […]. Podobnie jest z innymi metodami inwigilacji. Rząd musi wiedzieć, czy ktoś nie szykuje czegoś złego i co robią ludzie. Pozwala to chronić bezpieczeństwo narodowe. Istnieje wiele sposobów na wykorzystanie eksploitów do zapewnienia bezpieczeństwa narodowego i ratowania życia".

Krytycy twierdzą, że firmy takie jak VUPEN nie mogą wiedzieć, gdzie trafią ich eksploity i w jaki sposób zostaną wykorzystane. Możliwe, że posłużą do szpiegowania niewinnych obywateli. Bekrar przyznaje, że umowy z klientami nie zabraniają bezpośrednio rządowym nabywcom używania pozyskanych od firmy VUPEN eksploitów do szpiegowania obywateli. „Piszemy jednak, że eksploity muszą być stosowane etycznie" — mówi.

Bekrar jest zdania, że nie da się tego zapisać w kontrakcie w bardziej szczegółowy sposób, ponieważ umowy prawne muszą być ogólne i uwzględniać wszystkie możliwe przypadki nieetycznego zastosowania kodu. „Dla nas sprawa jest jasna — mówi. — Eksploity muszą być używane etycznie, zgodnie z międzynarodowymi regulacjami i prawami. Ponadto nie można z nich korzystać w operacjach na masową skalę". Jednak każdy uważa za etyczne coś innego i Bekrar przyznaje, że nie ma możliwości kontrolowania, jak klienci interpretują zapisy o etycznym postępowaniu. „Z mojej strony jedynym, co mogę zrobić, jest wybór państw, z którymi handlujemy. Sprzedajemy tylko do państw demokratycznych".

Jednym z największych krytyków firmy VUPEN jest Christopher Soghoian z Amerykańskiego Związku Praw Obywatelskich (ang. *American Civil Liberties Union*). Nazywa on sprzedawców eksploitów, w tym firmę VUPEN, współczesnymi handlarzami śmiercią i kowbojami, którzy biorą rządowe dolary za dostarczanie narzędzi i kul umożliwiających opresyjną inwigilację oraz wojnę cybernetyczną. Stanowi to zagrożenie dla wszystkich[11]. Soghoian przyznaje, że rządy mogłyby produkować i stosować własne eksploity typu zero-day niezależnie od tego, czy firmy takie jak VUPEN by je sprzedawały. Uważa jednak, że sprzedawcy z wolnego rynku są „tykającą bombą", ponieważ nie można kontrolować prowadzonego przez nich handlu.

[11] Ryan Naraine, „0-Day Exploit Middlemen Are Cowboys, Ticking Bomb", *ZDNet.com*, 16 lutego 2012 (*http://www.zdnet.com/article/0-day-exploit-middlemen-are-cowboys-ticking-bomb/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Gdy tylko jeden z uzbrojonych eksploitów typu zero-day sprzedany rządowi zostanie zdobyty przez złych ludzi i użyty do ataku na krytyczną infrastrukturę Stanów Zjednoczonych, rozpęta się piekło — powiedział Soghoian słuchaczom na konferencji dla informatyków w 2011 r. — Pytanie brzmi nie »czy«, ale »kiedy« […]. Co się stanie, gdy skorumpowany słabo opłacany policjant sprzeda kopię jednego z uzbrojonych eksploitów zorganizowanej grupie przestępczej lub terrorystom? Co się stanie, gdy grupa Anonymous włamie się do sieci organów ścigania i wykradnie jeden z takich eksploitów?”[12].

W 2013 r. zostały podjęte wstępne kroki w celu uregulowania sprzedaży luk zero-day i innej cyberbroni. Wassenaar Arrangement, organizacja zajmująca się kontrolą zbrojeń i zrzeszająca 41 państw, w tym Stany Zjednoczone, Wielką Brytanię, Rosję i Niemcy, ogłosiła, że po raz pierwszy sklasyfikowała oprogramowanie i sprzęt, które można wykorzystać do hakowania i inwigilacji. Stwierdziła też, że takie narzędzia są produktami o podwójnym zastosowaniu, dlatego „mogą być szkodliwe dla bezpieczeństwa i stabilności na arenie międzynarodowej i lokalnej”. Kategoria produktów o podwójnym zastosowaniu służy do ograniczania dostępu do materiałów i technologii (np. do używanej w wirówkach stali maraging), które mogą być używane zarówno w celach wojskowych, jak i pokojowych. Choć zalecenia wspomnianej organizacji nie są wiążące prawnie, oczekuje się, że państwa członkowskie wprowadzą licencje na sprzedaż takich materiałów i będą współpracować ze sobą w zakresie kontroli sprzedaży produktów o podwójnym zastosowaniu[13]. Niemcy, jeden z członków organizacji Wassenaar, już stosują prawo, które zabrania sprzedaży eksploitów, a także bezpłatnego ich przekazywania, co badacze z branży zabezpieczeń regularnie robią na potrzeby testowania systemów i zwiększania bezpieczeństwa. Prawodawcy w Stanach Zjednoczonych z Senackiej Komisji Sił Zbrojnych w 2013 r. wezwali prezydenta do opracowania polityki „kontroli rozprzestrzeniania cyberbroni za pomocą jednostronnych i wielostronnych mechanizmów kontroli eksportu, działań organów ścigania, środków finansowych, kroków dyplomatycznych i innych rozwiązań, które prezydent uzna za właściwe”.

[12] *Ibid.*

[13] „The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies”, publiczne wystąpienie na zgromadzeniu plenarnym w 2013 r. (*http://www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jest jednak niejasne, jak taka kontrola miałaby wyglądać, ponieważ luki i eksploity typu zero-day oraz inna broń cyfrowa są znacznie trudniejsze do monitorowania niż tradycyjne uzbrojenie. Ponadto mechanizmy wymagające licencji na eksport eksploitów i sprawdzania nabywców mogą zwiększyć koszty legalnych sprzedawców, natomiast nie wszyscy sprzedawcy są zainteresowani działaniem zgodnym z prawem.

Ponadto tego rodzaju mechanizmy kontrolne mają zapobiegać dostaniu się eksploitów w ręce przestępców i niebezpiecznych podmiotów, np. grup terrorystycznych. Nie będą w żadnym stopniu ograniczać wykorzystywania eksploitów przez rząd do egzekwowania prawa i zapewniania bezpieczeństwa narodowego. Kwitnący szary rynek eksploitów typu zero-day jest dowodem na to, że organy ścigania i agencje wywiadowcze chętnie sięgają po eksploity takie jak te zastosowane w Stuxnecie i są gotowe dobrze za to zapłacić. Ten szalony popyt na eksploity typu zero-day zapewne jeszcze wzrośnie, a wraz z nim zwiększy się też liczba sponsorowanych przez państwo programów, w których te eksploity są używane.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 8

ŁADUNEK

Nico Falliere garbił się przy biurku na ósmym piętrze 40-piętrowego Tour Egée, trójkątnego budynku ze szkła i betonu w biznesowej dzielnicy Paryża La Défense. Na zewnątrz widoczny był ponury las wież biznesowych, zasłaniający widok na gołębie i letnich turystów kierujących się w stronę Wielkiego Łuku Braterstwa. Jednak Falliere nie interesował się widokiem. Był skupiony na zrobieniu pierwszego kroku do zrozumienia skomplikowanego ładunku Stuxneta.

Był początek sierpnia 2010 r. Zaledwie dwa tygodnie po rozpoczęciu przez zespół z Symanteca analizy Stuxneta Chien i O'Murchu znaleźli bezprecedensową liczbę eksploitów typu zero-day kryjących się w tym robaku. W ciągu tych pierwszych dwóch tygodni Falliere współpracował z O'Murchu nad analizą dużego pliku .DLL dla systemu Windows, wiedział jednak, że prawdziwe sekrety Stuxneta tkwią w ładunku, i nie mógł się doczekać zajęcia się nim.

Właśnie wrócił z lunchu ze znajomymi i zaczął przekopywać się przez pliki ładunku, oddzielając jedne od drugich i próbując zrozumieć ich format oraz strukturę. Zauważył, że jednym z nich był plik .DLL o znajomej nazwie. Badacze z Symanteca do tego czasu pozyskali już oprogramowanie Siemens Step 7, dlatego Falliere przejrzał pliki zainstalowane przez ten program w systemie testowym. Szybko znalazł to, czego szukał — plik .DLL z oprogramowania Siemens Step 7 o nazwie identycznej z plikiem Stuxneta. Uznał to za ciekawy trop.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Niedługo potem ustalił, że gdy tylko Stuxnet znajdzie się na komputerze z zainstalowanym oprogramowaniem Siemens Step 7 lub WinCC, wypakowuje plik .DLL o wspomnianej nazwie z większego pliku .DDL dla systemu Windows i odszyfrowuje go.

Falliere posłużył się ukrytym w złośliwym oprogramowaniu kluczem do odszyfrowania tego pliku .DLL i odkrył, że obejmuje on wszystkie funkcje z poprawnego pliku .DLL narzędzia Step 7. Ponadto plik zawierał podejrzany kod z poleceniami takimi jak „zapisz" i „wczytaj". Falliere w trakcie swojej kariery widział wystarczająco dużo złośliwego oprogramowania, aby dokładnie wiedzieć, czego szuka. Użyty w Stuxnecie plik .DLL dla narzędzia Step 7 pełnił funkcję rootkita, który po cichu czaił się w systemie w oczekiwaniu na przejęcie tych funkcji w momencie, gdy system próbował wczytać lub zapisać bloki kodu w docelowych sterownikach PLC. Ten rootkit (podobnie jak rootkit z części Stuxneta będącej pociskiem) przejmował funkcję odczytu, aby ukryć coś, co Stuxnet robił ze sterownikami PLC. Według wiedzy Falliere'a był to pierwszy rootkit atakujący system kontroli przemysłowej. To kolejny „pierwszy przypadek w historii" na rosnącej liście takich przypadków związanych ze Stuxnetem.

Falliere nie potrafił stwierdzić, czy szkodliwy plik .DLL ze Stuxneta przechwytywał funkcję odczytu w celu pasywnego śledzenia pracy sterownika PLC i rejestrowania danych na temat jego działania, czy miał groźniejsze przeznaczenie. Jednak to, że rootkit przejmował także funkcję zapisu, wskazywało raczej na drugą z tych ewentualności. Oznaczało to, że rootkit zapewne próbował zatrzymać pracę sterownika PLC lub wpłynąć na jego działanie. Falliere spojrzał na zegarek. W Kalifornii była mniej więcej piąta rano — zbyt wczesna pora, by dzwonić do Chiena. Dlatego zdecydował się kontynuować analizę.

Pracował przez kilka kolejnych godzin. Gdy zebrał wszystkie kawałki układanki, otrzymał dokładnie to, co podejrzewał. Stuxnet rzeczywiście przechwytywał polecenia kierowane z pliku .DLL Siemensa do sterowników PLC i zastępował je własnymi. Falliere nie był jednak pewien, co robak nakazywał robić sterownikom PLC. Nie umiał znaleźć bloków kodu, które Stuxnet wstrzykiwał do sterownika PLC. Miał jednak pewność, że ten kod nie robi niczego dobrego. W Kalifornii była już dziewiąta, dlatego badacz zadzwonił do Chiena.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Zwykle ci dwaj rozmawiali raz w tygodniu, aby Falliere mógł pokrótce opisać to, czym się zajmuje. Te rozmowy były zwięzłe i konkretne. Trwały nie dłużej niż kilka minut. Jednak tym razem Falliere szczegółowo opisał wszystko, co znalazł. Chien uważnie wysłuchał relacji, zaskoczony tym, co usłyszał. Atak okazywał się coraz bardziej złożony. Gdziekolwiek spojrzeli, Stuxnet szykował dla nich nowe niespodzianki.

Chien zgodził się, że Falliere powinien zająć się wyłącznie szukaniem bloków kodu wstrzykiwanych przez Stuxneta do sterowników PLC. Badacze ustalili też, że Falliere zamieści na blogu krótką wiadomość o rootkicie atakującym sterownik PLC. Pozostałe informacje miały pozostać nieujawnione do czasu ustalenia przez badacza natury kodu wstrzykiwanego przez Stuxneta do sterowników.

Gdy wieczorem Falliere wracał metrem z pracy do domu, przepełniała go energia połączona ze zdenerwowaniem. Analizował wirusy i robaki już od czterech lat. W tym czasie widział tak wiele szkodliwych programów, że rzadko ekscytował się czymś nowym. Jednak ten przypadek był inny. Atak na sterowniki PLC był czymś bez precedensu i mógł stanowić wstęp do działań zupełnie nowego rodzaju.

Mimo ekscytacji badacz wiedział, że czeka go wiele trudności. Zastępowany przez Stuxneta plik .DLL Siemensa był duży, a struktura oprogramowania Step 7 i kontrolowanych przez nie sterowników PLC — w większości nieudokumentowana. Falliere i Chien nie wiedzieli, jak działa ten system, a techniczne wyzwania związane z odszyfrowaniem ładunku zapowiadały się na poważne. Ponadto nie było gwarancji, że badaczom uda się złamać szyfr. Na tym etapie dalsza droga była pełna niewiadomych. Falliere wiedział, że czeka go długa i męcząca przygoda.

FALLIERE BYŁ 28-LATKIEM z galijską urodą człowieka, który wyglądał raczej na DJ-a puszczającego transową muzykę w podziemnych nocnych klubach Paryża, a nie analityka ślęczącego w trakcie dojazdów metrem nad ryzami papieru zadrukowanego kodem komputerowym. W rzeczywistości badacz był dość nieśmiały i zamknięty w sobie, a analizowanie kodu komputerowego pociągało go znacznie bardziej niż spędzanie nocy w dusznym i dudniącym klubie.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Falliere był mistrzem inżynierii odwrotnej. Specjalizował się w dogłębnych analizach szkodliwego kodu. Inżynieria odwrotna przypomina czarną magię i polega na przekształcaniu zer i jedynek w zrozumiałym dla komputera języku binarnym na czytelny dla człowieka kod w języku programowania. Ta dziedzina wymaga intensywnego skupienia i dużych umiejętności, zwłaszcza w sytuacji gdy kod jest tak złożony jak w Stuxnecie. Jednak Falliere'owi to nie przeszkadzało. Im bardziej skomplikowany był kod, tym większą miał satysfakcję z jego złamania.

Początkowo, jako nastolatek, rozwijał swoje umiejętności, łamiąc pliki „crackme". Były to łamigłówki, które programiści przygotowywali dla siebie nawzajem, aby sprawdzić umiejętności z zakresu inżynierii odwrotnej. Pisali krótkie programy ukryte w zaszyfrowanej powłoce, a druga strona za pomocą inżynierii odwrotnej musiała złamać szyfr i pokonać inne zabezpieczenia, aby odkryć tajną wiadomość. Tę wiadomość należało następnie odesłać autorowi, aby udowodnić rozwiązanie zadania. Wirusy i robaki były w pewnym sensie innym rodzajem plików „crackme", przy czym niektóre z nich były bardziej skomplikowane od innych. Jedyną różnicą było to, że obecnie Falliere otrzymywał wynagrodzenie za łamanie zabezpieczeń.

Falliere urodził się i spędził dzieciństwo pod Tuluzą w południowej Francji, gdzie mieści się siedziba Airbusa (korporacji z branży lotniczej) i centrum technologii satelitarnych. W regionie zdominowanym przez inżynierów — zajmujących się lotnictwem i nie tylko — wydawało się czymś naturalnym, że będzie interesował się technologią. Ale początkowo kierował się w stronę mechaniki. Jego ojciec był mechanikiem samochodowym pracującym we własnym warsztacie. Jednak zetknięcie Falliere'a w szkole średniej z komputerami popchnęło go w innym kierunku — na studia z dziedziny nauk komputerowych we francuskim Narodowym Instytucie Nauk Stosowanych. Rozprzestrzenienie się w 2001 r. płodnego robaka Code Red, który zainfekował ponad 700 tys. maszyn, sprawiło, że Falliere zaciekawił się zabezpieczeniami komputerów. Jeszcze w college'u napisał kilka artykułów na temat zabezpieczeń dla małego francuskiego magazynu technicznego. Ponadto napisał pracę dla SecurityFocus, należącej do Symanteca witryny poświęconej bezpieczeństwu[1]. Pod koniec 2005 r., w trakcie studiów magisterskich z dziedziny nauk komputerowych, dowiedział się,

[1] Symantec przejął witrynę SecurityFocus w 2002 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

że w celu otrzymania dyplomu musi odbyć półroczny staż. Wykorzystał swoje kontakty z redaktorami witryny SecurityFocus, którzy skierowali go do Chiena. Falliere nie mógł trafić na lepszy moment. Symantec właśnie zatrudniał nowe osoby w Dublinie, a Chien starał się znaleźć doświadczonych specjalistów od inżynierii odwrotnej. Powiedział Falliere'owi, że zamiast półrocznego stażu w Symantecu mógłby zaproponować mu pełnoetatową pracę. „Ile chcesz zarabiać?" — zapytał.

„Nie potrzebuję pieniędzy — powiedział Falliere — tylko stażu".

„Zwariowałeś? — odpowiedział Chien. — Prześlę ci ofertę e-mailem. Po prostu ją przyjmij".

Kilka miesięcy później Falliere mieszkał już w Dublinie. Dość szybko przyzwyczaił się do nowego życia, jednak po dwóch latach ciągłych lotów do Francji w celu spotkań z dziewczyną poprosił o przeniesienie do Paryża, gdzie Symantec prowadził biuro sprzedaży i marketingu. Okazało się, że w Paryżu był jedynym pracownikiem technicznym. Dlatego czasem czuł się odizolowany, ale jednocześnie pomagało mu to skoncentrować się na pracy.

Jego biurko znajdowało się w gabinecie współdzielonym z dwoma współpracownikami. Na blacie panował uporządkowany nieład. Wokół maszyny testowej używanej do uruchamiania złośliwego oprogramowania i laptopa z debuggerem służącym do analizowania kodu leżały liczne teksty i książki techniczne. Cylindryczna kostka Rubika była jedynym osobistym przedmiotem na biurku. Falliere bawił się nią, gdy natrafił na skomplikowaną porcję kodu, który nie pozwalał się złamać.

Choć był geniuszem w dziedzinie inżynierii odwrotnej, w okresie wykrycia Stuxneta zajmował się nią w niewielkim stopniu. Z czasem stał się w Symantecu „człowiekiem od narzędzi". Tworzył programy oraz narzędzia, aby ułatwić innym analitykom odszyfrowywanie złośliwego oprogramowania. To zajęcie go wciągnęło. Zaczął dopracowywać na swoje własne potrzeby nieporęczne i niewydajne narzędzia analityczne. Później zaczął robić to także dla współpracowników, a nawet tworzył na ich prośbę nowe oprogramowanie. Doprowadziło to do tego, że Falliere więcej czasu poświęcał na pracę nad narzędziami niż na odszyfrowywanie kodu. Złośliwym oprogramowaniem zajmował się tylko na specjalną prośbę Chiena, tak jak w przypadku Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

FALLIERE ROZPOCZĄŁ ANALIZOWANIE ładunku od zapoznania się z atakowanym przez Stuxneta oprogramowaniem Step 7. Była to zastrzeżona aplikacja Siemensa służąca do programowania sterowników PLC z serii S7. Step 7 działał w systemie operacyjnym Windows i umożliwiał programistom pisanie oraz kompilowanie poleceń (bloków kodu) dla sterowników PLC Siemensa. Ten system nie był kompletny bez programu Simatic WinCC, narzędzia do wizualizacji służącego do monitorowania sterowników PLC i kontrolowanych przez nie procesów. Sterowniki PLC, podłączone do stacji monitorujących za pomocą sieci produkcyjnej obiektu, nieustannie komunikowały się z tymi maszynami, przesyłając raporty o stanie i aktualizacje. Zapewniało to operatorom podgląd w czasie rzeczywistym sprzętu i operacji kontrolowanych przez dany sterownik PLC. Plik .DLL Siemensa był ważnym elementem programów Step 7 i WinCC. Pełnił funkcję pośrednika w generowaniu poleceń dla sterowników PLC i przekazywaniu raportów o stanie z tych urządzeń. Właśnie tu pojawiał się szkodliwy plik .DLL Stuxneta. Robił on wszystko to, do czego został zaprojektowany pierwotny plik .DLL, a także wykonywał dodatkowe operacje.

Aby zrozumieć działanie sobowtóra pliku .DLL, Falliere musiał najpierw zrozumieć funkcjonowanie systemu Step 7 i oryginalnego pliku .DLL. Szukał w internecie ekspertów, z którymi mógłby się skonsultować. Myślał nawet o zgłoszeniu się do Siemensa, ale nie wiedział, do kogo powinien zadzwonić. Plik .DLL z systemu Step 7 był tylko jednym z wielu podobnych plików w oprogramowaniu Siemensa. Znalezienie dwóch lub trzech programistów, którzy znali ten kod wystarczająco dobrze, zajęłoby równie wiele czasu jak jego samodzielne zrozumienie. Ponadto samodzielne złamanie kodu było czymś, z czego Falliere mógłby być dumny.

W celu zastosowania inżynierii odwrotnej do plików .DLL (oryginalnego i sobowtóra) otworzył je w deasemblerze — narzędziu przeznaczonym do przekształcania kodu binarnego na język asemblerowy, czyli o krok wstecz względem kodu binarnego. Używany deasembler umożliwiał dodawanie do kodu notatek i komentarzy oraz przenoszenie sekcji kodu, aby zwiększyć jego czytelność. Badacz pracował nad małymi porcjami kodu, dodając do każdej z nich opis wykonywanych przez nią funkcji.

Falliere stosował typową technikę badania złożonego złośliwego oprogramowania tego rodzaju. Łączył analizy statyczne (badanie kodu na ekranie w deasamblerze i debuggerze) z analizami dynamicznymi (obserwowanie

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

działania kodu w systemie testowym z użyciem debuggera do wstrzymywania i wznawiania pracy, co pozwala dopasować określone fragmenty kodu do efektów ich działania na maszynie testowej). Nawet w najlepszych warunkach proces ten jest bardzo powolny, ponieważ wymaga przechodzenia między dwiema maszynami. Analiza Stuxneta była jednak wyjątkowo trudna z powodu wielkości i złożoności kodu.

Udokumentowanie wszystkich działań pliku .DLL zajęło dwa tygodnie. Ostatecznie Falliere potwierdził to, co cały czas podejrzewał — Stuxnet zastępował plik .DLL Siemensa sobowtórem, aby przejąć system. W tym celu zmieniał nazwę pliku .DLL Siemensa z *s7otbxdx.DLL* na *s7otbxsx.DLL* i instalował szkodliwy plik .DLL o nazwie oryginalnego, w ten sposób przejmując tożsamość pliku Siemensa. Gdy system wywoływał plik .DLL Siemensa w celu wykonania potrzebnych operacji, odpowiadał mu szkodliwy plik.

To zaś, co robił szkodliwy plik .DLL po znalezieniu się w docelowym miejscu, było niezwykłe.

Gdy inżynier próbował przesłać polecenia do sterownika PLC, Stuxnet przekazywał wykonywane później własne szkodliwe instrukcje. Jednak nie zastępował pierwotnych poleceń w jednym prostym kroku. Zamiast tego zwiększał wielkość bloku kodu i umieszczał na początku własny szkodliwy kod. Następnie, aby mieć pewność, że zamiast poprawnych poleceń uruchomione zostaną szkodliwe, Stuxnet przejmował też podstawowy blok kodu w sterowniku PLC, odpowiedzialny za wczytywanie i wykonywanie instrukcji. Niezauważalne wstrzyknięcie kodu w ten sposób bez spowodowania „bricka" sterowników PLC (czyli unieruchomienia ich) wymagało dużej wiedzy i wysokich umiejętności, jednak napastnicy świetnie poradzili sobie z tym zadaniem.

Druga część ataku była jeszcze bardziej pomysłowa. Zanim szkodliwe polecenia Stuxneta zaczynały działać, to złośliwe oprogramowanie przez dwa tygodnie (a czasem dłużej) rejestrowało w sterowniku PLC poprawne operacje, gdy sterownik przesyłał raporty z powrotem do stacji monitorujących. Kiedy później szkodliwe polecenia Stuxneta zaczynały działać, złośliwe oprogramowanie odtwarzało zarejestrowane dane operatorom, by ukryć przed nimi, że z urządzeniami dzieje się coś złego. Przypominało to hollywoodzki film akcji, w którym złodzieje przesyłają odtwarzane w pętli nagranie do kamery monitoringu. Gdy Stuxnet przeprowadzał sabotaż sterownika PLC, wyłączał zautomatyzowane alarmy cyfrowe, aby zapobiec

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

włączeniu się systemów bezpieczeństwa i wstrzymaniu procesów kontrolowanych przez sterownik w wyniku wykrycia tego, że raporty wskazują na niebezpieczeństwo. W tym celu modyfikował bloki kodu OB35 będące częścią systemu bezpieczeństwa sterowników PLC. Służyły one do monitorowania kluczowych operacji, np. szybkości turbin kontrolowanych przez sterownik. Te bloki były generowane przez sterownik PLC co 100 ms, dzięki czemu system bezpieczeństwa mógł szybko zainterweniować, gdyby turbina zaczęła obracać się zbyt szybko (lub po wystąpieniu innych problemów). System lub operator mógł wtedy uruchomić przycisk zamykania i zainicjować wyłączenie sprzętu. Ponieważ jednak Stuxnet modyfikował dane wykorzystywane przez system bezpieczeństwa, system był nieświadom zagrożeń i nie mógł zainterweniować[2].

[2] W Stuxnecie występowało bardzo niewiele udziwnień i nadmiarowych rozwiązań. Jednak we fragmencie kodu odpowiedzialnym za przechwytywanie bloków OB35 napastnicy umieścili „magiczny znacznik" (jest to umieszczana w kodzie wartość oznaczająca warunek lub uruchamiająca operację), który wyglądał jak żart — 0xDEADF007. Ten znacznik był reprezentacją liczby zapisaną w systemie szesnastkowym. Gdy Stuxnet sprawdzał warunki w atakowanym systemie, aby ustalić, czy powinien rozpocząć blokowanie systemu bezpieczeństwa, generowany był „magiczny znacznik". Oznaczał on, że robak może przystąpić do działania. Napastnicy mogli wybrać dowolną liczbę, np. 1234, jednak posłużyli się wartością, która zapisana w formacie szesnastkowym tworzyła słowo i liczby — DEADF007. Stosowanie przez programistów wartości tworzących w formacie szesnastkowym słowa nie jest niczym niezwykłym. Na przykład pierwsze cztery bajty plików klas Javy to w formacie szesnastkowym 0xCAFEBABE. Inną wartością w formacie szesnastkowym stosowaną w żargonie hakerów jest 0xDEADBEEF, oznaczająca awarię oprogramowania. Chien zastanawiał się, czy 0xDEADF007 w Stuxnecie oznacza *dead fool* (czyli „martwy głupek"), co jest pejoratywnym określeniem niedziałającego systemu bezpieczeństwa, czy *dead foot* (dosłownie „martwa stopa"). To ostatnie wyrażenie jest stosowane przez pilotów samolotowych i oznacza awarię silnika. „Niesprawna stopa to niesprawny silnik" to zwrot pomagający pilotom w stresujących sytuacjach szybko zdać sobie sprawę z tego, że gdy pedał nie reaguje, oznacza to awarię silnika. Pilot nie ma wtedy kontroli nad silnikiem. Podobnie 0xDEADF007 w Stuxnecie mogło sygnalizować moment, w którym operatorzy w Iranie tracili kontrolę nad sterownikami PLC w wyniku sabotażu przeprowadzonego przez Stuxneta. System bezpieczeństwa nie mógł wtedy zainicjować automatycznego wyłączania urządzeń, podobnie jak operatorzy nie mogli zainterweniować, by w trybie awaryjnym ręcznie wyłączyć sprzęt. Chien zastanawiał się, czy przynajmniej jeden z twórców Stuxneta nie jest pilotem.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Na tym atak się jeszcze nie kończył. Gdyby programiści zauważyli problemy z turbiną lub innym sprzętem kontrolowanym przez sterownik PLC i próbowali sprawdzić bloki poleceń w celu ustalenia, czy w programie nie występują błędy, Stuxnet miał interweniować i uniemożliwiać zapoznanie się ze szkodliwym kodem. W tym celu przechwytywał wszystkie żądania odczytu bloków kodu w sterowniku PLC i zwracał „oczyszczoną" wersję kodu, pozbawioną szkodliwych poleceń. Gdy rozwiązujący problem inżynier próbował przeprogramować urządzenie, zastępując istniejące bloki kodu w sterowniku PLC nowymi, Stuxnet infekował szkodliwymi poleceniami także nowy kod. Programista mógł przeprogramować sterownik setki razy, a Stuxnet po każdej próbie zastępował poprawny kod zmodyfikowanymi instrukcjami.

Falliere był zdumiony złożonością ataku i tym, do jakich wniosków to prowadziło. Nagle stało się jasne, że — w przeciwieństwie do tego, w co wszyscy początkowo wierzyli — Stuxnet nie próbował pobierać danych ze sterowników PLC w celu szpiegowania ich pracy. To, że robak wstrzykiwał polecenia do sterownika PLC i próbował ukryć ten fakt, a jednocześnie wyłączał alarmy, było dowodem na to, że atak miał na celu nie szpiegowanie, a sabotaż.

Nie był to jednak prosty atak DoS. Napastnicy nie próbowali dokonać sabotażu sterownika PLC, wyłączając go. W czasie trwania ataku sterownik kontynuował pracę. Napastnicy chcieli fizycznie uszkodzić procesy lub urządzenia kontrolowane przez ten sterownik. Falliere po raz pierwszy zetknął się z kodem, który zamiast modyfikować lub wykradać dane, fizycznie zmienia lub uszkadza jakieś urządzenie.

Był to scenariusz żywcem wyjęty z hollywoodzkiego hitu, a konkretnie filmu z Bruce'em Willisem. Trzy lata wcześniej w *Szklanej pułapce 4.0* przedstawiono tego rodzaju niszczycielskie metody, choć z typowymi dla Hollywoodu rozmachem i przesadą. W firmie grupa cyberterrorystów dowodzona przez sfrustrowanego byłego pracownika rządowego przeprowadza skoordynowane cyberataki, by zakłócić działanie rynku akcji, sieci transportowych i elektrowni. Te poczynania mają odwrócić uwagę władz od rzeczywistego celu — wykradzenia milionów dolarów z rządowych skarbców. Nastaje chaos z nieodłącznymi w serii *Szklana pułapka* eksplozjami.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Specjaliści od zabezpieczeń komputerowych już dawno temu uznali tego typu hollywoodzkie scenariusze za czystą fantazję. Haker może zablokować krytyczny system lub dwa, ale żeby miał coś wysadzać? Wydawało się to mało prawdopodobne. Nawet większość eksplozji w *Szklanej pułapce* wynikała z ataków fizycznych, a nie cybernetycznych. Stuxnet był jednak dowodem na to, że filmowy scenariusz jest realny. Robak znacznie wykraczał ponad wszystko, co Falliere do tej pory napotkał i co spodziewał się znaleźć w kodzie.

Mimo dużych rozmiarów i sukcesów Symantec był tylko pełną nerdów firmą zajmującą się chronieniem swoich klientów. Przez 15 lat jej przeciwnikami byli hakerzy-żartownisie i cyberprzestępcy, a od niedawna także finansowani przez państwo szpiedzy wykradający korporacyjne i rządowe sekrety. Wszyscy oni byli mniej lub bardziej poważnymi wrogami, jednak żaden z nich nie uciekał się do powodowania szkód fizycznych. Przez lata złośliwe oprogramowanie stopniowo ewoluowało. Początkowo jego twórcy mieli podobną motywację. Choć niektóre programy powodowały więcej szkód niż inne, w latach 90. głównym celem autorów wirusów było zdobycie chwały i sławy. Typowy ładunek w wirusach zawierał pozdrowienia dla leniwych znajomych hakera. Sytuacja zmieniła się, gdy rozwinął się handel elektroniczny i hakowanie zaczęło być wykorzystywane do działalności przestępczej. Wtedy celem nie było już zdobycie uwagi, ale ukrycie się na możliwie długi czas w systemie w celu wykradzenia numerów kart kredytowych i danych uwierzytelniających do kont bankowych. Jeszcze później hakowanie zaczęto stosować w toczących się o wysoką stawkę rozgrywkach szpiegowskich. Finansowani przez rząd szpiedzy infiltrują sieci przez miesiące lub lata, by po cichu wyprowadzać tajemnice państwowe i inne poufne dane.

Twórcy Stuxneta posunęli się zdecydowanie dalej. Była to nie tyle ewolucja, ile rewolucja w świecie złośliwego oprogramowania. Wszystko, co Falliere i jego współpracownicy badali w przeszłości, nawet najpoważniejsze zagrożenia dotyczące operatorów kart kredytowych i sekretów Departamentu Obrony, w porównaniu ze Stuxnetem wydawało się mało istotne. Stuxnet oznaczał pojawienie się zupełnie nowego pola bitwy, na którym stawki są znacznie wyższe niż wcześniej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Od dawna opowiadana była historia, wedle której w przeszłości mogło wydarzyć się coś podobnego, nikt jednak nie przedstawił dowodów na jej prawdziwość. Wedle tej historii w 1982 r. CIA uknuła spisek, aby zainstalować bombę logiczną w oprogramowaniu kontrolującym rosyjski gazociąg, co miało doprowadzić do sabotażu. Gdy kod zadziałał, spowodował błędne funkcjonowanie zaworów gazociągu. W efekcie nastąpiła eksplozja tak gwałtowna i potężna, że została zarejestrowana przez znajdujące się na orbicie satelity[3].

W Culver City Chien zastanawiał się, czy w Iranie nastąpiły niewyjaśnione eksplozje, które można przypisać Stuxnetowi. Gdy przeszukał wiadomości, z zaskoczeniem odkrył, że w ostatnich tygodniach było kilka takich wybuchów[4]. Pod koniec lipca rurociąg do przesyłu gazu z Iranu do Turcji eksplodował pod tureckim miastem Doğubayazıt kilka kilometrów od irańskiej granicy. Wybuch wybił okna w pobliskich budynkach i spowodował groźny pożar, którego gaszenie trwało wiele godzin[5].

Inna eksplozja wydarzyła się pod irańskim miastem Tebriz, gdzie znajduje się rurociąg o długości 2500 km przesyłający gaz z Iranu do Ankary. Trzeci wybuch zarejestrowano w państwowym zakładzie petrochemicznym na wyspie Chark w Zatoce Perskiej; zginęły w nim cztery osoby[6]. Kilka tygodni później nastąpiła czwarta eksplozja gazu, tym razem w zakładzie petrochemicznym firmy Pardis w miejscowości Asaluyeh. Pięć osób zginęło, a trzy zostały ranne[7]. Wybuch miał miejsce zaledwie tydzień po wizycie w zakładzie irańskiego prezydenta Mahmuda Ahmadineżada.

Wszystkie te eksplozje zostały jednak wyjaśnione. Kurdyjscy rebelianci przyznali się do ataków w Doğubayazıcie i Tebrizie, a irańska agencja informacyjna IRNA jako przyczynę pożaru na wyspie Chark podała zbyt

---

[3] Więcej informacji o tym rzekomym sabotażu rurociągu znajdziesz na s. 206 – 208.

[4] Con Coughlin, *Who's Blowing up Iran's Gas Pipelines?*, „The Telegraph", 18 sierpnia 2010 (*http://www.deepjournal.com/p/7/a/en/2801.html*).

[5] Agence France-Presse, „Suspected Kurd Rebels Blow up Iran – Turkey Gas Pipeline", 21 lipca 2010 (*http://www.institutkurde.org/en/info/latest/suspected-kurd-rebels-blow-up-iran-turkey-gas-pipeline-2372.html*).

[6] „Petrochemical Factory Blast Kills 4 in Iran", Associated Press, 25 lipca 2010 (*http://www.gainesville.com/news/20100725/petrochemical-factory-blast-kills-4-in-iran*).

[7] „Explosion in Petrochemical Complex in Asalouyeh Kills 5", Tabnak News Agency, 4 sierpnia 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wysokie ciśnienie w głównym kotle[8]. Eksplozję w firmie Pardis wyjaśniono wyciekiem etanu, który zapalił się, gdy robotnicy zaczęli spawać rurę. Chien zastanawiał się jednak, czy przyczyną jednej lub kilku z tych eksplozji nie był Stuxnet.

Było to znacznie więcej niż ktokolwiek w zespole spodziewał się kilka tygodni wcześniej, w momencie rozpoczęcia analizowania Stuxneta. Jeśli robak działał zgodnie z podejrzeniami Chiena i jego współpracowników, był pierwszą udokumentowaną cyberbronią.

Chien, O'Murchu i Falliere omawiali telefonicznie swoje możliwości. Nadal nie wiedzieli, co dokładnie Stuxnet robił ze sterownikami PLC ani jaki cel miał atakować. Wiedzieli jednak, że muszą ujawnić odkryte informacje na temat ładunku. Dlatego 17 sierpnia 2010 r. publicznie poinformowali, że Stuxnet nie był — wbrew powszechnemu przekonaniu — narzędziem szpiegowskim, tylko bronią cyfrową zaprojektowaną w celu sabotażu. „Wcześniej stwierdziliśmy, że Stuxnet może wykradać kod […] i ukrywać się za pomocą klasycznego rootkita dla systemu Windows — napisał Falliere z typową dla siebie powściągliwością — jednak, niestety, potrafi też dużo więcej"[9].

Aby zilustrować niszczycielskie możliwości Stuxneta, badacze nawiązali do przeprowadzonego w 1982 r. ataku na syberyjski rurociąg. Ich słowa zostały starannie dopracowane przez firmowy dział PR, jednak szokujący charakter płynących z nich wniosków był niezaprzeczalny. Gdy tylko wiadomość została upubliczniona, badacze niecierpliwie czekali na odpowiedź społeczności. Spodziewali się dramatycznej reakcji, jednak zetknęli się z „ciszą, w której słychać było cykanie świerszczy", jak ujął to Chien.

---

[8] Ivan Watso, Yesim Comert, „Kurdish Rebel Group Claims Responsibility for Gas Pipeline Blast", CNNWorld, 21 lipca 2010 (*http://edition.cnn.com/2010/WORLD/meast/07/21/turkey.pipeline.blast/*).

[9] Nicolas Falliere, „Stuxnet Introduces the First Known Rootkit for Industrial Control Systems", blog Symanteca, 6 sierpnia 2010 (*https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-industrial-control-systems*). Zauważ, że data publikacji artykułu to 6 sierpnia. Jest to jednak data pierwszej publikacji tekstu z informacjami o rootkicie atakującym sterowniki PLC. Artykuł został później zaktualizowany o informację, że Stuxnet miał służyć do sabotażu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Chien był zdziwiony brakiem reakcji. Chodziło przecież o kod, który potrafi doprowadzić do eksplozji. Badacze zakładali przynajmniej tyle, że po opublikowaniu ich odkryć inni analitycy przedstawią własne wnioski na temat Stuxneta. Tak wyglądały badania nad złośliwym oprogramowaniem. Po odkryciu nowego ataku zespoły konkurujących ze sobą badaczy z różnych firm równolegle starały się rozszyfrować kod, ścigając się, kto pierwszy opublikuje wyniki. Po przedstawieniu rezultatów przez jeden zespół szybko dołączały inne prezentujące własne odkrycia. Jeśli kilka grup doszło do tych samych wniosków, wykonanie przez badaczy tej samej pracy było potwierdzającym ich odkrycia nieformalnym procesem wzajemnej oceny. Cisza po artykule na temat Stuxneta była więc nietypowa i niepokojąca. Chien zaczął się zastanawiać, czy nie są jedynym zespołem analizującym ładunek Stuxneta i czy ktokolwiek inny się nim zainteresował.

Przez krótką chwilę zwątpił nawet w zasadność decyzji o poświęceniu tak dużej ilości czasu na zbadany kod. Czy wszyscy inni widzieli coś, przez co uznali, że Stuxnet nie ma znaczenia? Czy Chien i jego zespół całkowicie to coś przeoczyli? Później jednak badacz przyjrzał się wszystkiemu, co odkryli w ostatnich tygodniach. Stwierdził, że nie mogli się mylić ani co do znaczenia Stuxneta, ani co do agresywnych zamiarów jego twórców.

Nie miał też więcej wątpliwości w kwestii kontynuowania analiz. Praca nad Stuxnetem wydawała mu się nawet pilniejsza niż wcześniej. Zespół właśnie ogłosił światu, że Stuxnet to broń cyfrowa zaprojektowana do wyrządzania fizycznych zniszczeń. Wciąż jednak nieznany był cel tego złośliwego oprogramowania. Zespół martwił się, że po publicznym ujawnieniu niszczycielskiego przeznaczenia kodu napastnicy mogą poczuć presję, by przyspieszyć misję i zniszczyć cel — jeśli jeszcze tego nie zrobili.

Najwyraźniej nie tylko badacze obawiali się wybuchów. Pięć dni po opublikowaniu przez zespół informacji stały napływ do ujścia danych z irańskich maszyn zainfekowanych Stuxnetem zatrzymał się. Wyglądało na to, że ktoś w Iranie zapoznał się z tą wiadomością. Irańczycy wreszcie zmądrzeli i aby zablokować napastnikom zdalny dostęp do zainfekowanych maszyn i uniemożliwić wyrządzenie szkód, nakazali przerwać wszystkie wychodzące połączenia z komputerów z tego kraju do dwóch domen C&C Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 9

NIEKONTROLOWANA KONTROLA PROCESÓW PRZEMYSŁOWYCH

O siemdziesiąt kilometrów od Idaho Falls w stanie Idaho, na rozległej pustynnej prerii należącej do Laboratorium Narodowego Idaho (ang. *Idaho National Laboratory* — INL; jest to jednostka Departamentu Energii), grupka inżynierów dygotała z zimna wokół stojącego na betonowej płycie generatora wielkości niewielkiego autobusu. Był 4 marca 2007 r. Pracownicy dokonywali ostatniej kontroli bezpieczeństwa przed przełomowymi testami, jakie mieli przeprowadzić.

Mniej więcej 1,5 km dalej, w laboratoryjnym ośrodku dla gości, grupa urzędników z Waszyngtonu oraz dyrektorów z branży energetycznej i NERC (ang. *North American Electric Reliability Corporation*) zebrała się w sali, grzejąc dłonie przy kubkach parującej kawy w oczekiwaniu na transmitowany na żywo pokaz.

W 2010 r., gdy badacze z Symanteca odkryli, że Stuxnet został zaprojektowany w celu sabotażu sterowników PLC Siemensa, sądzili, że był to pierwszy udokumentowany przypadek zastosowania kodu do fizycznego uszkadzania sprzętu. Jednak przeprowadzony trzy lata wcześniej na równinach Idaho test Aurora Generator udowodnił wykonalność takiego ataku.

Około 11:30 tego marcowego dnia jeden z pracowników w Idaho Falls otrzymał sygnał rozpoczęcia ataku szkodliwego kodu na cel. Gdy silnik diesla generatora o mocy 5000 KM (koni mechanicznych) zabrzmiał w głośnikach

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

niewielkiej sali ośrodka, wszyscy zaczęli wpatrywać się uważnie w ekran w poszukiwaniu oznak efektów działania kodu. Początkowo nie były one widoczne. Jednak nagle goście usłyszeli głośny trzask przypominający uderzenie ciężkiego łańcucha o metalowy bęben. Stalowy potwór zatrząsł się. Po kilku sekundach trzask się powtórzył. Tym razem generator przechylił się i mocno zadrżał, jakby ktoś podłączył go do defibrylatora. Śruby i części z gumowego pierścienia uszczelniającego wystrzeliły w kierunku kamery. Obserwatorzy aż się wzdrygnęli. Po ok. 15 s następny głośny trzask ponownie spowodował przechylenie się maszyny. Tym razem po ustaniu wibracji z generatora wydobyła się smuga białego dymu. Wtedy nagle — *trach!* — maszyna ponownie zadygotała, po czym uspokoiła się na dobre. Po długiej chwili, gdy wydawało się, że bestia mogła przetrwać atak, z jej wnętrza zaczęły wydobywać się obłoki czarnego dymu.

Od rozpoczęcia testu minęły tylko trzy minuty. To wystarczyło, aby zmienić wielką maszynę w dymiącą i pozbawioną życia stertę metalu. Po tym wszystkim w sali nie było słychać oklasków. Zapanowała przejmująca cisza. Poruszenie sprzętu wielkości czołgu powinno wymagać wyjątkowej siły. Jednak w tym przypadku wystarczyło 21 wierszy szkodliwego kodu.

Opisany test był przez całe tygodnie szczegółowo planowany i modelowany, mimo to siła i gwałtowność ataku zaskoczyły inżynierów. Był to „niezwykle obrazowy moment" — powiedział Michael Assante, jeden z architektów testu[1]. Jedną rzeczą było zasymulować atak na niewielki silnik umieszczony na stole, a zupełnie inną obserwować 27-tonową maszynę podskakującą jak zabawka i rozpadającą się na części.

Ten test był dowodem na to, że sabotażysta nie potrzebuje fizycznego dostępu do obiektu, aby zniszczyć krytyczny sprzęt w elektrowni. Ten sam efekt można osiągnąć zdalnie za pomocą fragmentu odpowiednio opracowanego kodu. Trzy lata później, gdy w irańskich maszynach został znaleziony Stuxnet, żaden z uczestników projektu Aurora nie był zaskoczony tym, że atak cyfrowy może prowadzić do fizycznych szkód. Ludzie ci byli zaskoczeni tylko tym, że dopiero teraz ktoś zdecydował się na taki atak.

[1] Z wywiadu autorki z Assantem z września 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

GDY BADACZE Z SYMANTECA w sierpniu 2010 r. odkryli, że Stuxnet został zaprojektowany w celu dokonania fizycznego sabotażu sterowników PLC Siemensa, nie byli jedynymi, którzy nie wiedzieli, czym są takie sterowniki. Niewiele osób słyszało kiedykolwiek o tych urządzeniach, choć sterowniki PLC są komponentami zarządzającymi niektórymi z najważniejszych obiektów i procesów na świecie.

Sterowniki PLC są używane w różnych zautomatyzowanych systemach kontroli, w tym w lepiej znanych systemach SCADA (ang. *Supervisory Control and Data Acquisition*), a także w rozproszonych systemach kontroli i innych mechanizmach odpowiedzialnych za płynną pracę generatorów, turbin i kotłów w elektrowniach[2]. Tego rodzaju systemy sterują też pompami przesyłającymi ścieki do stacji uzdatniania wody, zapobiegają przelewaniu się wody w zbiornikach, a także otwierają i zamykają zawory w gazociągach, aby uniknąć powstawania nadmiernego ciśnienia, które mogłoby prowadzić do śmiertelnych pęknięć i eksplozji. Jeden z takich wypadków w 2010 r. zabił 8 osób i uszkodził 38 domów w San Bruno w Kalifornii.

Są też mniej oczywiste, ale równie ważne zastosowania systemów kontroli. Takie systemy sterują robotami na liniach montażowych w fabrykach samochodów oraz pobierają i mieszają odpowiednie ilości składników w zakładach chemicznych i farmaceutycznych. Systemy kontroli są też używane przez producentów żywności i napojów do ustawiania i utrzymywania temperatury, pozwalając na bezpieczne gotowanie i pasteryzację produktów w celu wyeliminowania zabójczych bakterii. Pomagają również zachować stałą temperaturę w piecach służących do produkcji szkła, włókna szklanego i stali, aby zapewnić wytrzymałość wieżowców, samochodów

[2] Systemy SCADA zwykle używane są tam, gdzie trzeba zarządzać urządzeniami występującymi na dużym obszarze, np.: rurociągami, sieciami kolejowymi lub sieciami dystrybucji wody i prądu. Natomiast rozproszone systemy kontroli sprawdzają się najlepiej, gdy operatorzy potrzebują kompletnych i złożonych mechanizmów kontroli w zamkniętych obiektach takich jak rafinerie, oczyszczalnie ścieków i elektrownie (przy czym w elektrowniach stosuje się też systemy SCADA do monitorowania odległych stacji przekaźnikowych). Systemy SCADA składają się ze stacji operatora, sieci komunikacyjnej i używanych w terenie zdalnych terminali (ang. *remote terminal unit* — RTU). Terminale RTU są podobne do sterowników PLC i przesyłają dane siecią z powrotem do stacji monitorującej operatora. Stacja operatora zwykle korzysta z systemu Windows (z wszystkimi nieodłącznymi lukami), a w urządzeniach polowych działają specjalne systemy operacyjne mające zwykle słabe zabezpieczenia.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i samolotów. Kontrolują światła drogowe, otwierają i zamykają drzwi cel w więzieniach federalnych o zaostrzonym rygorze oraz podnoszą i opuszczają mosty na autostradach i drogach wodnych. Ponadto pomagają kierować pociągami towarowymi i pasażerskimi oraz zapobiegają ich zderzeniom. W mniejszej skali sterują windami w wieżowcach oraz systemami ogrzewania i klimatyzacji w szpitalach, szkołach i biurach. Krótko mówiąc: są to krytyczne komponenty, dzięki którym przemysł i infrastruktura na całym świecie poprawnie działają. Dlatego muszą być niezawodne i bezpieczne. Niestety, Stuxnet był jednoznacznym dowodem na to, że jest inaczej.

A teraz, gdy kod robaka był dostępny i każdy mógł go przeanalizować oraz skopiować, ta cyfrowa broń mogła posłużyć za wzorzec do zaplanowania kolejnych ataków na podatne na nie systemy kontroli w Stanach Zjednoczonych i innych państwach. Tego rodzaju działania mogły polegać na manipulowaniu zaworami w gazociągach, uwalnianiu ścieków do akwenów wodnych lub nawet wysadzaniu generatorów w elektrowniach. Przeprowadzenie takich ataków nie wymagało zasobów bogatego państwa. Ponieważ większość podstawowych badań i prac została już wykonana przez twórców Stuxneta, którzy ujawnili luki w systemach, inni napastnicy (finansowani przez rząd lub nie) mieli łatwiejszą drogę. Od anarchistycznych grup hakerskich takich jak Anonymous i LulzSec, przez szantażystów grożących przejęciem sterowania elektrownią, po hakerów do wynajęcia pracujących dla grup terrorystycznych — Stuxnet otworzył drzwi różnorodnym hakerom, którzy nie musieli przekraczać granic ani nawet opuszczać sypialni, aby przeprowadzić atak. I choć był przeprowadzonym z chirurgiczną precyzją atakiem na konkretne maszyny bez wyrządzania szkód innym komputerom, nie wszystkie akcje musiały być równie ukierunkowane lub umiejętnie realizowane. Dlatego ataki mogły prowadzić do — przypadkowych lub nie — szeroko zakrojonych zakłóceń lub szkód.

Napastnicy nie musieli też projektować zaawansowanego robaka podobnego do Stuxneta. Zwykły, standardowy wirus lub robak też mógł wyrządzić szkody[3]. W 2003 r. system sygnalizacji w sieci kolejowej na Wschodnim Wybrzeżu przestał działać, gdy komputery należące do firmy CSX Corporation

[3] Wypadki związane z systemami kontroli przemysłowej są rejestrowane w bazie RISI (ang. *Repository of Industrial Security Incidents*). Incydenty zaczęto w niej odnotowywać od 2001 r., jednak w latach 2006 – 2009 baza była nieaktywna. Subskrypcjami danych z bazy zarządza organizacja Security Incidents Organization (*http://www.risidata.com/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

na Florydzie zostały zainfekowane wirusem Sobig. Firma CSX jest operatorem systemów dla pociągów towarowych i pasażerskich w 23 stanach. Wskutek wyłączenia sygnalizacji konieczne było zatrzymanie pociągów od Pensylwanii do Karoliny Południowej i w okolicy Waszyngtonu[4]. W tym samym roku robak Slammer wyłączył na pięć godzin system monitorowania bezpieczeństwa i sieć kontroli procesów w elektrowni atomowej w Davis-Besse w stanie Ohio[5].

W skali mierzącej przygotowanie infrastruktury krytycznej Stanów Zjednoczonych do oparcia się cyberatakom, gdzie 1 oznacza brak przygotowania, a 10 pełne przygotowanie, gen. Keith Alexander, dyrektor NSA, poinformował w 2013 r. senat, że ocena Stanów to 3. Ta ocena wynikała po części z braku zabezpieczeń systemów kontrolnych[6].

„Od ponad dziesięciu lat pracujemy w Departamencie Obrony nad rozwijaniem cybernetycznego potencjału ofensywnego — powiedział Jim Lewis z Centrum Studiów Strategicznych i Międzynarodowych. — Jednak […] moim zdaniem ludzie […] nie zdają sobie sprawy, że na zapleczu występują nowego rodzaju słabe punkty, które narażają wiele obiektów na atak"[7].

Problemy z systemami kontroli nie są tak naprawdę niczym nowym. Stuxnet jedynie po raz pierwszy spowodował ich publiczne ujawnienie. Jednak niektórzy eksperci od systemów kontrolnych wiedzieli o tych kłopotach od lat.

---

[4] Marty Niland, „Computer Virus Brings Down Train Signals", Associated Press, 20 sierpnia 2003 (*http://www.informationweek.com/computer-virus-brings-down-train-signals/d/d-id/1020446*).

[5] Robak dostał się do systemu przez sieć korporacyjną firmy, która obsługiwała elektrownię, i rozprzestrzenił się z sieci biznesowej do sieci systemów kontroli. Na szczęście elektrownia z powodu innych problemów od dwóch lat była nieczynna, dlatego nic się nie stało. Operatorzy obiektu stwierdzili też, że zachowali ręczne mechanizmy, które mogą posłużyć jako rozwiązanie zapasowe na wypadek awarii systemów automatycznych. Zob. Kevin Poulsen, „Slammer Worm Crashed Ohio Nuke Plant Network", *SecurityFocus.com*, 19 sierpnia 2003 (*http://www.securityfocus.com/news/6767/*).

[6] „Cybersecurity: Preparing for and Responding to the Enduring Threat", wystąpienie przed Senacką Komisją ds. Wydatków, 12 czerwca 2013 (*http://hsdl.org/?view&did=739096*).

[7] Lewis powiedział to w programie radiowym Diane Rehm emitowanym przez rozgłośnię WAMU w południowej Kalifornii 3 czerwca 2012 r. Wywiad z Lewisem jest dostępny na stronie: *http://dianerehm.org/shows/2012-06-04/growing-threat-cyberwarfare*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

STEROWNIKI PLC ZOSTAŁY opracowane w latach 60., gdy hakerzy (i wirusy) pojawiali się tylko w książkach z dziedziny fantastyki naukowej[8]. Te sterowniki zostały zaprojektowane na potrzeby branży motoryzacyjnej, aby zastąpić stałe logiczne systemy przekaźnikowe kontrolujące linie montażowe w halach fabrycznych. Stałe systemy sprawiały, że jedynym sposobem na zmodyfikowanie linii montażowej było wysłanie elektryka, by fizycznie zmienił układ kabli w przekaźniku. Sterowniki PLC umożliwiały łatwe aktualizowanie systemów za pomocą kilkuset wierszy kodu, choć technicy i tak musieli osobiście modyfikować systemy, docierając do urządzeń w terenie w celu wczytania poleceń z taśmy.

Gdy w latach 90. zaczęły zyskiwać popularność cyfrowe systemy kontroli, operatorzy przekonali producentów do umożliwienia zdalnego logowania się do systemów za pomocą modemów z połączeniami wdzwanianymi. Hakerów było już wtedy wielu, jednak operatorzy nie martwili się o bezpieczeństwo swoich systemów, ponieważ systemy kontroli działały w niezależnych sieciach oraz używały niestandardowych protokołów do komunikacji i zastrzeżonego oprogramowania niezgodnego z innymi programami i systemami. Nie dało się nawiązać komunikacji z systemem kontroli, podłączając do niego dowolny komputer. Nawet jeśli ktoś miał system umożliwiający taką komunikację, liczba osób, które rozumiały działanie systemów kontroli i potrafiły nimi manipulować, była niewielka.

Pod koniec lat 90. wszystko to zaczęło się zmieniać. Kongres przegłosował przepisy ochrony środowiska nakładające na firmy obowiązek monitorowania i kontroli emisji w fabrykach. Federalna Komisja ds. Regulacji Energii zaczęła żądać dostępu do systemów przesyłu elektryczności w celu monitorowania ich wydajności i dystrybucji energii. Nagle inspektorzy ds. zgodności i dyrektorzy w korporacjach zaczęli domagać się dostępu do danych i systemów używanych wcześniej wyłącznie przez operatorów zakładu. Do lamusa odeszły zastrzeżone systemy operacyjne, których nikt nie rozumiał

[8] Jedna z pierwszych wzmianek o wirusie komputerowym pojawiła się w opowiadaniu *The Scarred Man* napisanym w 1969 r. przez fizyka Gregory'ego Benforda. Tekst ten został opublikowany w magazynie „Venture" w numerze z maja 1970 r. Cyfrowe robaki pojawiły się w książce z dziedziny fantastyki naukowej, *The Shockwave Rider*, napisanej w 1975 r. przez Johna Brunnera. W tym tekście opisany został cyfrowy tasiemiec przemykający się z jednej maszyny do następnej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i z którymi nikt nie potrafił się komunikować. Zamiast nich pojawiły się systemy kontroli działające w komercyjnych systemach operacyjnych takich jak Windows i Linux. Jednak zastosowanie Windowsa oznaczało, że systemy kontroli stały się podatne na te same wirusy i robaki, które były plagą komputerów osobistych. Ponadto systemy kontroli coraz częściej były podłączane do internetu (lub modemów z dostępem wdzwanianym), aby umożliwić operatorom zdalny dostęp do nich. Stały się przez to bardziej podatne na zdalne ataki hakerów.

W marcu 1997 r. nastoletni haker z Massachusetts znany pod pseudonimem Jester dał krótki pokaz tego, co może się wydarzyć. Jester za pomocą modemu połączył się z systemem komputerowym firmy Bell Atlantic i wyłączył systemy zarządzające komunikacją telefoniczną i radiową wieży kontroli ruchu lotniczego na lotnisku Worcester Airport. Wyłączone zostały też telefony w 600 domach w pobliskim mieście. Komunikacja ochrony i straży pożarnej lotnisk była nieaktywna przez sześć godzin, podobnie jak system używany przez pilotów do aktywowania świateł na pasach startowych. Kontrolerzy ruchu lotniczego w czasie awarii musieli korzystać z telefonów komórkowych i radia na baterie do kierowania samolotami[9]. Nie wydarzyły się żadne wypadki, jednak menedżer kontroli ruchu lotniczego powiedział stacji CNN, że „tamtego dnia uciekliśmy spod topora"[10].

Tego samego roku specjalnie powołana Komisja Marsha opublikowała raport na temat podatności systemów infrastruktury krytycznej na ataki — zarówno fizyczne, jak i cyfrowe. Komisja miała zbadać sprawę Timothy'ego McVeigh, który w 1995 r. wysadził budynek federalny w Oklahoma City i uszkodził przy tym wiele ważnych centrów danych i centrów komunikacyjnych. Członkowie komisji ostrzegali przed wzrostem zagrożeń dotyczących podłączania do internetu krytycznych systemów związanych z ropą, gazem i elektrycznością. „Możliwości w zakresie wyrządzania szkód […] rosną w alarmującym tempie, a nasze zabezpieczenia są nikłe" — pisali. Odpowiednie polecenia przesłane przez sieć do komputera sterującego elektrownią „mogą być równie niszczycielskie jak plecak pełen materiałów wybuchowych. […] Powinniśmy zadbać o kluczową infrastrukturę, zanim

[9] *Teen Hacker Pleads Guilty to Crippling Mass. Airport*, „Boston Globe", 19 marca 1998.

[10] „Teen Hacker Faces Federal Charges", CNN, 18 marca 1998 (*http://edition.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

nastąpi kryzys, a nie później. Oczekiwanie na katastrofę będzie równie kosztowne, jak nieodpowiedzialne”[11].

W drugim raporcie, wydanym w tym samym roku przez Narodową Komisję Doradczą ds. Bezpieczeństwa Telekomunikacyjnego przy Białym Domu, ostrzegano, że sieć elektryczna kraju i zasilające ją obiekty są pełne luk w zabezpieczeniach, co naraża je na ataki. „Intruz korzystający z urządzeń elektronicznych […] może połączyć się z niechronionym portem i przestawić wyłącznik na wyższy poziom tolerancji, niż urządzenie chronione przez ten wyłącznik potrafi wytrzymać — napisali śledczy, przewidując test Aurora Generator dziesięć lat przed jego przeprowadzeniem. — W ten sposób można fizycznie uszkodzić wybrane urządzenie w rozdzielni”[12].

Mimo tych wczesnych ostrzeżeń nie było oznak, że ktoś jest zainteresowany przeprowadzeniem takich ataków, przynajmniej do 2000 r., kiedy to były pracownik dokonał sabotażu pomp w zakładzie uzdatniania wody w Australii. Był to pierwszy publicznie opisany przypadek celowego włamania do systemu kontroli.

HRABSTWO MAROOCHY NA SŁONECZNYM Wybrzeżu w stanie Queensland to miejsce wprost stworzone do robienia pocztówkowych zdjęć. Znajdziesz tu gęste lasy deszczowe, górę wulkaniczną i lazurowe przybrzeżne wody z plażami pokrytymi białym piaskiem. Jednak na początku 2000 r. piękno hrabstwa zostało zakłócone, gdy w okresie czterech miesięcy haker spowodował wyciek ponad 2800 m^3 ścieków z kilku pompowni do publicznych akwenów.

Pierwotnie nastąpił tylko mały wyciek ścieków z pompowni w hotelu Hyatt Regency do laguny na polu golfowym klasy PGA przy tym pięciogwiazdkowym obiekcie. Gdy robotnicy uprzątnęli lagunę, pompownia wylała ponownie, a potem jeszcze raz. Jednak najgorszy wyciek miał miejsce w Pacific Paradise, dzielnicy leżącej wzdłuż rzeki Maroochy. Kilkaset tysięcy galonów ścieków wylało się tam do kanału pływowego, zagrażając zdrowiu dzieci bawiących się na przyległych do tego kanału podwórkach, oraz do samej rzeki Maroochy, zabijając ryby i inne organizmy.

---

[11] „Critical Foundations: Protecting America’s Infrastructures”, Prezydencka Komisja ds. Ochrony Krytycznej Infrastruktury, październik 1997.

[12] „Electric Power Risk Assessment”, Narodowa Komisja Doradcza ds. Bezpieczeństwa Telekomunikacyjnego, Grupa Robocza ds. Zabezpieczania Informacji (*http://www.solarstorms.org/ElectricAssessment.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Problemy rozpoczęły się w sylwestra 1999 r., kiedy to zakład usług wodnych hrabstwa Maroochy zainstalował nowy cyfrowy system zarządzania. System kontroli w zakładzie uzdatniania wody był instalowany etapami przez zleceniobiorcę — firmę Hunter WaterTech. Był już prawie gotowy, gdy konfiguracja pompowni odpowiedzialnych za przesył ścieków do zakładu uzdatniania zaczęła się z tajemniczych powodów zmieniać. Pompy wyłączały się lub działały niezgodnie z instrukcjami operatora, a nadawczo-odbiorcza sieć radiowa używana do przekazywania poleceń do pompowni była przeładowana, uniemożliwiając operatorom kontakt z pompowniami. Ponadto alarmy, które powinny się odezwać w reakcji na problemy, pozostawały ciche[13].

Pompami sterowały dwa centralne komputery używające zastrzeżonego oprogramowania firmy Hunter WaterTech. Te komputery komunikowały się z jednostką RTU z każdej pompowni za pomocą nadawczo-odbiorczych przekaźników radiowych. Sygnały były przesyłane z komputerów do jednostek RTU lub między jednostkami RTU za pomocą polowych stacji przekaźnikowych korzystających z niepublicznych częstotliwości. Tylko osoba korzystająca z centralnych komputerów lub pozostająca w zasięgu stacji przekaźnikowej i używająca zastrzeżonego oprogramowania firmy Hunter WaterTech oraz odpowiednich protokołów komunikacji mogła przesyłać polecenia do pompowni. Początkowo Hunter WaterTech podejrzewała, że atak przeprowadził haker z zewnątrz. Dotąd w wodociągach nie używano narzędzi do wykrywania włamań ani systemu logowania, co pozwoliłoby wykryć włamanie. Mimo zainstalowania takich narzędzi firma nie potrafiła znaleźć napastnika.

Ataki powtarzały się tygodniami. Ich szczyt nastąpił pewnej marcowej nocy, kiedy to odnotowano ponad 20 incydentów. Śledczy stwierdzili wtedy, że przyczyną musi być nieuczciwy pracownik wysyłający szkodliwe polecenia w terenie za pomocą radiowego urządzenia nadawczo-

[13] Informacje o przypadku z hrabstwa Maroochy pochodzą z wywiadu przeprowadzonego przez autorkę w sierpniu 2012 r. z Robertem Stringfellowem (inżynierem wodociągów, który pomagał w śledztwie) oraz z ocenzurowanych dokumentów sądowych i raportu policji napisanego przez śledczego Petera Kingsleya. Niektóre informacje z dokumentów sądowych po raz pierwszy zostały opublikowane w książce Joego Weissa *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, Nowy Jork 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

-odbiorczego[14]. Policja namierzyła byłego pracownika kontraktowego Vitka Bodena, 49-letniego inżyniera, który pracował dla firmy Hunter WaterTech do czasu wygaśnięcia jego kontraktu w grudniu, czyli mniej więcej do momentu awarii pierwszej pompy. Boden starał się później o pracę na pełny etat w wodociągach, jednak w styczniu jego podanie zostało odrzucone. Zbiegało się to w czasie z rozpoczęciem poważniejszych problemów.

Gdy policja schwytała Bodena jednej z kwietniowych nocy, kiedy wyłączone zostały systemy alarmowe w czterech pompowniach, znalazła w samochodzie inżyniera laptopa z zainstalowanym zastrzeżonym oprogramowaniem firmy Hunter WaterTech i urządzeniem nadawczo-odbiorczym nastawionym na niepubliczną częstotliwość używaną przez wodociągi do komunikacji z pompowniami. Znaleziono też jednostkę RTU, z której Boden najwyraźniej wysyłał błędne polecenia[15].

Sprawa Bodena była pierwszym ujawnionym cyberatakiem na infrastrukturę krytyczną, jednak podobne ataki zapewne zdarzały się już wcześniej, lecz pozostały niewykryte lub niezgłoszone[16]. W kontekście incydentu z hrabstwa Maroochy pracownicy innych przedsiębiorstw użyteczności

[14] Od 14 marca do 23 kwietnia zanotowano ok. 90 incydentów. Jeden z pracowników wyśledził, że źródłem szkodliwych sygnałów radiowych jest jednostka RTU w pompowni nr 14. Pracownik wiedział, że łatwo można było zmienić adres jednostki RTU, przestawiając określone przełączniki w urządzeniu. Doszedł więc do wniosku, że napastnik musi się posługiwać jednostką RTU z przełącznikami ustawionymi na nr 14 i używać jej do przesyłania szkodliwych poleceń w taki sposób, jakby pochodziły z rzeczywistej pompowni nr 14. Aby zastawić pułapkę, pracownik zmienił adres pompowni z 14 na 3. Gdyby intruz *rzeczywiście* wysyłał fałszywe komunikaty, nie wiedziałby o zmianie adresu i nadal wysyłałby komunikat z użyciem dawnego numeru. Dokładnie to stało się pewnej nocy, gdy w sieci pojawiła się duża ilość szkodliwych komunikatów z pompowni nr 14, które miały doprowadzić do awarii centralnego komputera. Śledczy stwierdzili wtedy, że napastnik musi być człowiekiem z wewnątrz znającym system używany w Maroochy i mającym dostęp do oprogramowania oraz sprzętu firmy Hunter WaterTech.

[15] W październiku 2001 r. Boden został skazany na dwa lata więzienia. Później złożył apelację, w wyniku której dwa z oskarżeń zostały oddalone, natomiast sąd utrzymał pozostałe oskarżenia oraz sam wyrok.

[16] W ankiecie dla przedsiębiorstw przeprowadzonej w 1996 r. przez Instytut Badań Energii Elektrycznej okazało się, że tylko 25% ankietowanych firm stosuje metody wykrywania włamań. To badanie (EPRI Summer 1996 Electronic Information Security Survey) i dane statystyczne są opisane na stronie: *http://www.solarstorms.org/ElectricAssessment.html*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

publicznej powiedzieli, że zrezygnowaliby ze stawiania oskarżeń Bodenowi, aby tylko wyciszyć sprawę[17].

Opisana sytuacja powinna być dzwonkiem ostrzegawczym dla operatorów systemów kontroli na całym świecie. Ale wiele osób zlekceważyło tę sprawę, ponieważ uczestniczył w niej napastnik z wewnątrz posiadający dużą wiedzę na temat systemów hrabstwa Maroochy i dostęp do specjalistycznego sprzętu potrzebnego do przeprowadzenia ataku. Te osoby utrzymywały, że nikt z zewnątrz nie mógłby zrobić tego, co udało się Bodenowi. Ignorowały jednak przy tym liczne problemy z zabezpieczeniami w sieci systemu kontroli hrabstwa. Napastnicy z zewnątrz mogli wykorzystać te luki do przeprowadzenia podobnych ataków. Peter Kingsley, jeden ze śledczych w tej sprawie, ostrzegał później uczestników konferencji poświęconej systemom kontroli, że choć włamanie w hrabstwie Maroochy było dziełem człowieka z wewnątrz, przeprowadzenie ataku z zewnątrz też jest możliwe. „Niektóre przedsiębiorstwa użyteczności publicznej sądzą, że są bezpieczne, ponieważ same nie potrafią znaleźć sposobów nieautoryzowanego dostępu do ich systemów — powiedział. — Jednak hakerzy nie ograniczają się do standardowych technik"[18].

W 2002 r. słowa Kingsleya wydawały się nieistotne, gdyż nadal niewiele było oznak świadczących o tym, że napastnicy z zewnątrz są zainteresowani włamaniami do systemów infrastruktury krytycznej. Ponieważ nie nastąpiła żadna poważna katastrofa, firmy nie przejmowały się zabezpieczeniami systemów kontroli.

---

[17] Wodociągi hrabstwa Maroochy musiały zaangażować w sprawę organy ścigania, ponieważ wycieki zostały upublicznione i zagrażały bezpieczeństwu ludzi. Te incydenty doprowadziły też do szczegółowych dociekań ze strony australijskiej agencji ochrony środowiska i lokalnych urzędników, którzy domagali się wyjaśnienia przyczyn problemu.

[18] Kingsley wystąpił na konferencji AusCERT2002 w Australii. W raporcie na temat sprawy z Maroochy opublikowanym w 2008 r. (osiem lat po incydencie) autorzy doszli do wniosku, że firmy dopiero zaczynają eliminować część problemów uwidocznionych przez ten atak, przy czym „niektóre kwestie wciąż nie są rozwiązane i nie widać perspektyw na zmianę sytuacji". Zob. Marshall Abrams, Joe Weiss, „Malicious Control System Cyber Security Attack Case Study — Maroochy Water Services, Australia", 23 lutego 2008 (*http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Mniej więcej w tym okresie Joe Weiss zaczął intensywnie zachęcać do wprowadzania zabezpieczeń systemów kontroli.

Weiss był szczupłym i pełnym energii 64-latkiem pracującym w swoim domu w Cupertino w Kalifornii — w sercu Doliny Krzemowej. Często zastanawiał się nad katastroficznymi scenariuszami. Mieszkał zaledwie 8 km od okrytego złą sławą kalifornijskiego uskoku San Andreas i 70-letniej tamy Stevens Creek. Gdy w 1989 r. na tym obszarze miało miejsce trzęsienie ziemi Loma Prieta, kominy się zawalały, światła drogowe i telefony nie działały przez kilka dni, a fale uderzeniowe w basenie w pobliskim DeAnza College wystrzeliły graczy w piłkę wodną na chodnik, gdzie zawodnicy wyglądali jak wyrzucone na brzeg foki.

Weiss po raz pierwszy uświadomił sobie problemy z zabezpieczeniami systemów kontroli w 1999 r. Z wykształcenia był inżynierem nuklearnym, a gdy wystąpił problem roku 2000, pracował dla Instytutu Badań Energii Elektrycznej. W publikowanych w prasie wizjach końca świata przewidywano kryzys rodem z dystopii, który miał nastąpić, gdy zegary komputerów w sylwestra wybiją północ. Wynikało to z błędu programistów, którzy nie przewidzieli milenijnego przejścia do daty z trzema zerami 1 stycznia 2000 r. Weiss zaczął się zastanawiać: skoro taki drobiazg jak zmiana daty grozi zatrzymaniem systemów kontroli, to co może się stać w obliczu poważniejszych problemów? I ważniejsza sprawa: jeśli rok 2000 może przypadkowo doprowadzić do poważnych trudności, to jakie skutki mogą mieć celowe ataki hakerów?

Każdego roku na świecie odbywają się dziesiątki konferencji dotyczących ogólnie zabezpieczeń komputerów, jednak żadna z nich nie jest poświęcona systemom kontroli. Dlatego Weiss zaczął brać udział w konferencjach, aby się dowiedzieć, jakie wytyczne w zakresie bezpieczeństwa powinna stosować społeczność użytkowników systemów kontroli. Jednak w im większej liczbie konferencji uczestniczył, tym bardziej zaczynał się martwić. Gdy administratorzy sieci mówili o stosowaniu szyfrowania i uwierzytelniania, aby zapobiegać dostępowi do systemów, Weiss zdał sobie sprawę, że systemy kontroli nie posiadają żadnych standardowych zabezpieczeń występujących w zwykłych sieciach. Kiedy eksperci od zabezpieczeń pytali go, jakiej marki zapór używają operatorzy systemów kontroli w elektrowniach i jak często szukają w dziennikach sieciowych dowodów włamań, Weiss musiał odpowiadać: „Nie stosujemy zapór. Nie mamy też

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

dzienników sieciowych"[19]. Ponadto gdy zaczął wypytywać producentów systemów kontroli o zabezpieczenia ich produktów, w odpowiedzi zobaczył zdziwione spojrzenia. Producenci poinformowali go, że nikt wcześniej nie pytał o coś takiego.

We wrześniu 2001 r. dwa samoloty uderzyły w wieże Twin Towers, a niedługo potem władze odkryły podejrzane wzorce wyszukiwań w rządowych witrynach w Kalifornii. Poszukiwania dotyczyły systemów cyfrowych służących do zarządzania obiektami użyteczności publicznej i biurami rządowymi w okolicach San Francisco. Źródłem tej aktywności były adresy IP z Arabii Saudyjskiej, Indonezji i Pakistanu, a koncentrowała się ona na systemach telefonów alarmowych, elektrowniach, oczyszczalniach wody i instalacjach gazu[20]. Inne wyszukiwania dotyczyły programowania systemów kontroli straży pożarnej i rurociągów.

Następnego roku siły Stanów Zjednoczonych w Kabulu przechwyciły komputer w biurze Al-Kaidy i znalazły modele tamy wraz z oprogramowaniem dla inżynierów, które mogło posłużyć do zasymulowania jej uszkodzenia[21]. Tego samego roku CIA opublikowała memorandum dyrekcji wywiadu, w którym stwierdziła, że Al-Kaida jest „znacznie bardziej zainteresowana" cyberterroryzmem, niż wcześniej zakładano, a także zaczęła rozważać zatrudnianie hakerów.

Pojawiły się też oznaki, że inne siły mogą być zainteresowane infrastrukturą krytyczną Stanów Zjednoczonych[22]. W 2001 r. hakerzy włamali się na serwery Cal-ISO (ang. *California Independent System Operator*), korporacji non profit zarządzającej siecią przesyłu energii w dużej części stanu Kalifornia.

[19] Ten i inne cytaty słów Weissa w tym rozdziale pochodzą z wywiadu przeprowadzonego z nim przez autorkę w czerwcu 2012 r.

[20] Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, „Washington Post", 27 czerwca 2002.

[21] *Ibid.*

[22] „Infrastruktura krytyczna" w Stanach Zjednoczonych jest ogólnie definiowana przez rząd jako wszystkie obiekty lub systemy należące do jednej z 16 kategorii, do których należą: rolnictwo i żywność, banki i finanse, chemia, obiekty komercyjne, krytyczna produkcja, tamy, przemysł obronny, woda pitna i systemy uzdatniania wody, służby ratunkowe, energia, obiekty rządowe, technologie informatyczne, reaktory i odpady nuklearne, ochrona zdrowia, telekomunikacja i transport (*https://www.dhs.gov/critical-infrastructure-sectors*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Napastnicy weszli przez dwa niezabezpieczone serwery i pozostali niewykryci przez dwa tygodnie, po których to pracownicy zaczęli zauważać problemy z maszynami[23]. Przedstawiciele Cal-ISO utrzymywali, że włamanie nie stanowi zagrożenia dla sieci. Jednak anonimowe źródła poinformowały gazetę „Los Angeles Times", że hakerzy zostali wykryci w momencie, gdy próbowali uzyskać dostęp do „kluczowych części systemu", które umożliwiłyby wywołanie poważnych zakłóceń w dostawach prądu. Jedna z osób nazwała to prawie katastrofalnym włamaniem. Źródłem ataku wydawały się Chiny, a nastąpił on w czasie panowania napiętych stosunków politycznych między Chinami a Stanami Zjednoczonymi po tym, jak amerykański samolot szpiegowski zderzył się w powietrzu z chińskim myśliwcem nad Morzem Południowochińskim.

W reakcji na rosnące obawy o infrastrukturę krytyczną, a zwłaszcza o bezpieczeństwo krajowych sieci energetycznych, Departament Energii uruchomił w 2003 r. program National SCADA Test Bed w Laboratorium Narodowym Idaho. Celem programu była współpraca z producentami systemów kontroli w celu oceny ich sprzętu pod kątem luk w zabezpieczeniach. To ten program doprowadził do testu Aurora Generator w 2007 r.[24].

W Stanach Zjednoczonych funkcjonuje 2800 elektrowni i 300 tys. obiektów wytwarzających ropę naftową i gaz naturalny[25]. Kolejnych 170 tys. zakładów tworzy w tym kraju publiczny system gospodarowania wodą.

---

[23] Dan Morain, *Hackers Victimize Cal-ISO*, „Los Angeles Times", 9 czerwca 2001.

[24] Poprzedni program testów systemów SCADA został uruchomiony w Laboratorium Narodowym Sandia w 1998 r., jednak w pracach nie brali wtedy udziału producenci. Laboratorium Narodowe Idaho to główne laboratorium Departamentu Energii w dziedzinie badań nad energią nuklearną. Działa tam największy reaktor badawczy na świecie. Komisja Energii Atomowej przejęła ziemie w Idaho po drugiej wojnie światowej, aby zbudować tam laboratorium badań nad energią nuklearną. W późniejszych latach laboratorium rozszerzyło zakres prac o sieci elektryczne oraz — po opublikowaniu przez administrację George'a Busha Narodowej strategii zabezpieczania cyberprzestrzeni w lutym 2003 r. — o zabezpieczenia przemysłowych systemów kontroli. Zgodnie z tą strategią Departament Energii i Departament Bezpieczeństwa Wewnętrznego miały we współpracy z sektorem prywatnym zająć się problemem bezpieczeństwa systemów kontroli.

[25] Raport Departamentu Bezpieczeństwa Wewnętrznego, „The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", Biały Dom, luty 2003 (*https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Obejmuje on zbiorniki, tamy, studnie, stacje uzdatniania, pompownie i rurociągi[26]. Jednak 85% tych i innych obiektów infrastruktury krytycznej znajduje się w rękach sektora prywatnego. Oznacza to, że oprócz kilku branż regulowanych przez rząd (np. przemysłu energii atomowej) państwo może niewiele zrobić, by wymusić na firmach zabezpieczenie ich systemów. Rząd może jednak przynajmniej próbować przekonać producentów systemów kontroli do zwiększenia bezpieczeństwa ich produktów. We wspomnianym programie badawczym rząd planował przeprowadzać testy dopóty, dopóki producenci nie zgodzą się wyeliminować wykrytych luk[27].

Mniej więcej w tym samym czasie Departament Bezpieczeństwa Wewnętrznego uruchomił program oceny obiektów prowadzony przez zespół ICS-CERT (ang. *Industrial Control System Cyber Emergency Response Team*). Pozwalał on ocenić konfigurację zabezpieczeń sprzętu i sieci zainstalowanych już w obiektach infrastruktury krytycznej. W latach 2002 – 2009 zespół przeprowadził ponad 100 ocen obiektów z różnych branż — ropy, gazu naturalnego, chemii i gospodarki wodnej — i wykrył ponad 38 tys. luk. Związane były one z krytycznymi systemami dostępnymi przez internet, domyślnymi hasłami producentów niezmodyfikowanymi przez operatorów, niemożliwymi do zmodyfikowania zapisanymi na stałe hasłami, nieaktualnymi łatkami i brakiem standardowych zabezpieczeń takich jak zapory i systemy wykrywania włamań.

Jednak choć badacze uczestniczący w testach i ocenach obiektów bardzo się starali, zmagali się z dziesięcioleciami bierności firm. Producenci potrzebowali miesięcy, a nawet lat, by załatać luki znalezione w ich systemach przez rządowych badaczy. Ponadto właściciele infrastruktury krytycznej byli gotowi wprowadzać w swoich systemach i sieciach tylko kosmetyczne zmiany, sprzeciwiając się poważniejszym modyfikacjom.

Weiss, współpracujący z INL w zakresie programu badawczego, zirytował się wspomnianą biernością i zorganizował konferencję, aby uświadomić operatorom infrastruktury krytycznej groźne problemy dotyczące zabezpieczeń ich systemów. W 2004 r. uciekł się do strategii wzbudzania strachu,

[26] *Ibid*., s. 39.

[27] Problematycznym słabym punktem w opisywanym programie badawczym jest to, że otrzymywane przez producentów raporty z opisem znalezionych w systemach luk są objęte klauzulą poufności. Producenci nie są zobowiązani informować klientów o lukach wykrytych w systemach.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

demonstrując zdalny atak w celu pokazania, co może się wydarzyć. W rolę hakera wcielił się Jason Larsen, badacz z INL, który zademonstrował atak na rozdzielnię w Idaho Falls przeprowadzony z komputera w Laboratorium Narodowym Sandia w Nowym Meksyku. Wykorzystując niedawno wykrytą lukę w oprogramowaniu serwera, Larsen ominął kilka warstw zapór, aby zhakować sterownik PLC kontrolujący rozdzielnię i w kilku etapach uwolnić przygotowany ładunek. W pierwszym kroku otworzył i zamknął wyłącznik. W drugim jednocześnie otworzył wszystkie wyłączniki. W trzecim otworzył wyłączniki i zmodyfikował dane przesyłane na ekrany operatora, aby wydawało się, że wyłączniki wciąż są zamknięte.

„Nazwałem to pokazem, który »moczy spodnie« — powiedział Weiss. — Okazał się wielkim sukcesem".

Po kilku latach Weiss przeprowadził inny pokaz, a później jeszcze następny. Za każdym razem zapraszał innych ekspertów od zabezpieczeń, aby zademonstrować inne sposoby ataku. Jedyny problem polegał na tym, że wyprzedzał swoje czasy. Za każdym razem, gdy inżynierowie wyjeżdżali z jego konferencji pełni pomysłów na poprawę bezpieczeństwa ich sieci, po powrocie do firmy natrafiali na dyrektorów niechętnych ponoszeniu kosztów zmiany architektury i zabezpieczania sieci. Dyrektorzy stwierdzali, że po co mają wydawać pieniądze na bezpieczeństwo, skoro konkurencyjne firmy tego nie robią i nikt ich nie atakuje.

Jednak to, co przez dziesięć lat nie udawało się Weissowi i laboratoriom badawczym, Stuxnet zrobił w kilka miesięcy. Ta broń cyfrowa po raz pierwszy spowodowała upublicznienie poważnych luk w krajowych systemach kontroli przemysłowej. Krytyczny sprzęt, który przez tak długi czas dla większości świata pozostawał nieznany, przyciągnął uwagę badaczy i hakerów. Zmusiło to także producentów i właścicieli infrastruktury krytycznej, by wreszcie zwrócili uwagę na omawiane problemy.

OPUBLIKOWANE W SIERPNIU 2010 r. informacje o tym, że Stuxnet miał dokonać sabotażu sterowników PLC Siemensa, zaciekawiły Dillona Beresforda, mieszkającego w Austin w Teksasie 25-letniego badacza z dziedziny zabezpieczeń komputerowych. Beresford, podobnie jak większość ludzi, nigdy nie słyszał o sterownikach PLC. Interesowało go, jak bardzo podatne mogą być one na ataki. Dlatego kupił w internecie kilka takich sterowników

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i poświęcił dwa miesiące na badanie i testowanie ich w sypialni swojego małego mieszkania. W zaledwie kilka tygodni znalazł kilka luk, które można wykorzystać w ataku.

Beresford odkrył np., że komunikacja między maszyną programisty a sterownikami PLC w ogóle nie była szyfrowana. Dlatego każdy haker, który włamał się do sieci, mógł podejrzeć i skopiować polecenia transmitowane do sterowników PLC, a później odtwarzać je sterownikowi, co pozwalało zatrzymywać go i kontrolować. Byłoby to niemożliwe, gdyby sterowniki PLC odrzucały polecenia od nieautoryzowanych komputerów. Beresford stwierdził jednak, że sterowniki PLC to „niewybredne" komputery rozmawiające z każdą maszyną posługującą się odpowiednim protokołem. Ponadto polecenia do sterowników nie musiały być cyfrowo podpisane certyfikatem udowadniającym, że instrukcje pochodzą ze źródła godnego zaufania.

Choć używany był pakiet uwierzytelniania i pewnego rodzaju hasła przesyłane między maszyną z systemem Step 7 a sterownikiem PLC, Beresford potrafił odszyfrować hasło w niecałe trzy godziny. Odkrył też, że mógł przechwycić pakiet uwierzytelniania przesyłany z maszyny z systemem Step 7 do sterownika PLC i odtworzyć go w taki sam sposób, w jaki odtwarzał polecenia. Całkowicie wyeliminował w ten sposób konieczność odszyfrowywania hasła. Po uzyskaniu kontroli nad sterownikiem PLC badacz mógł też wysłać polecenie zmieniające hasło, by zablokować dostęp prawowitym użytkownikom[28].

Beresford znalazł też inne luki, w tym tylną furtkę (ang. *backdoor*) pozostawioną przez programistów Siemensa w firmwarze sterowników PLC (**firmware** to podstawowe oprogramowanie sprzętu umożliwiającego jego pracę). Producenci często umieszczają w systemach globalne, zapisane na stałe hasła, co umożliwia im zdalny dostęp do systemów na potrzeby usuwania usterek u klientów (działa to jak funkcja OnStar, ale przeznaczona dla systemów kontroli). Jednak tylne furtki umożliwiające dostęp producentom pozwalają też wkraść się napastnikom[29]. Nazwa użytkownika i hasło

[28] Kim Zetter, „Hard-Coded Password and Other Security Holes Found in Siemens Control Systems", *Wired.com*, 3 sierpnia 2011 (*https://www.wired.com/2011/08/siemens-hardcoded-password*).

[29] Joe Weiss szacuje, że w ponad połowie wszystkich systemów kontroli znajdują się tylne furtki dodane przez producentów.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

potrzebne do otwarcia tylnej furtki Siemensa w każdym systemie były takie same: *basisk*. Dane te były zapisane na stałe w firmwarze, dlatego każdy, kto zbadał to oprogramowanie, mógł je znaleźć. Dzięki tej tylnej furtce napastnik mógł usunąć pliki ze sterownika PLC, przeprogramować go lub wysłać polecenia w celu sabotażu operacji kontrolowanych przez dany sterownik[30].

Beresford zgłosił swoje odkrycia zespołowi ICS-CERT, który we współpracy z Siemensem miał wyeliminować luki. Jednak nie każdą z nich można było usunąć. Niektóre, np. przesyłanie niezaszyfrowanych poleceń i brak silnych mechanizmów uwierzytelniania, wynikały z podstawowych założeń projektowych (a nie z błędów programistycznych). Dlatego usunięcie tych luk wymagało od Siemensa aktualizacji firmware'u w swoich systemach lub, w niektórych sytuacjach, zmiany architektury rozwiązań. Problemy te nie ograniczały się do sterowników PLC Siemensa. Przyczyną były podstawowe założenia projektowe z wielu systemów kontroli. Te założenia pochodziły z czasów przed pojawieniem się internetu, gdy urządzenia działały w odizolowanych sieciach i nie musiały być odporne na ataki z zewnątrz.

Odkrycia Beresforda zaprzeczały zapewnieniom od dawna powtarzanym przez producentów i właścicieli infrastruktury krytycznej. Zdaniem tych osób systemy były bezpieczne, ponieważ tylko ktoś z dużą wiedzą na temat sterowników PLC i doświadczeniem w pracy z nimi mógł je zaatakować. Jednak za pomocą kupionego w internecie używanego sprzętu o wartości 20 tys. dolarów Beresford, pracując przez dwa miesiące w wolnych chwilach, znalazł kilkanaście luk i poznał systemy wystarczająco dobrze, by się do nich włamać.

---

[30] Beresford znalazł też jeszcze jedną niespodziankę — „jajo wielkanocne" (ang. *Easter egg*) ukryte przez programistów Siemensa w firmwarze. Jaja wielkanocne to typowe dla branży żarty, które programiści umieszczają w programach, aby użytkownicy mogli je odnaleźć. Często można je odkryć dopiero po wpisaniu konkretnej sekwencji znaków lub otwarciu rzadko używanej części programu. W oprogramowaniu Siemensa jajem wielkanocnym była animacja przedstawiająca tańczące szympansy i niemieckie przysłowie. W luźnym tłumaczeniu oznaczało ono: „Sama praca bez rozrywki robi z człowieka nudziarza". Choć to jajo wielkanocne nie było szkodliwe, wzbudziło poważne obawy o zabezpieczenia urządzeń Siemensa. Skoro programiści ukryli żart przed wewnętrznymi recenzentami kodu, co jeszcze mogło umknąć uwadze tych ostatnich?

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Od czasu odkryć Beresforda inni badacze wykryli dalsze luki w systemach kontroli Siemensa i innych firm. Według bazy luk w systemach kontroli prowadzonej przez Wurldtech Security (producenta systemów do zabezpieczania infrastruktury krytycznej) od 2008 r. w takich systemach i ich protokołach znaleziono ok. 1000 luk. Większość z nich pozwalała napastnikom tylko na uniemożliwienie operatorom monitorowania systemu, jednak wiele problemów umożliwiało przejęcie systemu[31].

W 2011 r. firma z branży bezpieczeństwa zatrudniona przez południowokalifornijskie przedsiębiorstwo użyteczności publicznej do oceny zabezpieczeń kontrolerów w rozdzielniach znalazła wiele luk, które pozwalały napastnikom przejąć kontrolę nad urządzeniami. „Nigdy wcześniej nie zetknęliśmy się z takimi urządzeniami, jednak udało nam się znaleźć luki już pierwszego dnia — powiedział Kurt Stammberger, wiceprezes firmy Mocana. — Były to istotne, poważne problemy, znane przynajmniej od półtora roku. Jednak przedsiębiorstwo nie miało o nich pojęcia"[32].

Problemy z zabezpieczeniami systemów kontroli są nasilane przez to, że takie systemy nie są wymieniane latami. Ponadto producenci nie udostępniają regularnie łatek do takich systemów, jak to się dzieje w przypadku komputerów o ogólnym przeznaczeniu. Czas życia standardowego komputera PC wynosi od trzech do pięciu lat. Później firmy wymieniają sprzęt na nowe modele. Jednak czas życia systemu kontroli może wynosić 20 lat.

---

[31] W 2013 r. dwóch badaczy wykryło problemy z protokołem często używanym w centrach sterowania do komunikowania się ze sterownikami PLC i jednostkami RTU zainstalowanymi w rozdzielniach. Intruz niepotrafiący za pomocą internetu bezpośrednio przejąć kontroli nad maszyną w centrum sterowania mógł włamać się do urządzenia komunikacyjnego w zdalnej rozdzielni (albo przez uzyskanie fizycznego dostępu do tego urządzenia, albo włamując się do bezprzewodowej sieci radiowej służącej do komunikowania się z centrum sterowania). Następnie mógł wykorzystać lukę w protokole, aby przesyłać szkodliwe polecenia do centrum sterowania. Pozwalało to napastnikowi spowodować awarię maszyny w centrum sterowania lub wykorzystać taką maszynę do rozesłania szkodliwych poleceń do wszystkich rozdzielni, z którymi dany komputer się komunikował. W ten sposób można było, w zależności od wielkości sieci, wyłączyć za jednym posunięciem dziesiątki, a nawet setki rozdzielni. Zob. Kim Zetter, „Researchers Uncover Holes That Open Power Stations to Hacking", *Wired.com*, 16 października 2013 (*https://www.wired.com/2013/10/ics*).

[32] Jordan Robertson, „Science Fiction-Style Sabotage a Fear in New Hacks", Associated Press, 23 października 2011 (*https://phys.org/news/2011-10-science-fiction-style-sabotage-hacks.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nawet po zastąpieniu systemu nowe modele muszą komunikować się ze starszymi systemami, dlatego często zawierają wiele luk występujących też w starszych rozwiązaniach.

Jeśli chodzi o łatki, niektóre systemy kontroli korzystają z przestarzałych wersji systemu Windows, dla których Microsoft już nie zapewnia pomocy technicznej. To oznacza, że jeśli w takim oprogramowaniu będą wykryte nowe luki, nigdy nie zostaną one wyeliminowane przez producenta. Jednak nawet jeśli łatki są dostępne, w systemach kontroli są one instalowane rzadko, ponieważ operatorzy boją się błędnych poprawek, które mogłyby doprowadzić do awarii systemu. Ponadto nie można łatwo zatrzymać systemów krytycznych (i kontrolowanych przez nie procesów) na kilka godzin potrzebnych do zainstalowania łatek lub przeprowadzenia innych prac związanych z bezpieczeństwem[33].

Wszystkie te problemy są nasilane z powodu producentów, którzy coraz częściej łączą systemy bezpieczeństwa z systemami kontroli. W przeszłości systemy bezpieczeństwa były wbudowanymi systemami analogowymi konfigurowanymi niezależnie od systemów kontroli. Dzięki temu problemy z systemem kontroli nie uniemożliwiały systemom bezpieczeństwa wyłączenia sprzętu w sytuacji awaryjnej. Obecnie wielu producentów wbudowuje system bezpieczeństwa w system kontroli, przez co łatwiej jest wyłączyć oba w ramach jednego ataku[34].

Wiele luk w systemach kontroli jest mniej groźnych, gdy system działa w niezależnej, odizolowanej sieci. Taka sieć nie jest podłączona do internetu ani do innych systemów łączących się z internetem. Jednak nie zawsze stosowane jest takie rozwiązanie.

---

[33] Według Joe Weissa w 2003 r., gdy w internecie buszował robak SQL Slammer, jeden z dostawców systemów kontroli przestrzegał klientów, by nie instalowali łatki udostępnionej przez Microsoft w celu ochrony przed tym robakiem. Dostawca twierdził, że z powodu łatki system przestanie działać.

[34] Joe Weiss informuje, że systemy bezpieczeństwa w elektrowniach atomowych wciąż są, na szczęście, kontrolowane za pomocą mechanizmów analogowych. W istniejących elektrowniach tego typu ryzyko stopienia rdzenia z powodu cyberataku jest bardzo niskie. Może się to jednak zmienić, ponieważ projekty elektrowni nowej generacji obejmują cyfrowe, działające w sieci systemy, które — zdaniem Weissa — mogą ułatwić atak na takie obiekty.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2012 r. badacze z Wielkiej Brytanii znaleźli ponad 10 tys. systemów kontroli podłączonych do internetu. Były to m.in. systemy w stacjach uzdatniania wody, elektrowniach, tamach, mostach i stacjach kolejowych. Badacze posłużyli się wyspecjalizowaną wyszukiwarką Shodan potrafiącą lokalizować urządzenia takie jak telefony VoIP, odbiorniki SmartTV i systemy kontroli podłączone do internetu[35].

W 2011 r. haker pr0f uzyskał dostęp do systemów kontroli stacji uzdatniania wody w miejscowości South Houston. Haker znalazł używany przez miasto system kontroli Siemensa w internecie. Choć system był chroniony hasłem, było ono tylko trzyliterowe i odgadnięcie go nie sprawiało trudności. „Przykro mi, że nie będzie to historia o zaawansowanych zagrożeniach i tego typu rzeczach — powiedział pr0f dziennikarzowi — ale po prawdzie większość ataków, z jakimi się zetknąłem, jest wynikiem głupoty, a nie niezwykłych umiejętności technicznych napastnika"[36]. Po włamaniu do systemu SCADA pr0f zrobił zrzuty ekranu pokazujące układ zbiorników wodnych i cyfrowych mechanizmów sterowania, natomiast nie przeprowadził sabotażu systemu. „Nie lubię bezmyślnego wandalizmu. To głupie i śmieszne — napisał w opublikowanym w internecie wpisie. — Z drugiej strony, to samo dotyczy podłączania interfejsu maszynerii z systemem SCADA do internetu"[37].

Liczne urządzenia polowe z systemem SCADA niepodłączone bezpośrednio do publicznego internetu są dostępne za pomocą modemu i zabezpieczone tylko hasłem domyślnym. Na przykład dla przełączników

[35] Kim Zetter, „10K Reasons to Worry About Critical Infrastructure", *Wired.com*, 24 stycznia 2012 (*https://www.wired.com/2012/01/10000-control-systems-online*). Badacz Eireann Leverett nie był w stanie ustalić, ile z tych systemów było narzędziami produkcyjnymi, a ile demonstracyjnymi. Nie potrafił też stwierdzić, ile z nich było systemami krytycznymi, a ile odpowiadało np. za system ogrzewania biura w elektrowni. Leverett zidentyfikował jednak systemy kontroli infrastruktury wodnej w Irlandii i oczyszczalni ścieków w Kalifornii. Ponadto nawet system ogrzewania można czasem wykorzystać do uzyskania dostępu do innych części sieci. Tylko 17% spośród 10 tys. znalezionych systemów żądało autoryzacji. W niektórych sytuacjach właściciele nawet nie wiedzieli, że ich systemy są dostępne w internecie.

[36] Paul F. Roberts, „Hacker Says Texas Town Used Three Character Password to Secure Internet Facing SCADA System", blog Threatpost, 20 listopada 2011 (*https://threatpost.com/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system-11201/75914/*).

[37] Wypowiedź pojawiła się w witrynie Pastebin 18 listopada 2011 r. (*https://pastebin.com/Wx90LLum*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i wyłączników w sieci zasilania często używane są hasła domyślne, dzięki czemu pracownicy potrzebujący w sytuacjach awaryjnych dostępu do tych komponentów będą pamiętać hasło. Z tego samego powodu systemy kontroli zwykle nie są projektowane w taki sposób, aby blokować dostęp po kilkukrotnym podaniu błędnego hasła (co jest standardowym zabezpieczeniem w wielu systemach informatycznych, zapobiegającym złamaniu hasła przez atak siłowy za pomocą wielu prób). Nikt nie chce, aby system kontroli zablokował dostęp operatorowi, który w panice kilka razy błędnie wpisał hasło. W 2011 r. zespół kierowany przez badacza zabezpieczeń Marca Maiffreta włamał się do systemu zdalnego dostępu w zakładzie uzdatniania wody w południowej Kalifornii i przejął kontrolę nad sprzętem używanym do dodawania chemikaliów do wody pitnej. Zespół uzyskał kontrolę nad systemem w jeden dzień, a Maiffret stwierdził, że wystarczyłoby kilka dalszych kroków, aby dodać chemikalia do wody i sprawić, by przestała się ona nadawać do picia[38].

Umożliwianie zdalnego dostępu z poziomu internetu do systemów krytycznych jest oczywistym zagrożeniem bezpieczeństwa. Jeśli jednak Stuxnet był czegoś dowodem, to tego, że napastnicy nie potrzebują zdalnego dostępu, by zaatakować system. Autonomiczny robak może zostać wprowadzony za pomocą pendrive'a lub plików projektu używanych przez inżynierów do programowania sterowników PLC. W 2012 r. do firmy Telvent Canada, producenta oprogramowania sterującego używanego w inteligentnych sieciach, włamali się intruzi wiązani z chińskim wojskiem. Napastnicy szukali plików projektów produkowanego przez firmę systemu SCADA instalowanego w Stanach Zjednoczonych w rurociągach naftowych i gazociągach oraz w systemach gospodarki wodnej. Firma Telvent korzystała z tych plików do zarządzania systemami klientów. Choć nigdy nie ujawniła, czy napastnicy zmodyfikowali pliki projektów, to włamanie pokazało, jak łatwo można zaatakować rurociągi naftowe i gazociągi, infekując pliki projektów firmy takiej jak Telvent[39].

[38] Ken Dilanian, *Virtual War a Real Threat*, „Los Angeles Times", 28 marca 2011.

[39] Kim Zetter, „Chinese Military Linked to Hacks of More Than 100 Companies", *Wired.com*, 19 lutego 2013 (*https://www.wired.com/2013/02/chinese-army-linked-to-hacks*). Więcej informacji o włamaniu do firmy Telvent znajdziesz w: Kim Zetter, „Maker of Smart-Grid Control Software Hacked", *Wired.com*, 26 września 2012 (*https://www.wired.com/2012/09/scada-vendor-telvent-hacked*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bezpośrednie włamania do sieci komputerowych nie są jedynym problemem związanym z infrastrukturą krytyczną. Istnieją udokumentowane przypadki zastosowania impulsów elektromagnetycznych zakłócających prace systemów SCADA i urządzeń polowych. W listopadzie 1999 r. system radarowy okrętu Marynarki Wojennej Stanów Zjednoczonych, który w trakcie manewrów znalazł się 40 km od brzegów San Diego, zakłócił działanie sieci bezprzewodowej systemów SCADA lokalnych zakładów uzdatniania wody i elektrowni. Zakłócenia uniemożliwiły pracownikom otwieranie i zamykanie zaworów rurociągu, przez co technicy musieli udać się w odpowiednie miejsca i ręcznie ustawić zawory, aby zapobiec przepełnieniu zbiorników przez wodę. Zakłócenia impulsami elektromagnetycznymi były też przyczyną eksplozji gazu, która wydarzyła się w pobliżu holenderskiego portu morskiego Den Helder pod koniec lat 80., kiedy to system radarowy okrętu spowodował, że system SCADA gazociągu zaczął otwierać i zamykać zawór[40].

PRZEZ LATA ZBADANYCH zostało wiele scenariuszy opisujących „dzień zagłady" spowodowany poważnym cyberatakiem[41]. Jednak do tej pory żaden taki atak nie nastąpił, a przypadkowe wypadki związane z systemami kontroli są znacznie liczniejsze niż celowe uszkodzenia takich urządzeń.

Wystarczy jednak przyjrzeć się przypadkowym katastrofom w przemyśle, aby zrozumieć zakres szkód, jakie cyberatak *mógłby* spowodować. Do skutków spowodowanych wypadkami w przemyśle często można doprowadzić także celowym atakiem. Inteligentny haker mógłby przeanalizować przyczyny i skutki wypadków opisywanych w serwisach informacyjnych

[40] „Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack", kwiecień 2008 (*http://empcommission.org/docs/A2473-EMP_Commission-7MB.pdf*). Zob. też przypis 25. w rozdziale 11, gdzie opisany jest plan celowego ataku z użyciem impulsów elektromagnetycznych.

[41] Przeprowadzone w 1996 r. przez organizację RAND badania The Day After… in Cyberspace były jednymi z pierwszych, w których opisano konsekwencje jednoczesnego ataku na samoloty, pociągi, systemy telefoniczne i bankomaty na wielu kontynentach. Zob. Robert H. Anderson, Anthony C. Hearn, „An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After… in Cyberspace II", RAND, 1996 (*http://www.rand.org/pubs/monograph_reports/MR797.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i wykorzystać uzyskane dane do zaprojektowania ataku, który doprowadziłby do takich samych niszczycielskich efektów.

Generał Keith Alexander z NSA przytoczył katastrofalny wypadek w Sajańsko-Szuszeńskiej Elektrowni Wodnej na południu Syberii jako przykład tego, co mogłoby się wydarzyć w wyniku ataku[42]. Działająca tam 30-letnia tama, szósta z największych na świecie, miała ponad 240 m wysokości i rozciągała się na szerokość 800 m w wąwozie rzeki Jenisej. W 2009 r. tama zawaliła się. W wypadku zginęło 75 osób.

Tuż po północy 17 sierpnia 940-tonowa turbina w elektrowni została poddana nagłemu wzrostowi ciśnienia wody, co doprowadziło do wyrwania urządzenia i wyrzucenia go w powietrze. Gdy strumień wody zalał maszynownię przez szyb, w którym była zamontowana turbina, spowodował poważne uszkodzenia kilku kolejnych turbin. Skutkiem były liczne eksplozje i zawalenie się dachu.

Za jedną z przyczyn katastrofy uznany został pożar elektrowni w Bracku ok. 800 km dalej. Pożar spowodował spadek dostaw energii z Bracka. To sprawiło, że turbiny w Sajańsko-Szuszeńskiej Elektrowni Wodnej musiały dostarczyć więcej prądu. Niestety, czas życia jednej z tych turbin dobiegał już końca. Urządzenie od czasu do czasu wpadało w niebezpieczne wibracje. Kilka miesięcy wcześniej zainstalowany został nowy system kontroli, aby ustabilizować turbinę. Niestety, to nie wystarczyło, by poradzić sobie z wibracjami spowodowanymi zwiększeniem obciążenia. Turbina wyrwała przytrzymujące ją śruby. Na nagraniach z systemu monitoringu widać, jak pracownicy starają się uciec z miejsca katastrofy. Wypadek spowodował nie tylko śmierć 75 osób i zalanie okolicy, ale też wyciek 100 t ropy do Jeniseju i zabicie 4000 t pstrągów w lokalnych zakładach rybnych. Eksperci oszacowali, że remont zajmie cztery lata i będzie kosztował 1,3 mld dolarów[43].

Eksplozja rurociągu, która wydarzyła się w stanie Waszyngton w czerwcu 1999 r., też ilustrowała schemat możliwy do wykorzystania przez hakerów. W tym przypadku należący do firmy Olympic Pipe Line Company w Bellingham rurociąg o średnicy 40 cm pękł, co spowodowało wyciek prawie 900 m^3

[42] Bill Gertz, *Computer-Based Attacks Emerge as Threat of Future, General Says*, „Washington Times", 13 września 2011.

[43] Joe P. Hasler, *Investigating Russia's Biggest Dam Explosion: What Went Wrong*, „Popular Mechanics", 2 lutego 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

benzyny do strumienia w parku Whatcom Falls. Paliwo wydostawało się z rury przez 90 min, po czym nastąpił wybuch. Ogień rozciągał się na prawie 2,5 km, zabijając dwóch 10-latków i nastolatka oraz raniąc 8 innych osób. Choć przyczyną tej katastrofy było wiele czynników, w tym niewłaściwie skonfigurowane zawory i koparka, która naruszyła fragment rury, pewną rolę odegrał też niereagujący system kontroli. „Gdyby komputery z systemem SCADA reagowały na polecenia od kontrolerów firmy Olympic — stwierdzili śledczy — kontroler zarządzający rurociągiem prawdopodobnie zdołałby podjąć działania i zapobiec wzrostowi ciśnienia, który doprowadził do pęknięcia rury”[44].

Operatorzy dowiedzieli się o wycieku dopiero po przeszło godzinie. Okoliczni mieszkańcy dzwonili już wtedy pod numer alarmowy 911, aby zgłosić wyraźny zapach benzyny w strumieniu. Choć wyciek nie został spowodowany przez hakerów, śledczy odkryli w systemie firmy Olympic wiele problemów z zabezpieczeniami narażających ten system na atak. Firma skonfigurowała np. zdalny dostęp wdzwaniany do systemu kontroli SCADA. Dostęp był zabezpieczony tylko nazwą użytkownika i hasłem. Ponadto sieć biznesowa i sieć systemu SCADA były ze sobą połączone. Choć były powiązane mostkiem, który w pewnym stopniu zabezpieczał sieci przed przypadkowymi intruzami, w połączeniu nie używano solidnej zapory, ochrony przed wirusami ani systemu monitorowania dostępu. Zwiększało to ryzyko, że zdeterminowany napastnik włamie się do sieci biznesowej z poziomu internetu, a następnie uzyska dostęp do krytycznej sieci systemu SCADA.

Eksplozja gazociągu w San Bruno w Kalifornii (2010 r.) to następna sytuacja, która może posłużyć za przestrogę. Nastąpiła po tym, jak w wyniku konserwacji zasilacza UPS nastąpiła przerwa w dostawie energii do systemu SCADA. Zawór kontrolny w rurociągu był zaprogramowany w taki sposób, aby po utracie zasilania przez system SCADA automatycznie się otwierał. W efekcie gaz bez przeszkód wpływał do rurociągu, co spowodowało wzrost ciśnienia w tej starzejącej się strukturze i w konsekwencji wybuch.

[44] „Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999”, tekst opublikowany przez Narodową Radę Bezpieczeństwa Transportu, 2002 (*https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ponieważ system SCADA był pozbawiony zasilania, operatorzy nie wiedzieli, co się dzieje w rurociągu[45].

Następnie puściła zapora na rzece Missouri w grudniu 2005 r. Katastrofę zapoczątkowało odłączenie się czujników na tamie od ich stanowisk. W efekcie czujniki nie wykryły, że mieszczący ponad 5,5 mln m^3 wody zbiornik się zapełnił. Gdy pompy cały czas pompowały wodę do zbiornika, zawiódł także system awaryjnego zamykania dopływu[46]. Przepełnienie nastąpiło o 5:10 rano. Po sześciu minutach puścił 18-metrowy fragment bariery. Ponad 3,7 mln m^3 wody wylało się na górę Proffit, porywając skały i drzewa. Później woda wlała się do parku stanowego Johnson's Shut-Ins, gdzie zmyła dom nadzorcy (z nim samym i jego rodziną w środku). Budynek zatrzymał się kilkaset metrów dalej[47]. Nikt nie odniósł poważnych obrażeń, jednak fala zmyła też samochody z pobliskiej autostrady, a kemping w parku został zalany. Na szczęście cała sytuacja zdarzyła się zimą, dlatego kemping był pusty.

Cyfrowe ataki można też wzorować na wypadkach kolejowych. Systemy zarządzające pociągami pasażerskimi obejmują wiele — często wzajemnie powiązanych — komponentów, co daje sporo możliwych dróg ataku. Te komponenty to: systemy kontroli dostępu uniemożliwiające osobom bez biletów wchodzenie na stacje, systemy operatorów kart kredytowych, systemy reklamy cyfrowej, systemy zarządzania światłami lub systemy telewizji przemysłowej. Nie wspominam tu nawet o krytycznych systemach przeciwpożarowych i reagowania kryzysowego, sterowaniu szlabanami na skrzyżowaniach i sygnalizacją oraz kierowaniu samymi pociągami. W przeszłości te systemy były od siebie oddzielone i komunikowały się ze sobą wyłącznie

[45] „Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire", Narodowa Rada Bezpieczeństwa Transportu, 9 września 2010 (*https://www.ntsb.gov/news/events/Pages/Pacific_Gas_and_Electric_Company_Natural_Gas_Transmission_Pipeline_Rupture_and_Fire_San_Bruno_California.aspx*).

[46] J. David Rogers, Conor M. Watkins, „Overview of the Taum Sauk Pumped Storage Power Plant Upper Reservoir Failure, Reynolds County, MO", prezentacja na 6. Międzynarodowej Konferencji Studiów Przypadków z Dziedziny Inżynierii Geotechnicznej, Arlington, 11 – 16 sierpnia 2008 (*http://web.mst.edu/~rogersda/dams/2_43_rogers.pdf*).

[47] Emitt C. Witt III, „December 14th, 2005 Taum Sauk Dam Failure at Johnson's Shut-Ins Park in Southeast Missouri", Narodowa Służba Oceaniczna i Meteorologiczna (*https://www.weather.gov/media/lsx/Events/12_15_2005.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

drogą kablową. Jednak dziś takie systemy są w coraz większym stopniu cyfrowe i wzajemnie powiązane. Używane są też systemy komunikujące się za pomocą sygnałów radiowych i przesyłające niezaszyfrowane polecenia. Choć w systemach kolejowych stosowane są mechanizmy rezerwowe i zabezpieczenia zapobiegające wypadkom, to w sytuacji, gdy wiele systemów jest wzajemnie powiązanych, mogą pojawić się błędy w konfiguracji umożliwiające dostęp do systemów bezpieczeństwa i uszkodzenie ich.

Dwudziestego drugiego czerwca 2009 r. pociąg pasażerski w systemie metra Waszyngtonu zderzył się w godzinach popołudniowego szczytu z innym, stojącym pociągiem. W wypadku zginęli jeden z maszynistów i 8 pasażerów, a 80 zostało rannych. Źle działające czujniki w torach nie wykryły stojącego pociągu i nie poinformowały o nim poruszającej się maszyny. Choć jadący pociąg był wyposażony w czujniki przeciwzderzeniowe, które powinny włączyć hamulce w odległości 365 m od innych pojazdów, także ten system nie zadziałał. Ponadto operator nie uruchomił ręcznych hamulców. Dziesięć lat wcześniej przekaźniki komunikacyjne w tym samym systemie metra kilkakrotnie przesłały pociągom błędne instrukcje. Raz zdarzyło się, że nakazały pociągowi jazdę z prędkością ponad 70 km/h w obszarze z ograniczeniem prędkości do 25 km/h[48].

Wszystkie te sytuacje były dziełem przypadku, jednak w Polsce w 2008 r. 14-latek z Łodzi spowodował wykolejenie kilku tramwajów, wykorzystując promiennik podczerwieni ze zmodyfikowanego pilota do telewizora, aby przejąć kontrolę nad kolejowym systemem sygnalizacji i przełączyć zwrotnice. Cztery tramwaje wypadły z torów, a 12 osób zostało rannych[49].

CHOĆ ISTNIEJE WIELE różnych możliwości zaatakowania infrastruktury krytycznej, jedną z najskuteczniejszych jest atak na sieć zasilania. Wynika to z tego, że elektryczność stanowi podstawę całej infrastruktury krytycznej. Jeśli na dłuższy czas odetniesz zasilanie, wpłynie to na wiele krytycznych usług i obiektów: pociągi pasażerskie, światła drogowe, banki, giełdy, szkoły, instalacje wojskowe, lodówki utrzymujące temperaturę żywności i zasobów krwi, respiratory, systemy monitorowania pracy serca, inny ważny

[48] Lyndsey Layton, *Metro Crash: Experts Suspect System Failure, Operator Error in Red Line Accident*, „Washington Post", 23 czerwca 2009.

[49] Graeme Baker, *Schoolboy Hacks into City's Tram System*, „Telegraph", 11 stycznia 2008.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

sprzęt w szpitalach, światła na pasach startowych czy systemy kontroli ruchu lotniczego. W niektórych krytycznych obiektach mogą się uruchomić generatory awaryjne. Jednak przy przedłużającym się braku prądu generatory nie wystarczą. Ponadto w elektrowniach atomowych przełączenie się na zasilanie z generatorów skutkuje automatycznym stopniowym wyłączaniem obiektu (wynika to z regulacji prawnych).

Sposobem na uszkodzenie sieci zasilania jest atak na inteligentne liczniki instalowane w Stanach Zjednoczonych w tysiącach domów i firm. Jedną z przyczyn popularności tych urządzeń jest kosztujący 3 mld dolarów rządowy program rozwoju inteligentnych sieci, który przyspieszył wprowadzanie inteligentnych liczników bez wcześniejszego upewnienia się, czy ta technologia jest bezpieczna.

Do podstawowych problemów odkrytych przez badaczy należy to, że inteligentne liczniki posiadają funkcję zdalnego odłączania. Dzięki temu firmy użyteczności publicznej mogą włączyć lub wyłączyć zasilanie budynku bez konieczności wysyłania technika. Jednak ta funkcja pozwala też napastnikom przejąć kontrolę nad licznikami i wyłączyć prąd u tysięcy klientów w sposób, którego skutki trudno będzie odwrócić. W 2009 r. badacz Mike Davis napisał robaka, który działał w ten właśnie sposób.

Davis został zatrudniony przez firmę energetyczną z Wybrzeża Północno-Zachodniego, by zbadać bezpieczeństwo inteligentnych liczników, które firma chciała zainstalować u klientów. Stwierdził, że te liczniki (podobnie jak badane przez Beresforda sterowniki PLC Siemensa) były „niewybredne" i komunikowały się z wszystkimi innymi inteligentnymi licznikami w pobliżu, o ile oba urządzenia używały tego samego protokołu komunikacyjnego. Liczniki akceptowały nawet aktualizacje firmware'u od innych takich urządzeń. Napastnik w celu zmiany firmware'u w liczniku musiał tylko ustalić stosowany w sieci klucz szyfrujący. Jednak ponieważ wszystkie liczniki, jakie firma planowała zainstalować, miały zapisany w firmwarze ten sam klucz, napastnik musiał tylko włamać się do jednego urządzenia, znaleźć w nim klucz, a następnie wykorzystać go do przesłania szkodliwych aktualizacji do innych liczników. „Po uzyskaniu kontroli nad jednym urządzeniem miałem w zasadzie wszystko, czego potrzebowałem — powiedział Davis. — Dotyczyło to różnych sprawdzanych liczników od różnych producentów"[50].

[50] Z wywiadu przeprowadzonego przez autorkę w sierpniu 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Liczniki komunikowały się między sobą drogą radiową. Stale pracowały w trybie nasłuchu, aby wykrywać inne liczniki w pobliżu. Niektóre liczniki potrafiły komunikować się z innymi oddalonymi o kilka kilometrów. Urządzenie sprawdzane przez Davisa miało zasięg ok. 120 m, czyli trochę więcej niż długość boiska do piłki nożnej. Jednak ta odległość całkowicie wystarczała, aby przekazać między sąsiednimi domami szkodliwe aktualizacje, które wyłączały zasilanie i przesyłały robaka do kolejnych urządzeń. Davis nie musiał nawet włamywać się do licznika zamontowanego w domu, aby rozpocząć infekcję. Wystarczyło, że kupił urządzenie tej samej marki (używające tego samego protokołu), umieścił w nim złośliwe oprogramowanie i potrzebny klucz szyfrujący oraz postawił je w pobliżu domu z zainstalowanym licznikiem. „Dzięki łączności radiowej licznik zostanie automatycznie wykryty [przez inne liczniki w pobliżu]" — powiedział. Po zakończeniu aktualizacji zaatakowany licznik wznawiał pracę z nowym firmware'em i automatycznie zaczynał rozsyłać aktualizację do innych liczników w jego zasięgu, co początkowało reakcję łańcuchową. Operatorzy dowiedzieliby się o zmianach w licznikach dopiero po wykryciu spadku zużycia prądu w danej okolicy.

Liczniki są zwykle aktualizowane zdalnie za pomocą centralnej sieci przedsiębiorstwa energetycznego lub przez pracującego w terenie technika, który używa podłączonego do laptopa specjalnego klucza sprzętowego w celu bezprzewodowej komunikacji z licznikami. Dlatego gdy Davis poinformował producenta, że może napisać oprogramowanie rozprzestrzeniające się automatycznie z jednego licznika na następny bez konieczności używania centralnego komputera lub klucza sprzętowego, producent wyśmiał go i stwierdził, że liczniki nie potrafią inicjować aktualizacji firmware'u w innych licznikach. „Powiedział nam […] że nie należy to do zestawu funkcji liczników — wspomina Davis. — Odpowiedzieliśmy, że wiemy o tym, i sami dodaliśmy taką funkcję [do naszej szkodliwej aktualizacji firmware'u]". Producent wciąż nie wierzył, że robak może wyrządzić jakieś szkody, dlatego Davis napisał program symulujący infekcję w dzielnicy mieszkaniowej Seattle. Program ten w ciągu dnia zainfekował 20 tys. inteligentnych liczników[51]. „W ciągu 24-godzinnego cyklu program opanował wszystkie liczniki"

[51] W serwisie YouTube możesz zobaczyć film ilustrujący wspomnianą symulację: *https://www.youtube.com/watch?v=kc_ijB7VPd8*. Pod adresem: *https://ioactive.com/services/scada-smart-grid-assessment.html* znajdziesz odnośniki do prezentacji Davisa i dwóch innych symulacji dotyczących inteligentnych liczników.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

— powiedział Davis. Infekcja rozprzestrzeniała się licznik po liczniku, jednak rzeczywisty atak przebiegałby znacznie szybciej, ponieważ napastnik mógł uruchomić wiele aktualizacji firmware'u z użyciem zestawu „pacjentów zero" zlokalizowanych w strategicznych punktach miasta.

Producent wyśmiał także symulację Davisa. Stwierdził, że aktualizacja firmware'u każdego licznika zajęłaby robakowi od dwóch do czterech minut, a przez ten czas technicy zauważyliby przerwy w dostawie prądu przed utratą zasilania przez większą liczbę klientów i wysłaliby zdalnie aktualizację firmware'u w celu ponownego włączenia elektryczności.

Wtedy Davis zadał ostateczny cios i poinformował producenta, że szkodliwe oprogramowanie nie tylko wyłączało zasilanie, ale też usuwało funkcję aktualizowania firmware'u w licznikach, dlatego nie można ich było ponownie zaktualizować w celu przywrócenia zasilania. Technicy musieliby wymienić liczniki w każdym domu lub odesłać je do warsztatu i zainstalować w nich nowy firmware. „To zainteresowało go bardziej niż wcześniejsze informacje — opowiadał Davis. — Udało nam się udowodnić, że sytuacja może wymknąć się spod kontroli, zanim firma zdąży wykryć, co się dzieje".

Davis zauważył, że od czasu przeprowadzenia symulacji producent usprawnił liczniki. Niektórzy producenci stosują w licznikach różne klucze sieciowe, przypisując inne klucze do rozmaitych obszarów. Ogranicza to zakres uszkodzeń, jakie napastnik może spowodować za pomocą jednego klucza. Jednak w większości inteligentnych liczników występuje problem zdalnego odłączania, ponieważ napastnik, który włamie się na centralny serwer elektrowni, będzie mógł zrobić to co robak Davisa, ale w znacznie łatwiejszy sposób. „Gdyby [zdalne odłączanie] nie było możliwe, żadna z opisanych kwestii nie byłaby poważnym problemem — powiedział Davis. — Moim zdaniem jeśli wbudowana jest funkcja zdalnego odłączania, to niezależnie od tego, czy jest ona aktywna, czy nie […] stanowi naprawdę istotny problem".

Zaatakowanie inteligentnych liczników to skuteczny sposób na odcięcie elektryczności. Jeszcze skuteczniejszą akcją o większym zasięgu rażenia może być wyłączenie generatorów zasilających sieć lub systemów przesyłu dostarczających prąd do odbiorców. Sekretarz obrony Leon Panetta na posiedzeniu oceniającym w czerwcu 2011 r. stwierdził, że następnym Pearl Harbor dla państwa może okazać się cyberatak, który spowoduje wyłączenie sieci zasilania.

Sieć zasilania w Ameryce Północnej jest duża i złożona. Składa się z trzech rozbudowanych regionalnych sieci: wschodniej, zachodniej i teksaskiej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Te sieci obejmują ponad 720 tys. km linii przesyłowych wysokiego napięcia, których właścicielami i operatorami jest ponad 3000 przedsiębiorstw użytku publicznego. Ponieważ handel elektrycznością odbywa się na giełdach energii, prąd jest czasem przesyłany na długie dystanse wewnątrz poszczególnych stanów i między nimi, aby zaspokoić zapotrzebowanie. Tak działa np. Cal-ISO — firma, do której włamano się w 2001 r. Choć istnienie wielu niezależnych systemów oznacza, że atak na jedną firmę lub rozdzielnię będzie miał ograniczony zasięg, to powiązania między sieciami sprawiają, iż skoordynowana i strategicznie zaplanowana akcja skierowana przeciw kilku systemom może kaskadowo spowodować serię awarii, które trudno będzie naprawić. Może to na tygodnie pogrążyć użytkowników w ciemnościach[52].

Na przykład wyłączniki monitorujące linie przesyłowe są zaprojektowane tak, by wykrywały niebezpieczne impulsy i odłączały linię od sieci, aby zapobiec uszkodzeniom. Ale gdy jeden wyłącznik zadziała, prąd z danej linii musi zostać przekierowany do innych. Jeśli możliwości tych linii zostaną przekroczone, ich wyłączniki także się aktywują, co doprowadzi do przerwy w dostawie prądu. Dobrze opracowany atak może spowodować aktywowanie wyłączników na niektórych liniach i zmianę ustawień na innych, tak by wyłączniki nie zadziałały, co doprowadzi do przegrzania się linii po przekroczeniu ich możliwości.

Przegrzanie się linii przesyłowych skutkuje ich zwisaniem lub stopieniem. Zwisające linie były powodem przerw w dostawie prądu na północy w 2003 r., które to przerwy odcięły od elektryczności 50 mln osób w ośmiu stanach i w części Kanady. Choć to nie cyfrowy atak był powodem tej sytuacji, błędy w oprogramowaniu uniemożliwiły wczesne wykrycie problemu i zapobieżenie kaskadowym awariom.

Problem rozpoczął się w Ohio, gdzie zwisające linie zasilania zaplątały się w drzewa. Sytuację pogorszył fakt, że system alarmowy w centrum kontrolnym firmy FirstEnergy w regionie Akron nie zarejestrował awarii w systemie,

[52] Organizacja NERC opracowała regulacje z zakresu cyberbezpieczeństwa, do których powinny się stosować przedsiębiorstwa użytku publicznego. Te regulacje dotyczą jednak tylko masowych systemów elektrycznych (zdefiniowanych jako obiekty i systemy operujące na napięciu przynajmniej 100 kV), a zgodność z nimi nie gwarantuje, że system nie zostanie złamany. Zabezpieczenia ewoluują (nie są czymś statycznym) i mogą się zmieniać w wyniku instalacji każdego nowego sprzętu lub modyfikacji konfiguracji.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

przez co operatorzy nie wiedzieli o pogarszającym się stanie sieci. Mniej więcej 2,5 godz. przed przerwaniem dostaw prądu odbiorcy przemysłowi, a nawet przedstawiciele innych elektrowni zaczęli dzwonić do FirstEnergy, aby zgłosić niskie napięcie i wyłączające się linie przesyłowe. Wskazywało to na poważne problemy w sieci. Jednak ponieważ operatorzy w firmie FirstEnergy nie widzieli na ekranach kontrolnych oznak problemów, założyli, że problem leży gdzie indziej. „[W American Electric Power] musiała nastąpić poważna awaria" — wyjaśnił jeden z operatorów w FirstEnergy dzwoniącemu klientowi, obwiniając inną firmę energetyczną[53]. Dopiero gdy światła w sterowni FirstEnergy zgasły, operatorzy zrozumieli, że problem dotyczył ich własnego systemu. Ostatecznie stwierdzili, że za awarię systemu ostrzegania odpowiadał błąd w oprogramowaniu. „Do tego dnia [błąd] nigdy się nie ujawnił — powiedział później rzecznik FirstEnergy. — Problem był ukryty tak głęboko, że znalezienie go wymagało tygodni analizowania milionów wierszy kodu i danych"[54].

Jeszcze bardziej niszczycielski atak dotyczyłby nie linii przesyłowych, ale sprzętu w rozdzielniach zasilających te linie. Sieć składa się z ponad 15 tys. węzłów (rozdzielni) trzech typów. Obejmują one: generatory wytwarzające prąd, rozdzielnie przesyłowe rozdzielające elektryczność między linie i rozdzielnie dystrybucyjne dostarczające zasilanie klientom. Najwięcej jest rozdzielni przesyłowych, odpowiadających za „zwiększenie" napięcia na potrzeby przesyłu prądu na duże odległości i późniejsze „zmniejszenie" go przed dostarczeniem prądu użytkownikom końcowym. Niedawne badania przeprowadzone przez Federalną Komisję ds. Regulacji Energii wykazały, że atak niszczący tylko dziewięć krytycznych rozdzielni (cztery w sieci wschodniej, trzy w sieci zachodniej i dwie w sieci teksańskiej) może spowodować ogólnokrajowe braki w dostawie prądu trwające tygodnie, a nawet miesiące, powodując panikę i zagrożenie życia[55].

---

[53] US-Canada Power System Outage Task Force, „Final Report on the August 14th Blackout in the United States and Canada", kwiecień 2004 (*https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf*).

[54] Kevin Poulsen, „Software Bug Contributed to Blackout", *SecurityFocus.com*, 11 lutego 2004 (*http://www.securityfocus.com/news/8016*).

[55] Rebecca Smith, *U.S. Risks National Blackout from Small-Scale Attack*, „Wall Street Journal", 12 marca 2004.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dobra wiadomość jest taka, że ponieważ właścicielami i operatorami systemów w tej sieci są różne firmy, używane są odmienne urządzenia i konfiguracje. Dlatego trudno jest zastosować te same techniki do szeroko zakrojonego jednego ataku na systemy z branży energetycznej. Jednak lokalne akcje prowadzące do przerw w dostawie prądu są w zasięgu przeciętnych hakerów. Ponadto atak uszkadzający duże generatory w elektrowniach utrudnia usunięcie awarii. Właśnie to miał udowodnić test Aurora Generator.

NAZWANY IMIENIEM RZYMSKIEJ bogini będącej matką czterech wiatrów test był wynikiem kaskadowo rozprzestrzeniających się awarii w regionie północnym w 2003 r. Problemy trwały tylko dwa dni, jednak niektórzy ludzie zaczęli wtedy zastanawiać się nad zagrożeniem zdalnymi atakami, których skutków nie da się tak łatwo naprawić. Mike Assante był odpowiedzialny za zorganizowanie zespołu, który przetestuje tę hipotezę.

W 2001 r. Assante był oficerem wywiadu marynarki wojennej i został przydzielony do pracy w nowym Narodowym Centrum Ochrony Infrastruktury prowadzonym przez FBI w Waszyngtonie. Badał tam zagrożenia cyberatakami na infrastrukturę energetyczną. Po roku odszedł z marynarki wojennej i został zatrudniony w American Electric Power (AEP) w Ohio — jednej z największych firm energetycznych w kraju. AEP chciała pomóc w realizacji programu ochrony infrastruktury. To wtedy Assante zaczął się zastanawiać nad atakami, które mogłyby doprowadzić do fizycznego uszkodzenia sieci.

Gdy pracował w AEP, zainteresował go artykuł z gazety „Washington Post" poświęcony programowi badawczemu systemów SCADA w Narodowym Laboratorium Idaho. Osoby uczestniczące w tym programie przestraszyły prezesa Federalnej Komisji ds. Regulacji Energii symulacją pokazującą, jak łatwo haker może uszkodzić turbinę, wyłączając mechanizm odpowiedzialny za smarowanie maszyny. Bez smarowania ruchomych metalowych części turbina zaczęła się zacinać, a następnie rozpadła się[56]. Prezes zareagował na to bardzo intensywnie. „Żałowałem, że nie miałem założonego pampersa" — powiedział po teście gazecie „Post"[57].

[56] Ten scenariusz był podobny do rzeczywistego wypadku w rozlewni firmy Coors w 2004 r., kiedy to pracownik pomyłkowo zmienił ustawienia systemu odpowiedzialnego za smarowanie łożysk maszyny konfekcjonującej. Zamiast smarować łożyska co 20 min, system robił to co 8 godz., przez co ostatecznie maszyna się zacięła.

[57] Justin Blum, *Hackers Target US Power Grid*, „Washington Post", 11 marca 2005.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Assante odwiedził pracownię INL i był pod wrażeniem grupy ekspertów, których zrekrutowano do programu. Oprócz inżynierów systemów kontroli laboratorium zatrudniło grupę „wojowników od kodu" — osób świeżo po szkole średniej lub college'u, które wiedziały, jak włamywać się do takich systemów. Te osoby łatwo łamały zabezpieczenia sieci systemów kontroli, wykorzystując słabe punkty niewidoczne dla inżynierów od lat pracujących nad takimi systemami. Laboratorium miało też własne rozdzielnie i małą sieć — 11-kilometrowy odcinek nadmiarowej sieci, którą badacze mogli odizolować od sieci publicznej. Na tych elementach pracownicy przeprowadzali testy praktyczne. Assantego na tyle zaciekawiła możliwość prowadzenia rzeczywistych badań na sieci (w odróżnieniu od samych symulacji), że w 2005 r. rzucił pracę w AEP i przyjął posadę w laboratorium.

Razem ze współpracownikami zaczął rozważać scenariusze, które mogły prowadzić do zniszczenia sprzętu. Do tego czasu większość obaw w obszarze cyberbezpieczeństwa sieci dotyczyła włamań do sieci zasilania w celu otwarcia wyłączników i doprowadzenia do awarii zasilania. Wprawdzie awarię zasilania można stosunkowo szybko wyeliminować, ponownie ustawiając wyłączniki, co się jednak stanie, jeśli napastnik złamie lub ominie zabezpieczenia i systemy bezpieczeństwa, aby fizycznie uszkodzić generator, którego nie da się łatwo naprawić?

Pracownicy laboratorium postanowili skoncentrować się na ataku na generator na przekaźnikach ochronnych — urządzeniach monitorujących zmiany w sieci i odpowiedzialnych za aktywowanie wyłączników, gdy warunki zaczynają grozić uszkodzeniem linii przesyłowych. Nieaktywne przekaźniki ochronne były jednym z powodów poważnej awarii w lutym 2008 r., kiedy to prawie 600 tys. osób na Florydzie straciło zasilanie, po tym jak inżynier z firmy Florida Power and Light wyłączył przekaźniki w rozdzielni w trakcie sprawdzania niedziałającego przełącznika[58]. Gdy na sprawdzanej linii nastąpiło zwarcie, zabrakło urządzenia, które mogłoby powstrzymać rozprzestrzenienie się problemu. W efekcie nastąpiła kaskadowa awaria zasilania, która objęła 38 rozdzielni, w tym obiekt dostarczający prąd do elektrowni atomowej, co spowodowało rozpoczęcie automatycznego wyłączania tej ostatniej.

[58] Florida Power and Light, „FPL Announces Preliminary Findings of Outage Investigation", 29 lutego 2008 (*http://newsroom.fpl.com/news-releases?item=101775*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Przekaźniki ochronne nie tylko sterują wyłącznikami na liniach przesyłowych. Odłączają też od sieci generatory i inny sprzęt, gdy sytuacja staje się niebezpieczna. Sieć zasilania działa z częstotliwością 60 Hz (czyli 60 cykli na sekundę), a podłączone do niej urządzenia muszą być zsynchronizowane, inaczej mogą zostać uszkodzone. Gdy podłączysz do sieci niezsynchronizowany sprzęt, wygenerowana siła może doprowadzić do jego uszkodzenia. Kiedy generator jest podłączany do sieci, działa na niego siła napięcia z tej sieci — podobnie jak siła grawitacji ciągnie w dół jadący pod górę samochód. Jednak gdy wyłącznik odłącza generator od sieci, wciąż pracujący generator przyspiesza z powodu braku przeciwstawnego obciążenia. Już 10 ms wystarczy, aby utracił synchronizację z siecią. Jeśli wyłącznik znów podłączy generator do sieci w momencie, gdy te komponenty są niezsynchronizowane, efekt będzie podobny do zderzenia się samochodu z ceglaną ścianą. Generator wytwarza zbyt dużo energii, która nie ma ujścia, i po podłączeniu do wolniejszej sieci siła tej energii uderza w nią. Jest to znane zjawisko, które w przeszłości bywało powodem wypadków.

Pytanie, które zespół Assantego postawił na potrzeby testu, było proste: skoro przekaźniki ochronne mają zapobiegać uszkodzeniom sprzętu, co się stanie, jeśli wykorzystać je do zniszczenia urządzenia? Zaprojektowanie takiego ataku okazało się tylko trochę bardziej skomplikowane niż postawienie pytania. Włamanie wymagało napisania szkodliwego kodu zmieniającego ustawienia cyfrowych przekaźników w taki sposób, że wyłączniki generatora w krótkich odstępach czasu były otwierane i zamykane. To sprawiało, że urządzenie było szybko i często odłączane od sieci, a następnie podłączane do niej w niezsynchronizowanym stanie. Bez ochrony ze strony przekaźników nic nie zapobiegało uszkodzeniu generatora. „To właśnie sprawia, że są tak bardzo zdradliwe — powiedział Joe Weiss. — Rzecz, która miała powstrzymywać tego rodzaju sytuacje, posłużyła do przeprowadzenia ataku". W wyniku szybkiego otwierania i zamykania zabezpieczającego obwodu przekaźnik „zamiast zapewniać maksymalną ochronę, wyrządzał maksymalne szkody", jak napisał później Departament Bezpieczeństwa Wewnętrznego w raporcie z testu[59].

[59] Z niedatowanej prezentacji Departamentu Bezpieczeństwa Wewnętrznego uzyskanej przez autorkę na mocy ustawy o wolności informacji. Prezentacja nosi tytuł *Control Systems Vulnerability — Aurora*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Na ofiarę badacze wybrali generator Wärtsilä wycofany z pól naftowych Alaski i zakupiony od pośrednika za jedną trzecią ceny nowego urządzenia wynoszącej milion dolarów[60].

Atak trwał 3 min, choć cel można było osiągnąć w 15 s. Badacze zastosowali w ataku przerwy, aby dać inżynierom czas na ocenę uszkodzeń i sprawdzenie systemów bezpieczeństwa po poszczególnych etapach. Za każdym razem, gdy wyłącznik podłączał zdesynchronizowany generator ponownie do sieci, maszyna podskakiwała i wibrowała od uderzenia własnej energii. Ostatecznie połączenie między silnikiem diesla a generatorem zostało zerwane[61].

Pracownicy w centrum operacyjnym, którzy monitorowali sieć pod kątem anomalii i nie byli uprzedzeni o ataku, nie zauważyli na ekranach nic podejrzanego. System bezpieczeństwa był zaprojektowany w taki sposób, by ignorować niewielkie skoki napięcia, które standardowo występują w sieci, dlatego też nie zarejestrował niszczycielskich przerw w pracy. „Mogliśmy przeprowadzić atak, otwierając i zamykając wyłącznik tak szybko, że systemy bezpieczeństwa tego nie zauważały" — powiedział Perry Pederson, który wówczas kierował prowadzonym przez Departament Bezpieczeństwa Wewnętrznego programem bezpieczeństwa systemów kontroli i nadzorował test[62].

Zastąpienie zniszczonego w ten sposób 27-tonowego generatora było trudne, ale wykonalne. Jednak w dużych elektrowniach i innych zakładach znajdowały się 800-megawatowe generatory, których wymiana mogła zająć

[60] Te dane pochodzą z szacunków kosztów ustalonych na potrzeby testu Aurora i ujawnionych przez Departament Bezpieczeństwa Wewnętrznego na żądanie autorki z tytułu ustawy o wolności informacji.

[61] W 2011 r. wystąpiła sytuacja ilustrująca, co może się stać po uszkodzeniu złącza turbiny. W irańskiej elektrowni w Iranszahrze eksplodował generator z turbiną parową. Jako przyczynę podano uszkodzenie złącza. Eksplozja była tak potężna, że śledczy po wypadku nie potrafili nawet *znaleźć* turbiny. Złącza trzeba regularnie sprawdzać pod kątem oznak zużycia oraz smarować w celu zapewniania sprawności urządzenia i zapobiegania wypadkom. W elektrowni w Iranszahrze w sali, w której znajdował się generator, stały też trzy palniki olejowe, co zapewne miało wpływ na siłę eksplozji. Mogła być ona rzeczywiście skutkiem niewłaściwej konserwacji złącza lub błędów w instalacji, ale niektóre osoby uważały, że mógł to też być wynik sabotażu podobnego do ataku w teście Aurora.

[62] Z wywiadu przeprowadzonego przez autorkę w sierpniu 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

miesiące, a nawet rok, ponieważ generatory tego rodzaju są często budowane na zamówienie w innych państwach. Nie wszystkie zasilające sieć generatory były podatne na tego rodzaju atak. Ważny był sposób równoważenia zasilania w danej części sieci. Jednak podobne problemy mogły dotyczyć krytycznego sprzętu zasilającego komponenty inne niż sieć i niemożliwe do łatwego zastąpienia. Na przykład wyłączenie rozdzielni zasilającej system pomp odpowiedzialnych za dostarczanie wody pitnej do obszarów miejskich spowodowałoby poważne trudności. „Nie wiem, co by się stało z dużą pompą o mocy 50 tys. KM. Wydaje mi się jednak, że problem byłby równie poważny jak w przypadku generatora" — powiedział Pederson[63].

Od czasu przeprowadzenia w 2007 r. testu Aurora zorganizowano też inne pokazy cyberataków powodujących fizyczne szkody. W raporcie z programu *60 Minutes* z 2009 r. badacze z Laboratorium Narodowego Sandia wykazali, że możliwe jest doprowadzenie do przegrzania komponentów w rafinerii ropy w wyniku prostej zmiany ustawień elementu grzejnego i wyłączenia pomp recyrkulacji pomagających w regulowaniu temperatury[64].

JEŚLI POMINĄĆ STUXNETa i incydent w hrabstwie Maroochy, na świecie nie zarejestrowano do tej pory niszczycielskich ataków cyfrowych. Eksperci tłumaczą to na wiele sposobów: takie ataki są znacznie trudniejsze do przeprowadzenia, niż wskazywałyby na to przedstawione tu przykłady, a ludzie posiadający umiejętności i zasoby do przeprowadzenia takich akcji nie mają do tego motywacji (natomiast osoby posiadające taką motywację nie mają odpowiednich środków).

Jedno jest pewne: zróżnicowane i duże możliwości przeprowadzenia takich ataków oraz dowód ich wykonalności w postaci Stuxneta sprawiają, że jest tylko kwestią czasu, kiedy pokusa dokonania cyfrowych ataków stanie się zbyt duża, by się jej oprzeć.

[63] *Ibid.*

[64] *60 Minutes*, „Cyber War: Sabotaging the System". Data pierwszej emisji: 6 listopada 2009 r., CBS.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 10

BROŃ O WYSOKIEJ PRECYZJI

Ralph Langner siedział w swoim biurze w Hamburgu i obserwował, jak dwóch inżynierów przekazuje strumień starannie przygotowanych kłamstw zainstalowanemu na testowej maszynie Stuxnetowi. Langner, ekspert ds. zabezpieczeń systemów kontroli procesów przemysłowych, razem ze współpracownikami od wielu dni starał się zidentyfikować i odtworzyć warunki, w jakich uparty kod Stuxneta uwolni ładunek w sterowniku PLC. Zadanie okazało się jednak trudniejsze, niż badacze oczekiwali.

Wiele dni wcześniej zespół Langnera przygotował komputer z zainstalowanym oprogramowaniem Step 7 Siemensa podłączony do akurat posiadanego sterownika PLC tej samej firmy. Badacze zainstalowali też analizator ruchu w sieci, aby obserwować dane przekazywane między maszyną z systemem Step 7 a sterownikiem PLC. W odróżnieniu od badaczy z Symanteca Langner i jego zespół na co dzień zajmowali się sterownikami PLC i dokładnie wiedzieli, jakiego rodzaju informacje powinny przepływać między maszyną a sterownikiem. Dlatego zakładali, że łatwo wykryją anomalie w komunikacji. Jednak gdy po raz pierwszy zainfekowali system Step 7 Stuxnetem, nic się nie wydarzyło. Odkryli (podobnie jak wcześniej inni badacze), że Stuxnet poluje na dwa *konkretne* modele sterowników PLC Siemensa: S7-315 i S7-417. Zespół nie posiadał żadnego z tych modeli.

Dlatego badacze zainstalowali w systemie Windows testowej maszyny debugger, aby śledzić kroki wykonywane przez Stuxneta przed fizycznym uwolnieniem ładunku. Wymyślili też sposób na przekonanie kodu Stuxneta,

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

że znalazł swój cel. Stuxnet sprawdzał długą listę kontrolną dotyczącą konfiguracji celu. Każdy jej punkt wydawał się bardziej szczegółowy od poprzednich. Langner i współpracownicy nie wiedzieli, co znajduje się na tej liście, ale nie było im to potrzebne. Gdy Stuxnet sprawdzał w systemie każdą pozycję z listy, badacze przekazywali sfabrykowane odpowiedzi aż do momentu ustalenia, jakich danych robak oczekiwał. Była to prosta technika oparta na ataku siłowym, wymagająca kilku dni pracy metodą prób i błędów. Jednak gdy badacze wreszcie uzyskali odpowiednią kombinację odpowiedzi i ostatni raz uruchomili kod, zobaczyli dokładnie to, co opisali pracownicy Symanteca: Stuxnet wstrzyknął serię szkodliwych bloków kodu do sterownika PLC. Langner pamięta, że pomyślał sobie wtedy: „To jest to. Dorwaliśmy tego małego sukinsyna”[1].

Badacze zauważyli szkodliwy kod przesyłany do sterownika PLC tylko dzięki temu, że bloki kodu były nieco większe od oczekiwanych. Przed zainfekowaniem systemu Step 7 Stuxnetem zespół przesłał bloki kodu do sterownika PLC i przechwycił je za pomocą narzędzia analitycznego, aby ustalić standardowy rozmiar i strukturę tych bloków. Po zainfekowaniu maszyny badacze ponownie przesłali te same bloki kodu i zauważyli, że stały się one większe.

Na razie nie potrafili określić, co kod Stuxneta robił ze sterownikami PLC. Jednak samo wstrzykiwanie kodu było ważną informacją. Znacznie wykraczało to ponad cokolwiek, przed czym zespół ostrzegał swoich klientów. Było to też znacznie więcej, niż badacze spodziewali się zobaczyć w pierwszym znanym ataku na sterowniki PLC.

GDY SYMANTEC 17 SIERPNIA ujawnił, że Stuxnet został zaprojektowany w celu sabotażu sterowników PLC, Chienowi i Falliere’owi mogło się wydawać, że nikt nie zwrócił na to uwagi. Jednak prawie 10 tys. km dalej Langner siedział w swoim niewielkim gabinecie na zielonych przedmieściach niemieckiego miasta, z wielkim zaciekawieniem czytając słowa badaczy z Symanteca. Langner od lat ostrzegał klientów z branży przemysłowej, że któregoś dnia ktoś opracuje cyfrowy atak w celu sabotażu systemów kontroli. Wyglądało na to, że ten dzień właśnie nadszedł.

[1] Wszystkie słowa Langnera pochodzą z wywiadów przeprowadzonych z nim w latach 2010, 2011 i 2012.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Langner był właścicielem małej, trzyosobowej firmy specjalizującej się w zabezpieczeniach systemów kontroli procesów przemysłowych. Firma zajmowała się wyłącznie tym. Langner nie interesował się ogólnymi zabezpieczeniami komputerów. W ogóle nie ciekawiły go ostrzeżenia przed najnowszymi wirusami i robakami atakującymi komputery PC. Nawet eksploity typu zero-day nie były dla niego atrakcyjne. Dlatego gdy Stuxnet po raz pierwszy trafił na nagłówki prasy technicznej i stał się tematem wielu rozmów na poświęconych zabezpieczeniom forach, Langner nie zwrócił na niego uwagi. Jednak kiedy Symantec napisał, że Stuxnet służy do sabotażu sterowników PLC Siemensa, badacza natychmiast to zaintrygowało.

Symantec nie ujawnił, co Stuxnet robił ze sterownikiem PLC. Stwierdzono tylko, że robak wstrzykiwał kod do schematu drabinkowego (ang. *ladder logic*) sterownika. Czy oznaczało to wyłączenie sterownika, czy coś jeszcze gorszego, firma antywirusowa nie podała[2]. Langner zrozumiał jednak, że tysiące użytkowników sprzętu Siemensa (w tym wielu klientów firmy samego Langnera) znalazły się w obliczu potencjalnie zabójczego wirusa i niecierpliwie czekają, aż Siemens lub Symantec poinformuje ich, co dokładnie Stuxnet robi ze sterownikami. Dziwne było jednak to, że po wstrząsającym ogłoszeniu badacze z Symanteca ucichli.

Langner podejrzewał, że badacze nie potrafili ruszyć dalej z powodu braku wiedzy o sterownikach PLC i systemach kontroli procesów przemysłowych. Jednak, co ciekawe, Siemens też nie udostępnił żadnych informacji. Langner uznał, że to kuriozalne. W końcu atakowane były sterowniki Siemensa. Firma powinna przeanalizować szkodliwy kod i poinformować klientów, co może stać się z ich systemami. Jednak niemiecka firma w lipcu opublikowała kilka krótkich komunikatów, a następnie zamilkła[3].

---

[2] Schemat drabinkowy to ogólne pojęcie opisujące strukturę poleceń służącą do programowania systemu kontroli. Nazwa pochodzi od przypominającej drabinę struktury kodu, w którym każdy proces jest zapisany w sekwencyjny sposób (krok po kroku).

[3] W pierwszym ogłoszeniu Siemens stwierdził, że zebrał zespół ekspertów w celu przeanalizowania Stuxneta i powiadomi klientów o potencjalnym ryzyku związanym z zagrożeniem. Później firma poinformowała, że zainfekowanych Stuxnetem zostało ok. 20 klientów. Drugie ogłoszenie dotyczyło zapisanego na stałe w oprogramowaniu Siemensa hasła do bazy wykorzystywanego przez Stuxneta do rozprzestrzeniania się. Siemens przestrzegał klientów przed zmianą hasła, ponieważ groziło to zakłóceniem krytycznych funkcji systemów. „Wkrótce opublikujemy wskazówki dla klientów, jednak nie będą one obejmować rady, by zmienić domyślne ustawienia, ponieważ może to wpłynąć na działanie zakładu" — powiedział rzecznik firmy tydzień po ujawnieniu Stuxneta. Zob. Robert McMillan, „After Worm, Siemens Says Don't Change Passwords", *PCWorld.com*, 19 lipca 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Zirytowało to Langnera. Choć wyglądało na to, że Stuxnet atakuje tylko maszyny z systemem Step 7 Siemensa, nikt nie wiedział, co może zrobić lub czy nie występują w nim błędy, które doprowadzą do uszkodzeń innych sterowników PLC. Ważna była jeszcze jedna kwestia — luka umożliwiająca Stuxnetowi wstrzyknięcie szkodliwego kodu do schematu drabinkowego sterowników PLC Siemensa występowała też w innych sterownikach[4]. Kod Stuxneta był dostępny do pobrania w internecie. Każdy haker lub szantażysta lub dowolna grupa terrorystyczna mogli przeanalizować ten kod i wykorzystać go jako wzorzec do zaprojektowania zakrojonego na szerszą skalę i bardziej niszczycielskiego ataku na inne modele sterowników PLC.

To sprawiało, że jeszcze bardziej zagadkowa była cisza ze strony dwóch innych jednostek. Były to: CERT-Bund, niemiecki krajowy zespół reagowania kryzysowego w branży informatycznej, i ICS-CERT ze Stanów Zjednoczonych. Obie organizacje miały pomagać w zabezpieczaniu systemów infrastruktury krytycznej w swoich państwach, jednak żadna z nich nie pisała dużo o Stuxnecie. W ostrzeżeniu od ICS-CERT nie było informacji o wstrzykiwaniu schematu drabinkowego do sterowników PLC Siemensa ani nawet wzmianki o sabotażu. Nie było też nic na temat zagrożeń przyszłymi atakami wzorowanymi na Stuxnecie[5]. Cisza ze strony władz niemieckich była jeszcze dziwniejsza, ponieważ sterowniki Siemensa były zainstalowane w prawie wszystkich znanych Langnerowi zakładach i fabrykach w tym kraju.

Langner porozmawiał na ten temat ze swoimi dwoma doświadczonymi inżynierami: Ralfem Rosenem i Andreasem Timmem. Żaden z nich nie miał doświadczenia w inżynierii odwrotnej wirusów lub robaków, skoro jednak nikt nie zamierzał powiedzieć, co Stuxnet robi ze sterownikami PLC Siemensa, zespół musiał przeanalizować kod samodzielnie. Oznaczało to wiele dni pracy na rzecz dobra publicznego wciśniętych między zlecenia od płacących klientów. Zespół stwierdził jednak, że nie ma innego wyboru.

---

[4] Ta luka po części wynika z tego, że system Siemensa nie używa uwierzytelniania. Umożliwia to przesłanie szkodliwego schematu drabinkowego do sterownika PLC. Gdyby system wymagał przesyłania podpisanego cyfrowo kodu, sterownik PLC nie zaakceptowałby przesyłanych instrukcji.

[5] Zob. ICS-CERT Advisory ICSA-10-201-01C, „USB Malware Targeting Siemens Control Software", 2 sierpnia 2010 i późniejsze aktualizacje (*https://ics-cert.us-cert.gov/advisories/ICSA-10-201-01C*), oraz ICS-CERT Advisory ICSA-10-238-01B, „Stuxnet Malware Mitigation", 15 września 2010 (*https://ics-cert.us-cert.gov/advisories/ICSA-10-238-01B*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Langner i jego współpracownicy tworzyli nietypowy, ale skuteczny zespół. W zawodzie, który czasem kojarzony jest z nieatrakcyjnymi, bladymi inżynierami z kucykiem, Langner był pełen energii, miał krótkie włosy bez śladów siwizny, nosił biznesowe garnitury i eleganckie skórzane buty. Miał 52 lata, przenikliwe niebieskie oczy, przywiezioną z wakacji opaleniznę i wysportowaną sylwetkę doświadczonego alpinisty będącą efektem ubocznym wyjazdów na narty w Alpy i wymagających wędrówek po górach. Gdyby sam elegancki wygląd nie wyróżniał Langnera spośród innych inżynierów, robiłby to jego szorstki i zuchwały sposób bycia. Langner miał reputację bezpośredniego indywidualisty i często wygłaszał prowokacyjne stwierdzenia, które irytowały inne osoby ze społeczności zajmującej się systemami kontroli. Przez lata zwracał uwagę na problemy z bezpieczeństwem takich systemów, jednak jego bezczelne i konfrontacyjne wypowiedzi często odstręczały osoby, dla których te informacje były najważniejsze. Z kolei Rosen i Timm byli inżynierami po czterdziestce z siwymi bródkami oraz bardziej swobodnym nastawieniem do ubioru i sprawności fizycznej. Przyjmowali mniej eksponowane, drugoplanowe role w porównaniu z wyrazistym Langnerem.

Choć ta trójka wydawała się pod wieloma względami niedopasowana do siebie, prawdopodobnie żaden inny zespół nie nadawał się tak dobrze do zbadania Stuxneta. Timm od co najmniej dziesięciu lat pracował dla Langnera jako ekspert od systemów kontroli, Rosen zajmował się tym trzy lata dłużej. Przez ten czas zebrali bogatą wiedzę na temat systemów kontroli procesów przemysłowych, a zwłaszcza sterowników Siemensa. Ta korporacja była zresztą ich długoletnim klientem. Siemens kupował oprogramowanie od firmy Langnera, a on sam i jego inżynierowie czasem szkolili pracowników Siemensa z zakresu systemów tej korporacji. Zapewne niewielu pracowników Siemensa znało systemy tej korporacji lepiej niż zespół Langnera.

Droga Langnera do branży zabezpieczeń systemów kontroli procesów przemysłowych była zawiła. Z zawodu był certyfikowanym psychologiem, co wydawało się bardzo odległe od świata systemów kontroli. Jednak to dzięki doświadczeniu psychologicznemu Langner trafił do obecnej branży. W latach 70., gdy studiował psychologię i sztuczną inteligencję na Wolnym Uniwersytecie Berlina, zaczął pisać oprogramowanie do wykonywania analiz statystycznych danych zebranych w trakcie eksperymentów. Napisał też program do modelowania wzorców podejmowania decyzji w zakresie diagnoz psychiatrycznych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak to sterownik, który stworzył w celu połączenia swojego prywatnego komputera z uniwersyteckim systemem mainframe, doprowadził do rozpoczęcia kariery w branży systemów kontroli procesów przemysłowych. W czasie studiów Langner posiadał komputer PC jednej z pierwszych generacji. Maszyna ta nie miała wystarczającej mocy obliczeniowej do przeprowadzania analiz statystycznych. Gdy Langner chciał przetwarzać dane zebrane w trakcie eksperymentów, musiał za każdym razem wybrać się na kampus i podłączyć komputer do uniwersyteckich systemów mainframe. Nie znosił dojazdów na kampus, dlatego zaczął studiować protokoły potrzebne do zdalnego komunikowania się z serwerami i napisał sterownik, który umożliwiał mu łączenie się z nimi z domu za pomocą modemu.

Nie było więc dla niego dużym wysiłkiem otwarcie po studiach firmy konsultingowej z branży oprogramowania. Jako podstawę biznesu Langner wykorzystał swój sterownik. Wówczas był to produkt przełomowy. Inżynierowie systemów kontroli szybko zaczęli korzystać z niego do komunikowania się z czujnikami i sterownikami używanymi w terenie. Stosowane wtedy techniki często skutkowały utratą danych w trakcie ich przesyłu, a sterownik Langnera okazał się niezawodny.

W 1997 r. do firmy dołączył Rosen. Miał projektować niestandardowe systemy dla klientów, którzy chcieli łączyć komputery PC ze sterownikami PLC Siemensa. Gdy Rosen i Langner przyjrzeli się protokołom i sterownikom PLC Siemensa, aby opracować potrzebne połączenia, byli zaskoczeni liczbą kłopotów z zabezpieczeniami systemów. Były to te same luki, jakie inni badacze odkryli ponad dziesięć lat później. Zaskoczeniem było również to, że właściciele i operatorzy systemów kontroli procesów przemysłowych nie mieli pojęcia o lukach w zabezpieczeniach, dlatego nie robili nic, by chronić swoje systemy przed atakami. Zamiast stosować warstwowe lub wydzielone sieci, w których krytyczne systemy byłyby oddzielone od standardowych komputerów biznesowych, firmy posługiwały się sieciami o płaskiej architekturze bezpośrednio podłączonymi do internetu. Nie stosowano zapór ani haseł do ochrony przed intruzami. Ponadto używane były domyślne i zapisane na stałe hasła, które nigdy się nie zmieniały.

Langner i jego zespół otworzyli wtedy firmę konsultingową, aby pomagać klientom w przebudowywaniu sieci na bardziej bezpieczną postać. Jednak marketing zabezpieczeń systemów kontroli okazał się trudny.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Społeczność korzystająca z systemów kontroli procesów przemysłowych przez lata była w dużym stopniu odporna na złośliwe oprogramowanie i ataki hakerów dotykające użytkowników zwykłych komputerów. Dlatego wiele osób z tej społeczności nie sądziło, że coś im grozi. Langner przestrzegał klientów, że kiedyś poniosą konsekwencje zaniedbań. Często pokazywał, w jaki sposób napastnik o nawet niewielkich umiejętnościach mógłby zablokować pracę firmy. Niestety, mało kto decydował się zrobić coś z tym problemem. „Nikt nie chciał słuchać — mówił Langner — oprócz bardzo nielicznych firm, które zainwestowały w zabezpieczenia systemów kontroli".

Obecnie, dziesięć lat później, Stuxnet był zwiastunem tego, przed czym ostrzegał Langner. Jednak nawet on sam był zaskoczony siłą i intensywnością ataku. Przez lata wyobrażał sobie różne scenariusze ataku hakerów na sterowniki PLC po publicznym ujawnieniu luk w zabezpieczeniach, lecz żaden z tych scenariuszy nie obejmował wstrzykiwania schematu drabinkowego do sterowników PLC. Ataki na komputery zwykle ewoluują w czasie i są stopniowo dopracowywane. Hakerzy początkowo przeprowadzali proste ataki wymagające minimalnych wysiłków i umiejętności. Firmy z branży zabezpieczeń i producenci oprogramowania zareagowali wprowadzeniem poprawek, które powstrzymały takie ataki. Następnie napastnicy odkryli inne ścieżki dostępu do systemów, po czym obrońcy załatali także te luki. Każda kolejna seria ataków była coraz bardziej zaawansowana, podobnie jak sposoby obrony przed nimi. W świecie systemów kontroli Langner oczekiwał, że hakerzy rozpoczną od nieskomplikowanych ataków typu DoS (zatrzymywanie przez sterowniki PLC kontrolowanych przez nie procesów), a następnie przejdą do bomb logicznych i innych prostych technik zmieniania ustawień. Jednak twórcy Stuxneta pominęli początkowe etapy tej ewolucji i przeszli bezpośrednio do jednego z najbardziej zaawansowanych ataków na sterowniki PLC, jakie ktokolwiek mógł wymyślić.

Z wszystkiego, co Langner zobaczył w kodzie Stuxneta, największe wrażenie zrobił na nim atak typu *man in the middle* (dosłownie „człowiek pomiędzy") na system zabezpieczeń i operatorów stacji monitorujących. Sposób, w jaki Stuxnet łatwo obezwładniał system zabezpieczeń i sprytnie rejestrował normalne działanie sterownika PLC, aby odtworzyć je operatorom w trakcie ataku, był dla badacza zdumiewający. Był to cyfrowy odpowiednik

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

sześciotonowego słonia cyrkowego balansującego na jednej nodze. Langner nigdy dotąd nie zetknął się z tego rodzaju gracją i finezją, nawet nie podejrzewał, że napastnicy mogą osiągnąć taki poziom.

Był to też najbardziej agresywny scenariusz, jaki badacz potrafił sobie wyobrazić. Po wyłączeniu przez napastnika logiki odpowiedzialnej za przekazywanie ważnych danych do systemu bezpieczeństwa poważne zranienie lub śmierć któregoś z pracowników były tylko kwestią czasu. Wyłączenie systemu bezpieczeństwa i czujników w zakładzie chemicznym lub rafinerii ropy naftowej mogły prowadzić do uwolnienia trującego gazu lub materiałów łatwopalnych, o czym pracownicy mogli dowiedzieć się dopiero, gdy było już za późno. Możliwe, że twórcy Stuxneta nie zamierzali nikogo zranić ani zabić, jednak naśladujący ich hakerzy stosujący techniki wykorzystane w Stuxnecie mogli okazać się mniej ostrożni.

Langner oszacował, że na świecie jest może kilkadziesiąt osób znających systemy kontroli Siemensa na tyle dobrze, by zaprojektować taki atak. Trzy z tych osób siedziały w jego biurze. Jednak nawet oni nie potrafiliby przeprowadzić ataku w tak wyrafinowany sposób, jak zrobili to napastnicy.

TRZY TYGODNIE OD ROZPOCZĘCIA badań nad Stuxnetem Langner wszedł do sali konferencyjnej, w której on i jego współpracownicy zbierali się każdego ranka, by omówić postępy w pracy nad kodem. Rosen i Timm spojrzeli na niego z zaskoczeniem. Zwykle szef był elegancko ubrany i ożywiony. Tym razem wyglądał nieporządnie i był wyraźnie zmęczony po bezsennej nocy spędzonej nad komputerem w poszukiwaniu informacji w internecie. Śledził jeden trop za drugim, zaglądając do króliczej nory i starając się ustalić, co atakował Stuxnet. Wreszcie udało mu się chwycić uciekającego królika za ogon i przytrzymać. Gdy wyciągnął rękę, był zaskoczony tym, co odkrył. „Wiem, o co w tym chodzi — zdradził współpracownikom. — Celem jest zniszczenie irańskiego programu nuklearnego. Chodzi o wyłączenie zakładu w Buszehrze".

W Buszehrze w południowym Iranie miała powstać elektrownia atomowa. Prace nad nią trwały z przerwami już od wielu lat. W tym czasie roboty były wielokrotnie opóźniane i anulowane, ale tamtego miesiąca elektrownia wreszcie miała zacząć działać. Jednak na krótko przed uruchomieniem elektrowni urzędnicy poinformowali o następnym opóźnieniu. Ponieważ

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

zbiegło się to w czasie z wykryciem Stuxneta, dla Langnera było logiczne, że powodem mógł być cyberatak[6].

Rosen i Timm spoglądali na niego z niedowierzaniem. Rosen pomyślał, że nikt nie jest na tyle głupi, by atakować elektrownię atomową. Czy nie grozi to uwolnieniem materiałów radioaktywnych? Ponadto po co stosować zawodnego robaka, skoro to samo zadanie można skuteczniej wykonać za pomocą bomby? Ale gdy Langner połączył wszystkie punkty, jego szalona teoria zaczęła nabierać sensu.

Przez prawie miesiąc od momentu pierwszego zaobserwowania złośliwego kodu, jaki Stuxnet wstrzyknął do sterownika PLC, Langner wraz z zespołem badali bloki kodu robaka pod kątem potencjalnych celów ataku. Konfiguracja systemów atakowanych przez Stuxneta mogła pomóc ustalić przeznaczenie robaka w równym (a nawet większym) stopniu jak sam kod. Gdyby badacze określili, jakiego rodzaju urządzenia są kontrolowane przez atakowane sterowniki PLC, a także dowiedzieli się, czy te urządzenia są skonfigurowane w nietypowy sposób, mogliby zawęzić listę potencjalnych celów.

Badacze przez kilka tygodni trudzili się nad odszyfrowywaniem bloków kodu w małym biurze na ostatniej kondygnacji dwupiętrowego budynku. Przy cichej ulicy, gdzie pracowali, rosło wiele drzew. Biuro firmy znacznie różniło się od nowoczesnego szklanego kompleksu Symanteca. Zamiast wielu pięter zapełnionych boksami tu znajdowały się: jedno pomieszczenie, w którym siedzieli Timm i Rosen, sala spotkań z klientami i biuro Langnera oraz jego asystenta.

Każdego ranka badacze zbierali się, aby wspólnie przedyskutować poczynione postępy. Następnie przez resztę dnia pracowali nad kodem, omawiając teorie w trakcie lunchu w sali konferencyjnej lub przy obiedzie w pobliskiej restauracji. Równocześnie odpowiadali na telefony od klientów potrzebujących pomocy technicznej. Jednak gdy dzwonili klienci z nowymi zleceniami, Langner odmawiał, ponieważ zależało mu przede wszystkim na rozgryzieniu Stuxneta. Nie wynikało to z tego, że mógł sobie pozwolić na odrzucanie płatnych zleceń. Jego firma nie miała tak dużych zasobów jak korporacja pokroju Symanteca, a żaden zewnętrzny klient nie finansował prowadzonych badań. Langner musiał opłacać czas i pracę swoich inżynierów z zysków firmy. Nikt jednak nie narzekał. Cały zespół

[6] Kilka tygodni później irańscy urzędnicy zaprzeczyli, że Stuxnet był powodem opóźnienia. Jako przyczynę podali wyciek ze zbiornika w pobliżu reaktora.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wiedział, że Stuxnet to wyzwanie, jakie zdarza się raz w życiu. „Rozumieliśmy, że to największa sprawa w historii złośliwego oprogramowania — wspominał Langner. — To była absolutnie fantastyczna praca, najlepsza, jaką kiedykolwiek wykonywałem. Jestem przekonany, że nic lepszego mnie nie czeka".

Po tygodniach męczących analiz zespół doszedł do zaskakującego wniosku. Stuxnet atakował nie tylko dwa konkretne modele sterowników PLC Siemensa, ale konkretny zakład, w którym były one używane. Był bronią o wojskowej precyzji nakierowaną na jeden cel. Nie szukał dowolnych sterowników PLC S7-315 i S7-417. Docelowe urządzenia musiały być dodatkowo skonfigurowane w bardzo specyficzny sposób. W kodzie znajdowały się szczegółowe informacje opisujące konfigurację techniczną szukanych sterowników PLC. W każdym zakładzie, gdzie używane były systemy kontroli procesów przemysłowych, stosowano niestandardową konfigurację. Nawet firmy z tej samej branży konfigurowały urządzenia pod kątem własnych potrzeb. Konfiguracja szukana przez Stuxneta była tak ściśle sprecyzowana, że występowała zapewne w tylko jednym obiekcie w Iranie lub, jeśli było ich więcej, w zakładach skonfigurowanych w identyczny sposób na potrzeby kontroli tego samego procesu. Każdy system, który nie był skonfigurowany w ten sposób, pozostawał nienaruszony. Stuxnet po napotkaniu takich systemów kończył pracę i przechodził do następnej maszyny w poszukiwaniu swoich celów.

Langner był zdumiony, że ktoś włożył tyle pieniędzy i pracy w przygotowanie broni atakującej jeden cel. Mogło to oznaczać tylko jedno — ów cel musiał być niezwykle ważny. Teraz musieli tylko ustalić, co to za cel.

Większość kroków w procesie analizy kodu jest usystematyzowana i wysoce techniczna. Należy odizolować komponenty, odszyfrować kod i zastosować inżynierię odwrotną. Jednak łączenie cyfrowego kodu z rzeczywistym światem jest w większym stopniu sztuką niż nauką. Trzech badaczy rozważało mnóstwo hipotez na temat tego, co może być celem, a następnie analizowało kod pod kątem dowodów. Langner skontaktował się też ze znajomymi z różnych branż, aby zapytać o konfigurację ich sterowników PLC. Chciał w ten sposób sprawdzić, czy znajdzie pasującą konfigurację. Niestety, po wielu dniach zespół nadal nie potrafił ustalić celu Stuxneta. Ostatecznie Langner zdecydował, że przestanie koncentrować się na szczegółach technicznych i spojrzy na problem z innej strony. Zaczął przeszukiwać

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

artykuły w serwisach informacyjnych i inne źródła pod kątem wskazówek. Po kilku długich wieczorach spędzonych na surfowaniu po internecie doszedł do teorii związanej z Buszehrem.

Podejrzenia Langnera dotyczące tej elektrowni pojawiły się, gdy badacz przypomniał sobie zdjęcie, na które w poprzednim roku natrafił w internecie. Zdjęcie to miało być zrobione w trakcie przeprowadzonego w Buszehrze pokazu dla prasy. Widoczny był na nim monitor komputera z komunikatem informującym, że licencja na oprogramowanie WinCC Siemensa wygasła. Dla Langnera było to dowodem na używanie w elektrowni oprogramowania Siemensa[7]. Znajomi ze społeczności zajmującej się systemami kontroli potwierdzili, że w Buszehrze zainstalowane były sterowniki S7-417 Siemensa. Z dalszych badań wynikało, że rosyjska firma odpowiedzialna za instalację sprzętu w tej elektrowni stosowała sterowniki PLC Siemensa także w innych obiektach, których wyposażeniem się zajmowała. Była to m.in. elektrownia w Bułgarii, podobno wzorowana na obiekcie z Buszehru. Langner dowiedział się, że w bułgarskiej elektrowni działała turbina parowa kontrolowana przez sterowniki Siemensa. Przypomniało mu to o teście Aurora Generator przeprowadzonym trzy lata wcześniej w Laboratorium Narodowym Idaho. Ten test był dowodem na to, że szkodliwy kod może zniszczyć turbinę.

Badacze siedzieli w sali konferencyjnej. Langner przedstawiał swoje odkrycia, a Rosen i Timm bez przekonania mu potakiwali. Wiedzieli, że na świecie znajduje się bardzo niewiele celów uzasadniających ogrom pracy włożonej w Stuxneta. Jeśli jednak Langner miał rację, a celem był fizyczny atak na elektrownię w Buszehrze, Stuxnet był jak wypowiedzenie wojny.

A skoro Stuxnet był wypowiedzeniem wojny, jakiego rodzaju reakcję Iranu wywoła, gdy informacje na ten temat się rozniosą? Ktokolwiek uruchomił Stuxneta, mógł zrobić to po to, by uniknąć otwartej wojny z Iranem. Jednak ujawnienie całej historii mogło do niej doprowadzić.

---

[7] To zdjęcie, wykonane przez fotografa z agencji UPI, jest opatrzone nagłówkiem informującym, że przedstawia ekran komputera w Buszehrze i zostało zrobione w lutym 2009 r. Niektórzy krytycy podają w wątpliwość prawdziwość nagłówka i twierdzą, że zdjęcie przedstawia zakład uzdatniania wody, a nie elektrownię w Buszehrze. Jednak zakłady uzdatniania wody często są potrzebne do działania elektrowni atomowych, dlatego obie opcje mogą być prawdziwe. Wspomniane zdjęcie znajdziesz na stronie: *http://www.upi.com/News_Photos/Features/The-Nuclear-Issue-in-Iran/1581/2/*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Po rozmowie z Rosenem i Timmem Langner był przekonany, że znalazł się na właściwym tropie. Jednak aby się upewnić, że to irański program nuklearny był celem, zadzwonił do klienta z bogatą wiedzą na temat elektrowni atomowych. Ten klient pracował dla Enrichment Technology Company, czołowego europejskiego producenta sprzętu do wzbogacania uranu. Wcześniejszą nazwą tego producenta była Urenco. To ta firma wytwarzała wirówki starszych generacji, których plany A.Q. Khan wykradł, a następnie sprzedał Iranowi. Langner podejrzewał, że jeśli Stuxnet nie miał atakować turbin, celem mogły być wirówki służące do wzbogacania uranu dla elektrowni w Buszehrze. Błędnie sądził, że te wirówki też znajdowały się w Buszehrze.

„Mam do ciebie jedno pytanie — powiedział Langner do znajomego przez telefon. — Czy można uszkodzić wirówkę poprzez samą zmianę kodu sterownika?".

Zanim padła odpowiedź, nastąpiła dłuższa przerwa.

„Nie mogę ci tego powiedzieć, Ralph. To poufne informacje — odpowiedział znajomy. Jednak potem dodał: — Wiesz, wirówki do wzbogacania uranu są używane nie tylko w Niemczech i Holandii. Stosuje się je także w innych państwach".

„Tak, wiem — rzekł Langner. — Na przykład w Iranie. Właśnie dlatego dzwonię. Analizujemy Stuxneta".

„Przykro mi — odrzekł stanowczo mężczyzna. — Nie mogę ci powiedzieć niczego na temat wirówek. To poufne".

Langnerowi to wystarczyło. Oświadczył Rosenowi i Timmowi, że muszą natychmiast upublicznić wiadomości. Jeśli to Buszehr był celem, ktoś powinien móc potwierdzić ich podejrzenia. Stuxnet i jego cel były jak klucz i zamek. Na świecie istniał tylko jeden zamek, który można było otworzyć danym kluczem. Po upublicznieniu informacji o projekcie klucza właściciel zamka powinien umieć stwierdzić, czy jego obiekt pasuje do opisu.

Trzynastego września 2010 r., prawie miesiąc po ujawnieniu przez Symantec, że Stuxnet miał dokonać sabotażu sterowników PLC, Langner opublikował na blogu krótki wpis zatytułowany „Hack of the Century" (czyli „włamanie stulecia"). W tym tekście stwierdził, że Stuxnet był bezpośrednim atakiem wymierzonym „w konkretną instalację systemu kontroli". Na tym etapie nie podał dalszych szczegółów. Ujawnił je dopiero po trzech dniach. „Na podstawie ekspertyz ewidentne i możliwe do udowodnienia

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

jest to, że Stuxnet to ukierunkowany sabotaż z wykorzystaniem zaawansowanej wiedzy osoby z wewnątrz — napisał. — Oto informacje, które wszyscy powinni poznać”[8].

Następnie Langner podał techniczny opis kroków wykonywanych przez Stuxneta w celu przejęcia kontroli nad maszyną i wstrzyknięcia instrukcji do sterownika PLC Siemensa dla dokonania sabotażu. „To nie jest praca hakera mieszkającego w piwnicy domu rodziców” — napisał. W akcji brały udział zaawansowane jednostki państwowe z bardzo dobrą znajomością atakowanego systemu. Badacz na ogólnym poziomie opisał, w jaki sposób złośliwe oprogramowanie wstrzykiwało szkodliwy kod do sterownika PLC w celu przejęcia nieustalonych krytycznych procesów. Następnie podzielił się swoimi przemyśleniami na temat Buszehru, ostrożnie opisując je jako spekulacje. Nadal wiele rzeczy pozostawało niewiadomych, jednak dowody w kodzie mogły ostatecznie doprowadzić nie tylko do systemu będącego celem Stuxneta, ale może nawet do samych napastników.

Ten krótki tekst oznaczał koniec akcji dla twórców Stuxneta. Cyberbroń, której zaplanowanie i opracowanie wymagało lat starań i zapewne milionów dolarów, została ujawniona i powstrzymana w ciągu kilku tygodni przez nieznaną firmę antywirusową z Białorusi, kilku badaczy z Kalifornii, którzy nic nie wiedzieli o wirówkach i sterownikach PLC, oraz bezpośredniego Niemca i jego zespół inżynierów.

Lecz teraz, po ujawnieniu sekretu Stuxneta, Langner zaczął mieć te same co Chien obawy dotyczące możliwej reakcji napastników. Po ujawnieniu celu ataku Stuxnet stał się prawie bezużyteczny. Napastnicy musieli przewidzieć, że ich kod ostatecznie zostanie wykryty i że będą mieli wtedy krótki czas na dokończenie misji. Czy w ostatniej próbie zrealizowania celu wykonają końcowy drastyczny krok? Langner uważał, że to możliwe. „Możemy się spodziewać, że wkrótce coś wybuchnie — przewidywał we wpisie. — Będzie to coś dużego”. Tekst zakończył nietypowym ostrzeżeniem: „Witajcie na cyberwojnie”.

Obok wpisu pojawiło się zdjęcie trzech „pogromców Stuxneta” wykonane przy tablicy w biurze. Langner był ubrany w elegancką białą koszulę i rozpiętą kamizelkę od garnituru, Rosen i Timm stali za nim. Ten ostatni, w uhonorowaniu tajnego charakteru Stuxneta, nosił okulary przeciwsłoneczne.

---

[8] „Stuxnet logbook, Sept 16, 2010, 1200 hours MESZ” (*https://www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Po zamieszczeniu wpisu Langner wysłał wiadomość prasową do kilku popularnych serwisów i oczekiwał, że informacja znajdzie się na nagłówkach. Ku jego konsternacji, nic takiego się nie stało. Podobnie jak wcześniejsze informacje od Symanteca, tak i najnowsze rewelacje spotkały się z całkowitym brakiem zainteresowania. Langner pamięta, że pomyślał sobie: „Pewnie wszyscy sądzą, że zwariowałem".

Przynajmniej jedna osoba uważała inaczej. Frank Rieger, dyrektor techniczny GSMK, niemieckiej firmy z branży zabezpieczeń, przeczytał spekulacje Langnera o Buszehrze i zgodził się, że Stuxnet został zapewne zbudowany w celu sabotażu irańskiego programu nuklearnego. Podejrzewał jednak, że bardziej prawdopodobnym celem był leżący kilkaset kilometrów na północ od Buszehru Natanz[9]. Zakład w Natanzie, w odróżnieniu od elektrowni w Buszehrze, już działał, i to od 2007 r. Ponadto, także inaczej niż obiekt w Buszehrze, był zapełniony tysiącami szybko obracających się wirówek, dlatego stanowił cenny cel dla każdego, kto chciał poprzez atak cyfrowy zaszkodzić irańskiemu programowi nuklearnemu. Rieger przedstawił swoje przemyślenia we wpisie na blogu oraz w artykule dla jednej z niemieckich gazet[10]. W obu przypadkach nawiązał do wcześniejszych tekstów Agencji Reutera opublikowanych w 2009 r. mniej więcej w czasie wypuszczenia Stuxneta. W artykule agencji opisywany był „dziesięcioletni projekt cyberbroni" uruchomiony przez Izrael przeciwko irańskiemu programowi nuklearnemu. Autor tekstu przytaczał słowa amerykańskiego źródła spekulującego, że można wykorzystać „szkodliwe oprogramowanie" do przejęcia sterowania lub spowodowania awarii w zakładzie wzbogacania uranu[11].

---

[9] Ten artykuł pojawił się w niemieckiej gazecie „Frankfurter Allgemeine Zeitung" 22 września 2010 r. Jest napisany po niemiecku, jednak autor opisuje jego treść po angielsku we wpisie na blogu: *http://frank.geekheim.de/?p=1189*.

[10] Gdy Langner spekulował na temat Buszehru, nie wiedział, że w tej elektrowni atomowej nie ma wirówek. Kiedy stało się to jasne, badacz nadal sądził, że celem był Buszehr, jednak podejrzewał, że Stuxnet ma atakować turbinę lub generator. Dopiero później, gdy pojawiło się więcej informacji na temat konkretnych urządzeń szukanych przez Stuxneta, Langner doszedł do wniosku, że Natanz lepiej niż Buszehr pasuje na cel Stuxneta.

[11] Dan Williams, „Wary of Naked Force, Israelis Eye Cyberwar on Iran", 7 lipca 2009 (*http://www.reuters.com/article/us-israel-iran-cyberwar-analysis-idUSTRE5663EC20090707*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Był też inny powód do tego, by podejrzewać, że to Natanz był celem Stuxneta. Szesnastego lipca 2009 r., trzy tygodnie po wypuszczeniu wersji Stuxneta z 2009 r., Julian Assange, założyciel serwisu WikiLeaks, opublikował w swojej witrynie tajemniczy komentarz na temat możliwych wypadków w Natanzie. Anonimowy informator twierdzący, że bierze udział w irańskim programie nuklearnym, poinformował Assange'a, że w zakładzie w Natanzie niedawno zdarzył się „poważny" incydent[12]. W serwisie WikiLeaks zwykle publikowane są tylko dokumenty, a nie plotki z anonimowych źródeł, jednak Assange złamał zasady, ponieważ — jak powiedział — miał powody, by wierzyć, że informator jest wiarygodny. Nawiązał też do opublikowanego tego dnia przez BBC artykułu opisującego rezygnację Gholama Rezy Aghazadeha, szefa irańskiej Agencji Energii Atomowej, który 20 dni wcześniej z nieznanych przyczyn odszedł ze stanowiska[13]. Zbiegło się to w czasie z pojawieniem się wersji Stuxneta z 2009 r.

Niezależnie od tego, czy rezygnacja Aghazadeha była związana z wypadkiem w Natanzie, „teoria Natanzu" Riegera zainteresowała media i wreszcie Stuxnet znalazł się w centrum uwagi. Główne media amerykańskie, do tej pory w większości ignorujące atak, podchwyciły spekulacje i zaczęły same opisywać całą historię. Przez prawie dziesięć lat Natanz był źródłem rosnącego napięcia politycznego związanego z wielokrotnymi próbami powstrzymania planowanego tam programu wzbogacania uranu. Teraz

[12] Te informacje z serwisu WikiLeaks znajdziesz na stronie: *https://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation*.

[13] Informacje zostały opublikowane na stronie: *http://news.bbc.co.uk/2/hi/middle_east/8153775.stm*. Choć możliwe było, że rezygnacja Aghazadeha wynikała z czegoś, co wydarzyło się w Natanzie pod koniec czerwca 2009 r., równie dobrze przyczyną mogły być kwestie polityczne. Aghazadeh był nie tylko szefem irańskiej Agencji Energii Atomowej, ale też wiceprezydentem Iranu. Z obu tych stanowisk zrezygnował jednocześnie po dwóch tygodniach od mocno kwestionowanych wyborów prezydenckich z 12 czerwca 2009 r. Aghazadeh wszedł w sojusz z politycznym przeciwnikiem Ahmadineżada (był to Mir-Hosejn Musawi). Pojawiły się spekulacje, że gwałtowne protesty w sprawie legalności wyników wyborów uniemożliwiły Aghazadehowi zachowanie rządowych stanowisk po usankcjonowaniu zwycięstwa Ahmadineżada. Problematyczny był też czas rezygnacji, niepokrywający się z działaniem wersji Stuxneta z czerwca 2009 r. Według raportu BBC Aghazadeh zrezygnował w okolicach 26 czerwca. Natomiast wspomniana wersja Stuxneta została wypuszczona 22 czerwca, a po znalezieniu się w odpowiednim sterowniku PLC potrzebowała jeszcze 13 dni, aby rozpocząć sabotaż. Jeśli więc to nie jakieś wcześniejsze wersje Stuxneta lub inne czynniki spowodowały problemy w Natanzie, czas ataku nie był zgodny z czasem rezygnacji Aghazadeha.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wyglądało na to, że związana z tym jest także zaawansowana broń cyfrowa, jakiej nigdy wcześniej nie widziano. Nagle historia Stuxneta okazała się bardzo atrakcyjna i pełna intryg. Zamiast suchych, technicznych opisów interesujących tylko prasę z branży technologicznej powstała opowieść z aurą tajemnicy i tajnymi rozgrywkami szpiegowskimi toczącymi się w tle poważnego nuklearnego starcia.

Langner krótko po tym, jak opublikował pierwszy wpis na temat Stuxneta, skontaktował się z Joem Weissem ze Stanów Zjednoczonych, aby omówić z nim poczynione odkrycia. Obaj mieli taki sam konfrontacyjny sposób bycia, który nie zawsze przysparzał im przyjaciół w społeczności zajmującej się systemami kontroli. Obaj przez lata walczyli po tej samej stronie barykady, starając się przekonać właścicieli systemów kontroli procesów przemysłowych, że ich systemy są podatne na atak. Członkowie społeczności często wzdychali, słysząc nazwisko któregoś z tych dwóch badaczy, jednak nikt nie wątpił w ich zaangażowanie. Langner miał niedługo wystąpić na poświęconej systemom kontroli konferencji organizowanej przez Weissa w stanie Maryland. Planował wygłosić tam wykład na inny temat, ale zapytał, czy zamiast tego nie może opowiedzieć o Stuxnecie. „Nie wiem, czy mam powiedzieć »tak«, czy »tak, do cholery«" — odpowiedział Weiss.

Tydzień później Langner leciał na konferencję. Szum wokół jego wystąpienia gwarantował, że sala konferencyjna będzie pełna. Langner na blogu zapowiadał, że w czasie prelekcji ujawni wszystkie szczegóły z badań swojego zespołu. Dlatego uczestnicy byli przygotowani i z niecierpliwością oczekiwali na to, co Niemiec ma do powiedzenia — zwłaszcza po tym, jak dwie prezentacje na temat Stuxneta, przeprowadzone przez Siemensa i jakiegoś człowieka z Departamentu Bezpieczeństwa Krajowego, okazały się pozbawione jakichkolwiek szczegółów.

Weiss przeznaczył na wystąpienie Langnera 45 min, a przeciągnęło się ono do 1,5 godz. Nikt jednak nie narzekał. Ponad 100 uczestników z branż gospodarki wodnej, chemicznej i energetyki z uwagą wsłuchiwało się w słowa zagranicznego gościa. „Wszyscy siedzieliśmy z otwartymi ustami, gdy przemawiał" — wspomina Weiss[14]. Ludzie tacy jak Langner zdarzali się w branży technicznej rzadko. Niemiec był uzdolnionym i charyzmatycznym mówcą, potrafiącym przedstawiać suche techniczne szczegóły z humorem i lekkością. Ale to, o czym mówił owego dnia, było czymś innym niż rozrywką.

[14] Z wywiadu przeprowadzonego przez autorkę we wrześniu 2010 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wszyscy w sali byli zszokowani. Do właścicieli systemów kontroli powoli zaczęło docierać, że jeśli następnego dnia na sterowniki PLC przeprowadzony zostanie inny, szerzej zakrojony atak, społeczność nie będzie potrafiła go powstrzymać ani nawet wykryć. Istniały sposoby na ustalenie, czy komputer PC lub laptop z systemem Windows zostały zaatakowane, jednak z powodu technik ukrywania ataku zastosowanych w Stuxnecie nie dało się stwierdzić, czy sterownik PLC został zainfekowany. Nie było oprogramowania antywirusowego dla sterowników PLC. Nie istniał łatwy sposób na stwierdzenie, czy w sterowniku zainstalowany jest szkodliwy kod, jeśli ten kod używał tego samego rodzaju podstępów co Stuxnet. Jedynym sposobem było wykrycie ataku na poziomie systemu Windows, zanim robak dotrze do sterownika PLC. Jednak Stuxnet ominął nawet to zabezpieczenie, ponieważ żaden skaner antywirusowy nie znalazł go przed dotarciem robaka do sterowników PLC. Operatorzy nie mogli więc wykryć głowicy do momentu, w którym było już za późno.

Langner podejrzewał, że pierwsze naśladowcze ataki rozpoczną się po jakichś sześciu miesiącach. Uważał, że nie będą to dokładne repliki Stuxneta oraz że ataki nie będą równie zaawansowane, jednak nie musiały takie być. Nie tylko kluczowe cele takie jak Natanz były narażone na atak. Stuxnet oznaczał zagrożenie dla każdego podatnego na atak obiektu. I choć twórcy robaka umiejętnie zaplanowali akcję w taki sposób, aby uniknąć przypadkowego uszkodzenia maszyn niebędących celem, kolejne ataki mogły nie być równie starannie dopracowane lub kontrolowane. Grupa przestępcza chcąca przejąć kontrolę nad sterownikami PLC elektrowni w celu szantażowania jej właścicieli nie będzie się przejmować, czy szkodliwy kod uszkodzi zakład lub rozprzestrzeni się także na inne systemy kontroli.

Po konferencji Langner spędził weekend w Waszyngtonie, aby spotkać się z Melissą Hathaway, byłą koordynatorką ds. cyberbezpieczeństwa narodowego przy Białym Domu, i przedstawić jej odkrycia zespołu. Hathaway natychmiast zrozumiała możliwość pojawienia się ataków na infrastrukturę krytyczną Stanów Zjednoczonych oraz problem rozprzestrzeniania się broni cyfrowej, z jakim świat będzie musiał się teraz zmierzyć. Później powiedziała gazecie „New York Times", że żaden kraj nie jest przygotowany, by poradzić sobie z tym problemem. „Mamy około dziewięćdziesięciu dni na poprawę sytuacji — powiedziała gazecie — zanim jakiś haker [naśladowca] zacznie używać takiej broni"[15].

[15] John Markoff, *A Silent Attack, but Not a Subtle One*, „New York Times", 26 września 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W weekend, który Langner spędził w Waszyngtonie, irańscy urzędnicy po raz pierwszy ujawnili, że komputery w Buszehrze rzeczywiście zostały zainfekowane przez Stuxneta. Nie wspominali jednak o Natanzie, a z podanych szczegółów ataku na Buszehr wynikało, że ładunek Stuxneta prawdopodobnie w ogóle nie został tam zainstalowany. Mahmoud Jafari, menedżer projektu w elektrowni, poinformował dziennikarzy, że dotknięte atakiem zostały tylko komputery PC niektórych pracowników zakładu, a nie systemy produkcyjne. „Wszystkie programy komputerowe w zakładzie działają normalnie i Stuxnet nie spowodował ich awarii" — powiedział[16]. Reza Taghipour, urzędnik z ministerstwa komunikacji i technologii informatycznych, także podkreślał, że szkody spowodowane przez robaka były niewielkie, a on sam został „w mniejszym lub większym stopniu" opanowany[17]. Doniesienia o ograniczonych szkodach nie były zaskoczeniem, jeśli wziąć pod uwagę wybiórczość Stuxneta w uwalnianiu szkodliwego ładunku. Robak zapewne dostał się do maszyn z systemem Windows w Buszehrze, a następnie zakończył pracę, gdy nie znalazł szukanych sterowników PLC[18].

---

[16] Laurent Maillard, „Iran Denies Nuclear Plant Computers Hit by Worm", Agence France-Presse, 26 września 2010 (*http://iranfocus.com/en/index.php?option=com_content&↪view=article&id=21820*).

[17] David E. Sanger, *Iran Fights Malware Attacking Computers*, „New York Times", 25 września 2010.

[18] Po sześciu miesiącach zaprzeczono tym doniesieniom w raporcie irańskiej Passive Defense Organization — kierowanej przez generała gwardii rewolucyjnej Gholama Rezę Jalalego wojskowej organizacji odpowiedzialnej za obronę irańskich obiektów nuklearnych. W raporcie stwierdzono, że Stuxnet tak poważnie zainfekował komputery w Buszehrze, że prace nad elektrownią trzeba było wstrzymać na czas nieokreślony. Według raportu włączenie elektrowni sprawi, że robak „zatrzyma pracę generatorów i sieci energetycznej kraju". Było jednak wiele powodów, dla których należało wątpić w przedstawione w dokumencie wnioski. Zawierał on przesadne stwierdzenia dotyczące możliwości Stuxneta. Napisano np., że robak może „krok po kroku zniszczyć sprzęt w systemie". Ponadto konfiguracja szukana przez Stuxneta nie pasowała do tej z elektrowni atomowej. Wszystko to wskazywało na to, że Iran posłużył się Stuxnetem jako wymówką do wyjaśnienia opóźnień w Buszehrze. Jednak możliwe było też to, że niezależnie przeprowadzony został na Buszehr inny atak cyfrowy, z użyciem zmodyfikowanej wersji Stuxneta. Zob. Ken Timmerman, „Computer Worm Wreaking Havoc on Iran's Nuclear Capabilities", Newsmax, 27 kwietnia 2011 (*http://www.newsmax.com/KenTimmerman/iran-natanz-nuclear-stuxnet/2011/04/27/id/394327/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W komentarzach Irańczyków uwagę zwracał jeden dziwny szczegół. Jafari w jednym z wywiadów stwierdził, że w Iranie znaleziono *pięć* wersji Stuxneta[19]. Symantec i inni badacze wirusów wykryli tylko trzy wersje.

Choć było możliwe, że Jafari się mylił, z jego słów wynikała intrygująca możliwość: zostały wypuszczone przynajmniej dwie inne wersje Stuxneta. A jeśli takie wersje rzeczywiście istniały, mogły zawierać dodatkowe wskazówki dotyczące Stuxneta i jego twórców. Niestety, zachodni badacze mieli niewielkie szanse na zapoznanie się z nimi, ponieważ urzędnicy irańscy zapewne nie chcieliby udostępnić kopii kodu komukolwiek spoza Iranu[20].

Po prezentacji na konferencji Weissa i po spotkaniu z Hathaway Langner potrzebował odpoczynku, aby poukładać sobie w głowie wszystko to, co wydarzyło się we wcześniejszych tygodniach. W weekend wybrał się do National Mall i godzinami siedział na schodach pomnika Lincolna, wpatrując się w lustrzaną taflę wody, gdy wokół niego turyści robili sobie zdjęcia. Zastanawiał się nad raportami ICS-CERT i Siemensa oraz nad milczeniem tych jednostek w sprawie wstrzyknięcia schematu drabinkowego przez Stuxneta i zagrożeń infrastruktury krytycznej wynikających z ataków naśladowców. Niezrozumiały był też brak reakcji opinii publicznej iKongresu, który najwyraźniej nie przejmował się tym, że Stuxnet był drogą do legitymizacji stosowania cyberbroni do rozwiązywania konfliktów politycznych.

---

[19] Maillard, „Iran Denies Nuclear Plant Computers Hit by Worm".

[20] Urzędnicy opublikowali też inne oświadczenia, które — jeśli były prawdziwe — wskazywały na istnienie innych wersji Stuxneta. Mahmoud Liayi, szef rady ds. technologii informatycznych przy ministerstwie przemysłu, powiedział dziennikarzom, że gdy Stuxnet został aktywowany, „przemysłowe systemy automatyki rozpoczęły przesyłanie danych o liniach produkcyjnych" do zewnętrznych jednostek. Generał Gholam Reza Jalali na konferencji prasowej w 2011 r. stwierdził, że odkryto, iż robak komunikował się z systemami w Izraelu i Teksasie. Tam dane o zainfekowanych maszynach miały być przetwarzane przez architektów robaka, którzy następnie zaprojektowali atak na program nuklearny (zob. „Iran Military Official: Israel, US Behind Stuxnet Computer Worm", Associated Press, 16 kwietnia 2011, *http://www.haaretz.com/world-news/iran-military-official-israel-u-s-behind-stuxnet-computer-worm-1.356287*). Jednak trzy odkryte wersje Stuxneta komunikowały się z serwerami C&C z Danii i Malezji. Nie wykluczało to jednak, że inna wersja prowadziła do Teksasu lub że pochodziło stamtąd narzędzie szpiegowskie poprzedzające Stuxneta. Jednak choć Agencja Bezpieczeństwa Narodowego USA posiada elitarny zespół hakerów w Teksasie, jest mało prawdopodobne, że hakerzy popełniliby błąd umożliwiający powiązanie ich z robakiem lub narzędziem szpiegowskim.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Kongres najwyraźniej nie martwił się też zainicjowanym przez Stuxneta cyfrowym wyścigiem zbrojeń, którego okiełznanie mogło okazać się niewykonalne. Langner stwierdził, że wyglądało to tak, jakby nikt nie chciał poruszać tej sprawy z obawy przed pojawieniem się pytań, kto stoi za atakiem.

Badacz zdecydował, że skoro pozostali zamierzają siedzieć cicho, on sam powinien upublicznić więcej informacji na temat kodu. Dlatego po powrocie do Niemiec opublikował na blogu nowy wpis z technicznymi szczegółami, które wcześniej ujawnił tylko za zamkniętymi drzwiami sali konferencyjnej Weissa. Wkrótce po pojawieniu się tych wpisów pojawiło się wielu czytelników z całego świata, w tym, co ciekawe, z rządowych i wojskowych domen amerykańskich. Langner miał nadzieję, że teraz, gdy znaczenie Stuxneta stało się już oczywiste, inne firmy zajmujące się bezpieczeństwem przejmą pałeczkę i będą kontynuować badania. Mimo wszystkiego, czego badacze się dowiedzieli, do wykonania pozostało jeszcze dużo pracy. Zespół odkrył tylko to, że Stuxnet miał sabotować jeden obiekt, którym prawdopodobnie był zakład w Natanzie. Nadal jednak nikt nie wiedział, co robak miał zrobić z zakładem. Ta informacja wciąż pozostawała ukryta w kodzie.

Przez następne trzy tygodnie Langner i jego współpracownicy zajmowali się kilkoma projektami płacących klientów, aby zrekompensować utratę przychodów spowodowaną analizowaniem Stuxneta. Jednak gdy nie pojawiały się nowe informacje o kodzie ze strony Symanteca czy innych jednostek, Langner zdecydował, że zespół powinien wznowić prace nad robakiem.

„Panowie — powiedział do Rosena i Timma. — Uważam, że powinniśmy wrócić do tej sprawy".

WBREW PRZEKONANIU LANGNERA, że rząd Stanów Zjednoczonych zignorował Stuxneta lub że umknęły mu ważne szczegóły ataku, pewne jednostki rządowe *poświęcały* uwagę tej sprawie, choć robiły to w tajemnicy. Grupa analityków z Departamentu Bezpieczeństwa Krajowego ukończyła większość analiz Stuxneta kilka dni od jego ujawnienia w lipcu i wcześniej od Langnera i badaczy z Symanteca wiedziała, że robak miał dokonać sabotażu sterowników PLC.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Stuxnet po raz pierwszy trafił do centrum kontroli Narodowego Centrum ds. Cyberbezpieczeństwa i Komunikacji (ang. *National Cybersecurity and Communications Integration Center* — NCCIC; jest to jednostka Departamentu Bezpieczeństwa Wewnętrznego) w Arlington w stanie Wirginia rankiem 15 lipca 2010 r. — w czasie, gdy badacze zabezpieczeń na całym świecie zaczynali przyglądać się kodowi robaka. Pliki nadeszły od organizacji CERT-Bund po tym, jak Siemens skontaktował się z zespołem reagowania na incydenty informatyczne i zgłosił atak wymierzony w sterowniki PLC tej firmy.

Centrum NCCIC (lub N-Kick, jak często wymawiana jest ta nazwa) istniało dopiero dziewięć miesięcy. Było częścią nowego rządowego planu kontroli misji służącą do monitorowania i koordynowania reakcji na cyberzagrożenia dotyczące infrastruktury krytycznej i cywilnych systemów rządowych. Zabawne było to, że w momencie otrzymania plików Sean McGurk, dyrektor centrum, był w trakcie planowania nadchodzących rządowych ćwiczeń Cyber Storm III. Były to przeprowadzane co dwa lata trzydniowe ćwiczenia symulujące cyfrowe ataki na infrastrukturę krytyczną Stanów Zjednoczonych. Miał to być pierwszy prawdziwy test możliwości koordynacyjnych tego działającego 24 godz. na dobę centrum kontroli. Jednak rzeczywiste zagrożenie ze strony Stuxneta było priorytetowe względem planowania postępowania na potrzeby symulowanego ataku.

Pozbawione okien centrum kontroli było pełne przedstawicieli agencji o trzyliterowych nazwach. Analitycy wywiadu z CIA i NSA siedzieli obok agentów organów ścigania z FBI i Secret Service oraz ekspertów od zabezpieczeń komputerowych z US-CERT i ICS-CERT. W centrum znajdowali się też przedstawiciele wszystkich czołowych firm telekomunikacyjnych i innych branż posiadających infrastrukturę krytyczną.

McGurk przesłał kopię Stuxneta do laboratorium ICS-CERT w Idaho Falls, gdzie analitycy stwierdzili, że kod uwalniał ładunek tylko w konkretnych modelach sterowników PLC Siemensa. Dwa lata wcześniej w ramach programu badawczego laboratorium przeprowadziło ocenę zabezpieczeń oprogramowania Step 7 — tego samego, które było atakowane przez Stuxneta. Jednak używany w trakcie testów sterownik PLC został zwrócony Siemensowi. Laboratorium musiało poprosić Siemensa o przesłanie nowego urządzenia, aby zobaczyć, w jaki sposób Stuxnet uwalnia ładunek. Sterownik dotarł po trzech tygodniach, a wraz z nim pojawiła się grupa inżynierów Siemensa.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W tym czasie badacze w Idaho zastosowali inżynierię odwrotną do kodu ładunku, a analitycy w centrum kontroli w Wirginii przyglądali się kodowi pocisku, dokumentując wszystkie jego funkcje na rozbudowanym schemacie blokowym. McGurk wyjaśnił, że w ciągu dwóch dni analitycy skatalogowali ok. 4000 funkcji (więcej niż w większości komercyjnych pakietów oprogramowania) i odkryli cztery eksploity typu zero-day znalezione później w firmach Symantec i Kaspersky.

Organizacja ICS-CERT 20 lipca opublikowała komunikat dla właścicieli systemów kontroli z informacją, że zostało znalezione złośliwe oprogramowanie atakujące system Step 7 Siemensa. W komunikacie podano bardzo niewiele szczegółów na temat działania Stuxneta. Autorzy napisali tylko, że „wszystkie możliwości tego złośliwego oprogramowania i jego przeznaczenie […] nie są jeszcze znane". W późniejszym komunikacie znalazło się więcej szczegółów na temat używanych w Stuxnecie eksploitów typu zero-day. Pojawiły się też informacje o tym, jak wykryć i usunąć szkodliwy kod. Autorzy nie napisali jednak, jak miał wyglądać sam atak. W ogóle nie wspomnieli też o sabotażu[21]. McGurk stwierdził, że zadaniem rządu jest pomagać właścicielom infrastruktury krytycznej w wykrywaniu i usuwaniu Stuxneta, a nie przedstawiać szczegółowe analizy złośliwego oprogramowania[22].

Kilka dni po zakończeniu analiz McGurk odbył telekonferencję z przedstawicielami kilku agencji rządowych i prywatnych firm, aby podzielić się swoimi odkryciami. W większości dyskusji na temat złośliwego oprogramowania i luk zwykle w grupie znajduje się kilku krytyków, którzy bagatelizują znaczenie problemu lub twierdzą, że dany fragment kodu nie jest niczym nowym. Czasem taką funkcję pełnili przedstawiciele agencji federalnych. W innych sytuacjach byli to właściciele i operatorzy infrastruktury krytycznej lub producenci omawianych systemów kontroli. Jednak gdy McGurk przedstawił szczegółowe informacje o Stuxnecie, w słuchawce zapadła cisza. „Wszyscy w tej samej chwili pomyśleli sobie: »O cholera«" — powiedział[23].

[21] ICS-CERT Advisory ICSA-10-201-01, „USB Malware Targeting Siemens Control Software", ICS-CERT Advisory ICSA-10-238-01B, „Stuxnet Malware Mitigation".

[22] W komunikatach organizacji ICS-CERT znajdował się odsyłacz do dodatkowych informacji w witrynie Symanteca, autorzy nie napisali jednak, co czytelnicy tam znajdą.

[23] Wszystkie cytowane słowa McGurka pochodzą z wywiadu przeprowadzonego przez autorkę we wrześniu 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dziwne było to, że nikt nie wspominał o źródle Stuxneta — ani w trakcie rozmowy, ani w centrum kontroli NCCIC. McGurk stwierdził, że gdy kod pojawił się po raz pierwszy, obecni na sali analitycy wywiadu z różnych agencji sprawdzili poufne źródła pod kątem informacji lub raportów dotyczących tego robaka, jednak niczego nie znaleźli. Powiedział też, że nikt w centrum kontroli nie rozważał głośno tego, czy robak nie został wypuszczony przez Stany Zjednoczone. Człowiek z zewnątrz mógł się zastanawiać, dlaczego nikt nie zwrócił się do siedzących na sali analityków z CIA lub NSA, aby mrugnąć do nich i zapytać: „Czy to wasze?". McGurk utrzymywał, że nikomu nie przyszło to do głowy, ponieważ zadaniem ludzi z centrum kontroli nie było ustalanie źródła ataku. Ich misja polegała na odkryciu, jakie są możliwości kodu, i ustaleniu najlepszego sposobu na ochronę przed nim amerykańskich sieci.

„Na początku, gdy przyglądasz się [złośliwemu oprogramowaniu] zakładasz, że nie jest to nasz ogień. Nie myślisz, że snajper na dachu to strzelający do nas jeden z naszych ludzi — powiedział. — Może się okazać, że jest inaczej […] Jednak w trakcie akcji, na samym początku, nie przejmujemy się tym nadmiernie i nie przyjmujemy domyślnie takiego założenia".

Jednak Stuxnet bardzo szybko stał się „obiektem poważnego zainteresowania" ze strony Waszyngtonu. W ciągu kilku następnych tygodni i miesięcy McGurk przedstawiał sprawę wielu wysoko postawionym osobom i ważnym jednostkom: sekretarz Departamentu Bezpieczeństwa Wewnętrznego Janet Napolitano, Johnowi Brennanowi i innym członkom Rady Bezpieczeństwa Narodowego przy Białym Domu, Senackiej i Prezydenckiej Komisji ds. Wywiadu, Departamentowi Obrony i Agencji Wywiadu Wojskowego. Pojechał nawet do Fortu Meade, aby wprowadzić w sprawę gen. Keitha Alexandra, dyrektora Cyberdowództwa Stanów Zjednoczonych i NSA, czyli jednostek, które wiele osób w społeczności zajmującej się zabezpieczeniami podejrzewało o autorstwo ataku.

W Forcie Meade kilkanaście wysokich rangą osób z wojska, rządu i wywiadu słuchało McGurka, jak opisywał odkrycia swojego zespołu. Pytanie o to, czy to Stany Zjednoczone stoją za atakiem, nigdy nie padło. Uczestnicy spotkania zapytali McGurka, czy Stuxnet jest wymierzony w amerykańskie systemy kontroli i ile amerykańskich systemów jest podatnych na

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

atak złośliwego kodu[24]. Chcieli się też dowiedzieć, czy zespół McGurka potrafi określić cel ataku. Na koniec zapytali, czy w kodzie znajdowało się coś, co ujawniało jego źródło. McGurk powiedział, że kod nie zawierał wskazówek pozwalających ustalić jego autorów. W kodzie nie było nawet „odcisków palców" pasujących do sposobu działania znanych grup hakerów lub międzynarodowych szpiegów.

McGurk utrzymuje, że nigdy — czy to w trakcie poufnych spotkań, czy w czasie publicznych zeznań — nikt nie zadał pytania, które wszystkim przychodziło do głowy. „Nie wydaje mi się, żeby ktokolwiek, choćby żartem, powiedział w trakcie formalnego spotkania: »Słuchajcie, czy to my to zrobiliśmy?«. Nie tak przebiegają tego rodzaju interakcje. Jestem pewien, że w innych miejscach pojawiały się różne spekulacje, jednak na naszym poziomie ich nie było".

McGurk stwierdził też, że żadna z osób, którym przedstawiał swoje odkrycia, nie wywarła na nim wrażenia pozwalającego sądzić, iż Stuxnet został opracowany w Stanach. „Gdy byłem w gabinecie, to niezależnie od tego, kim byli słuchacze — nawet jeśli były to wysoko, naprawdę *wysoko* postawione osoby z wywiadu — nigdy nie odniosłem wrażenia, że cała ta sprawa jest dla nich tylko zasłoną dymną — powiedział. — To samo dotyczy Departamentu Bezpieczeństwa Wewnętrznego, gdzie prezentowałem sprawę ludziom aż do poziomu sekretarza. Nigdy nie odczułem, że, rozumiesz, już o tym wiedzieli […] i czekali tylko na to, aż sobie pójdę".

Nikt też nie sugerował McGurkowi, że powinien zrezygnować z analizowania Stuxneta. „Nikt nie stwierdził: »Słuchaj, przestań w tym grzebać, zostaw to w spokoju, nie interesuj się tym« — mówił. — Wszystkie organizacje chętnie z nami współpracowały […] wspierając nas w analizach i pomagając zrozumieć, co nam grozi".

[24] Okazało się, że system Step 7 Siemensa zdobył niecałe 10% amerykańskiego rynku systemów kontroli. Analitycy z NCCIC ustalili to na podstawie bazy danych używanej przez firmy badawcze do prezentowania statystyk dotyczących penetracji rynku przez różne produkty. Baza obejmowała m.in. rozmaite sprzedawane w Stanach Zjednoczonych systemy kontroli procesów przemysłowych wytwarzane przez rozmaitych producentów. Badacze stwierdzili, że w Stanach najwięcej systemów Step 7 jest używanych w fabrykach, choć systemy te były stosowane także w rolnictwie, zakładach uzdatniania wody i elektrowniach.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak nawet jeśli urzędnicy w Waszyngtonie nie zadawali otwarcie oczywistego pytania, eksperci i obserwatorzy byli prawie pewni, że to Stany Zjednoczone odpowiadają za atak — same lub wespół z Izraelem. Ujawnienie szczegółów związanych z atakiem wydawało się tylko kwestią czasu.

Stwierdzenie Ralpha Langnera, że Stuxnet był precyzyjną bronią wymierzoną w irański program nuklearny, musiało zasiać konsternację i panikę w korytarzach Białego Domu i Pentagonu, ponieważ intryga, przez wiele lat starannie planowana i realizowana, powoli była ujawniana na ich oczach.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 11

CYFROWA INTRYGA SIĘ ROZWIJA

W 2010 r. Stuxnet stanowił przyczynę zmartwień na korytarzach Białego Domu, jednak w maju 2008 r. osoby mające wiedzę na temat tego tajnego programu były pełne optymizmu, ponieważ intryga związana z nową cyberbronią rozwijała się dokładnie zgodnie z planem.

W Stanach Zjednoczonych w najlepsze trwała właśnie kampania prezydencka, w której kandydaci Barack Obama i John McCain walczyli o pozycję lidera w sondażach. George Bush zaczynał ostatni okres prezydentury, gdy w trakcie wizyty w Izraelu związanej z 60. rocznicą powstania tego kraju usłyszał odważną prośbę. Izraelczycy chcieli pomocy i poparcia Stanów Zjednoczonych w kwestii nalotów na zakład wzbogacania uranu w Natanzie.

Izrael nalegał na naloty przynajmniej od 2003 r., kiedy to inspektorzy MAEA po raz pierwszy odwiedzili Natanz i w próbkach środowiskowych znaleźli cząsteczki wysoko wzbogaconego uranu. Rozmowy o ataku zamarły na pewien czas, po tym jak irańscy urzędnicy w latach 2003 i 2004 zgodzili się zawiesić prace nad wzbogacaniem uranu. Plany nalotów pojawiły się ponownie w 2006 r., gdy Iran wycofał się z porozumienia o wstrzymaniu prac i przystąpił do instalowania pierwszych wirówek w jednej z podziemnych hal zakładu. Obecnie, gdy działało już 3000 wirówek, a wkrótce ich liczba miała zostać podwojona, o ataku mówiło się głośniej niż kiedykolwiek wcześniej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Izrael nie był jedynym państwem optującym za nalotami. Według tajnych depesz rządowych ujawnionych przez serwis WikiLeaks za zamkniętymi drzwiami arabscy sąsiedzi Iranu byli równie stanowczy w sprawie powstrzymania programu nuklearnego realizowanego w tym kraju. „Wszyscy jesteśmy przerażeni" — powiedział w pewnym momencie egipski prezydent Hosni Mubarak amerykańskim dyplomatom[1]. Król Arabii Saudyjskiej Abdullah w prywatnej rozmowie nalegał, by Stany Zjednoczone wyświadczyły wszystkim przysługę w kwestii Iranu i Ahmadineżada i „odcięły wężowi głowę"[2]. Wyposażony w broń nuklearną Iran był zagrożeniem nie tylko dla Izraela, ale dla pokoju w całym regionie, jak powiedział Muhammad ibn Zaid an-Nahajan, książę Abu Zabi. Stwierdził też, że jeśli Iran wyprodukuje bombę, „rozpęta się piekło". Ostrzegł, że Egipt, Arabia Saudyjska, Syria i Turcja też będą starały się uzyskać broń nuklearną, aby zachować równowagę[3]. Także w administracji Busha znajdowały się osoby o „jastrzębim" nastawieniu, które popierały naloty. Bush nazywał ich chłopcami od bombowców. Jednym z nich był wiceprezydent Dick Cheney, popierający rok wcześniej atak Izraela na Syrię[4].

Jednak Bush sprzeciwiał się nalotom. „Zupełnym absurdem jest podejrzewanie, że szukam pretekstu do ataku na Iran" — powiedział w 2007 r.[5]. Nawet gdyby prezydent popierał naloty, miałby trudności ze zdobyciem dla nich powszechnej akceptacji. W badaniu Instytutu Gallupa z listopada 2007 r. 73% Amerykanów preferowało sankcje i działania dyplomatyczne, a nie atak z powietrza. Ponadto w opublikowanym w tym samym roku raporcie NIE stwierdzono, że Iran nie pracuje aktywnie nad bronią nuklearną, co dodatkowo zmniejszyło poparcie dla nalotów.

---

[1] Dziennikarze „Spiegla", *Cables Show Arab Leaders Fear a Nuclear Iran*, „Der Spiegel", 1 grudnia 2010.

[2] Depesza Departamentu Stanu USA od *chargé d'affaires* Michaela Gfoellera, 20 kwietnia 2008 (*http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html?_r=0#report/iran-08RIYADH649*).

[3] *Cables Show Arab Leaders Fear a Nuclear Iran*, „Der Spiegel".

[4] Jeffrey Goldberg, „*The Point of No Return*, „The Atlantic Monthly", wrzesień 2010.

[5] Catherine Collins, Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking*, Free Press, Nowy Jork 2011, s. 212.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Izrael znajdował się już wcześniej w podobnej sytuacji, gdy potrzebował poparcia Stanów Zjednoczonych dla nalotów. Było tak w 1981 r., gdy zlikwidowano reaktor w irackim Osiraku, oraz w roku 2007, gdy zbombardowano domniemany reaktor nuklearny w Syrii[6]. Agenci wywiadu izraelskiego zdobyli kluczowe informacje na temat tego ostatniego obiektu w 2006 r., kiedy to pojechali za wysoko postawionym urzędnikiem syryjskim do Londynu i zainstalowali konia trojańskiego w jego laptopie, pozostawionym nierozsądnie w pokoju hotelowym. Złośliwe oprogramowanie przesłało z tego komputera dziesiątki dokumentów, w tym plany i zdjęcia kompleksu w miejscowości al-Kibar. Zdaniem Izraelczyków Syryjczycy chcieli wybudować tam reaktor nuklearny na potrzeby produkcji broni. Izrael zdobył poparcie Stanów Zjednoczonych dla ataku po przedstawieniu dowodów na to, że Syrii w budowie pomaga Korea Północna[7].

Wieczorem 5 września 2007 r. rozpoczęła się operacja Orchard. Izraelskie myśliwce wystartowały z bazy w północnym Izraelu i ruszyły na zachód w kierunku morza, po czym nagle odbiły na wschód. Przeleciały nisko nad granicą syryjską i zlikwidowały stację radarową w pobliżu granicy z Turcją, używając ataków elektronicznych i bomb o wysokiej precyzji. Mniej więcej 20 min później zrzuciły ładunek nad kompleksem al-Kibar, po czym bezpiecznie wróciły do domu. Syryjski prezydent Baszszar al-Asad zbagatelizował nalot i stwierdził, że Izraelczycy trafili tylko w pusty budynek wojskowy. „Nie ma w nim ludzi ani wojska. Nic w nim nie ma" — powiedział[8].

---

[6] W czerwcu 1991 r. Cheney, ówczesny sekretarz obrony, w trakcie wizyty w Izraelu podobno przekazał izraelskiemu generałowi Davidowi Ivry'emu zdjęcie satelitarne reaktora w Osiraku po jego zniszczeniu. Cheney dodał do zdjęcia podpis: „Dla gen. Ivry'ego z podziękowaniami i uznaniem za świetną robotę, jaką wykonał w sprawie irackiego programu nuklearnego w 1981 r., co znacznie ułatwiło nasze zadanie w czasie Pustynnej Burzy". Zob. Douglas Frantz, Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets*, Free Press, Nowy Jork 2007, s. 190.

[7] Erich Follath, Holger Stark, *The Story of „Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor*", „Der Spiegel", 2 listopada 2009. Informacje o elektronicznej broni służącej do wyeliminowania stacji radarowej znajdziesz w: David A. Fulghum, *U.S. Watches Israeli Raid, Provides Advice*, „Aviation Week", 21 listopada 2007.

[8] Julian Borger, *Israeli Airstrike Hit Military Site, Syria Confirms*, „Guardian", 1 października 2007.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak wywiad Stanów Zjednoczonych ustalił, że reaktor mógłby zacząć działać ledwie kilka tygodni od czasu zniszczenia go przez Izraelczyków[9].

Teraz Izrael chciał przeprowadzić podobną akcję w Iranie, uważając, że nalot spowolni irański program nuklearny przynajmniej o trzy lata. Przy czym atak na Iran niósł za sobą znacznie więcej komplikacji i zagrożeń niż naloty na Syrię i Irak. W obu wcześniejszych przypadkach Izraelczycy atakowali jeden nadziemny obiekt bez silnych umocnień. Ponadto w Syrii cel był na tyle blisko, że piloci mogli szybko przeprowadzić atak i wrócić, zanim Syryjczycy mieliby czas zareagować. Natomiast nalot na Iran wymagał uzupełniania paliwa i przelotu nad dużymi obszarami arabskiej przestrzeni powietrznej. Dodatkowo zamiast jednego celu samoloty miały zaatakować przynajmniej sześć obiektów rozproszonych po kraju, w tym zakład wzbogacania uranu w Natanzie i zakład przetwarzania tego pierwiastka w Isfahanie. Niektóre z tych kompleksów znajdowały się pod ziemią. Iran wyciągnął wnioski z izraelskiego ataku na Irak sprzed wielu lat i wiedział, że kluczem do utrzymania programu nuklearnego jest rozproszenie obiektów na terenie państwa. Amerykańscy urzędnicy mieli „niewielką wiarę" w to, że Izrael w ogóle zna lokalizację wszystkich obiektów, które powinien zniszczyć, aby spowolnić program[10]. Izraelski doradca ds. bezpieczeństwa narodowego, Giora Eiland, nawet się do tego przyznał, gdy w 2006 r. powiedział delegacji amerykańskiego Kongresu: „Nie znamy wszystkich lokalizacji i nie wiemy, czego nie wiemy"[11].

W orędziu ze stycznia 2002 r. prezydent Bush umieścił Iran wśród krajów „osi zła" (obok Iraku i Korei Północnej), zagrażających pokojowi na świecie. Stwierdził, że Stany Zjednoczone nie pozwolą „najbardziej niebezpiecznym reżimom świata zagrażać nam najbardziej niszczycielską bronią"[12].

---

[9] David Albright zauważył, że po uzyskaniu pełnej mocy reaktor mógłby co rok – dwa lata produkować wystarczająco dużo plutonu do zbudowania broni nuklearnej. Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*, Free Press, Nowy Jork 2010, s. 3.

[10] Tim Shipman, *U.S. Pentagon Doubts Israeli Intelligence Over Iran's Nuclear Program*, „Telegraph", 5 lipca 2008.

[11] Depesza Departamentu Stanu USA, „Israeli NSA Eiland on Iranian Nuclear Threat", 26 kwietnia 2006. Została ona opublikowana w serwisie WikiLeaks: *https://wikileaks.org/plusd/cables/06TELAVIV1643_a.html*.

[12] Erich Follath, Holger Stark, *The Birth of a Bomb: A History of Iran's Nuclear Ambitions*, „Der Spiegel", 17 czerwca 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Były to mocne słowa. W późniejszych latach, pełnych trudności związanych z prowadzeniem wojny w Iraku, Bush złagodził nastawienie. Sekretarz obrony Robert M. Gates był przekonany, że atak na Iran nie tylko zakończy się niepowodzeniem, ale też będzie miał poważne konsekwencje dla wojsk amerykańskich w Iraku i Afganistanie. Taka akcja mogła też prowadzić do odwetu terrorystów na Izraelu ze strony proirańskich grup w Libanie i Strefie Gazy, a także do zmian cen ropy i zawirowań ekonomicznych na całym świecie. Najważniejsze było jednak to, że naloty, zamiast ograniczyć ambicje nuklearne Iranu, mogły zwiększyć determinację tego kraju w kwestii budowy broni atomowej i spowodować usunięcie inspektorów MAEA. W efekcie działania nuklearne Iranu stałyby się jeszcze mniej jawne. Z tych i innych powodów Bush odrzucił naciski Izraela na naloty, co nie oznaczało braku alternatywnej strategii[13].

Dwa lata później doradcy Busha przedstawili mu coś, co wydawało się lepszym, a może nawet doskonałym rozwiązaniem problemu z Iranem. Gdy wiosną 2008 r. Bush odbył ostatnią wizytę w Izraelu jako prezydent, wydawało się, że plan może zostać zrealizowany.

NIE WIADOMO, KIEDY dokładnie rozpoczęto planowanie i budowanie Stuxneta. Jednak mniej więcej w 2006 r., po zerwaniu przez Iran porozumienia o wstrzymaniu programu nuklearnego, przedstawiciele amerykańskiego wojska i wywiadu mieli zaprezentować prezydentowi propozycję cyberoperacji nazwanej później Olympic Games (czyli „igrzyska olimpijskie"). Bush przez pewien czas rozważał różne możliwości. Ponieważ Stany toczyły dwie przedłużające się i trudne wojny w Iraku i Afganistanie, już wcześniej zdecydował, że nie chce otwierać trzeciego frontu na Bliskim Wschodzie. Wykluczone były też tajne akcje lądowe prowadzące do fizycznego sabotażu irańskich obiektów nuklearnych, ponieważ takie działania zapewne doprowadziłyby do wojny[14].

Dlatego doradcy zaproponowali trzecią możliwość — cyfrową bombę, która odpowiednio zaprojektowana i użyta pozwoli osiągnąć te same efekty

[13] David E. Sanger, *U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site*, „New York Times", 10 stycznia 2009.

[14] David E. Sanger, *Iran Moves to Shelter Its Nuclear Fuel Program*, „New York Times", 1 września 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

co jej kinetyczna odpowiedniczka, ale bez ryzyka i konsekwencji tradycyjnych ataków.

Pracownicy wojska i wywiadu przygotowywali się do tego rodzaju ataku od prawie dziesięciu lat. Angażowali się wcześniej w mniejsze cyberoperacje, ale nigdy nie podejmowali akcji na proponowaną skalę. Poprzednie operacje były zwykle prostymi misjami szpiegowskimi realizowanymi za pomocą narzędzi cyfrowych lub działaniami cyfrowymi wspomagającymi broń konwencjonalną. Tego typu posunięcia miały wspomagać żołnierzy na polu walki, a nie ich zastępować[15].

Proponowany innowacyjny plan wymagał cyfrowego ataku na wirówki i systemy komputerowe w Natanzie w celu fizycznego sabotażu prac Irańczyków nad wzbogacaniem uranu. Z taką operacją związanych było wiele wymogów i ograniczeń. Uderzenie musiało cechować się chirurgiczną precyzją i trafiać w konkretne maszyny, które Stany Zjednoczone chciały zaatakować. Inne systemy powinny pozostać nienaruszone. Kod musiał ominąć wewnętrzne zabezpieczenia, tak aby mógł niewykryty miesiącami wykonywać swoją czarną robotę. Ponadto powinien wyrządzić na tyle duże szkody, aby przynieść znaczące efekty, a jednocześnie nie zwracać na siebie uwagi.

Gdyby jednak atak się powiódł, przyniósłby bardzo duże korzyści. Uszkodzenie za pomocą cyberataku irańskich wirówek IR-1 lub spowolnienie w inny sposób szybkiej drogi tego kraju do nuklearnego przełomu dałoby więcej swobody w działaniach dyplomatycznych. Zapewniłoby też MAEA i wywiadowi więcej czasu na zebranie dowodów na nuklearne aspiracje Iranu, a także pozwoliło tymczasowo uspokoić Izraelczyków. Izraelscy urzędnicy oskarżali Stany Zjednoczone o nadmierną ostrożność w stosunku do Iranu. Cyfrowy atak na program nuklearny byłby dowodem na to, że Amerykanie nie ograniczają się do biernego oczekiwania na powodzenie sankcji i działań dyplomatycznych.

Co ważniejsze, gdyby udało się uszkodzić wirówki i doprowadzić do zmarnowania uranu w formie gazowej, wyczerpałoby to już malejące irańskie zapasy cennych materiałów potrzebnych w programie nuklearnym. Eksperci szacowali, że Iran posiada materiały wystarczające do zbudowania tylko od 12 tys. do 15 tys. wirówek. Gdyby atak spowodował zniszczenie

[15] Więcej informacji o historii cyberbroni w Stanach Zjednoczonych znajdziesz w rozdziale 12.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

kilku tysięcy tych urządzeń, podane szacunki znacznie by zmalały. Przy odrobinie szczęścia atak mógł też doprowadzić do sporów politycznych w irańskim reżimie. Na Ahmadineżada i jego zwolenników już wywierana była presja w kwestii postępów programu nuklearnego. Gdyby tajny atak zaprzepaścił ich starania i cofnął program o kilka lat, mogło to doprowadzić do rozłamu we władzach.

Cyberatak miał wiele zalet w porównaniu z operacjami innego typu. Cyfrowa bomba mogła przynieść te same efekty co bomba kinetyczna bez narażania życia pilotów. Ponadto skutki można było osiągnąć z ukrycia, co było niewykonalne w przypadku bomby fizycznej. Robak mógł tygodniami i miesiącami pozostawać niewykryty i uszkadzać system. Irańczycy ostatecznie dostrzegliby efekty cyfrowego sabotażu, gdyby jednak został on przeprowadzony prawidłowo, nigdy nie poznaliby przyczyn uszkodzeń. Mogliby tylko dociekać, czy źródłem problemów był defekt materiałów, błąd programistyczny, czy jeszcze coś innego. Nawet gdyby wykryli złośliwe oprogramowanie, odpowiednio przeprowadzony atak cyfrowy nie powinien zostawić odcisków palców pozwalających wyśledzić jego źródło. Ta wygodna możliwość wyparcia się ataku była niezwykle istotna, ponieważ Stany Zjednoczone próbowały zapobiec wojnie, a nie ją wywołać.

Cyfrowy atak związany był też z innymi korzyściami. Naloty były utrudnione, gdy celem bombardowań miały być obiekty ukryte głęboko pod ziemią, takie jak kompleks w Natanzie i inne irańskie zakłady[16]. Jednak cyfrowy atak pozwalał prześliznąć się przez systemy obrony powietrznej i płot pod napięciem oraz łatwo przedostać się do podziemnej infrastruktury

[16] W połowie 2007 r. satelity zachodnich państw zarejestrowały dowody wskazujące na możliwość budowy tunelu w górze w pobliżu Natanzu. Możliwe, że miało to pozwolić ukryć materiały i sprzęt w obawie przed spodziewanym atakiem na obiekt. NCRI donosiła, że Iran rzeczywiście w kilkunastu miejscach kraju buduje tajne tunele, aby chronić instalacje rakietowe i nuklearne przed potencjalnym atakiem. Izrael podpisał ze Stanami Zjednoczonymi kontrakt na bomby penetrujące nowej generacji. Miały być one dziesięciokrotnie potężniejsze niż bomby poprzedniej generacji i przebijać cement oraz docierać w głąb ziemi. Jednak nowe bomby miały być gotowe dopiero w 2009 lub 2010 r. Nie było też gwarancji, że sprawdzą się w Natanzie. Zob. David Albright, Paul Brannan, „New Tunnel Construction at Mountain Adjacent to the Natanz Enrichment Complex", ISIS, 9 lipca 2007 (*http://isis-online.org/uploads/isis-reports/documents/IranNatanzTunnels.pdf*), oraz William Broad, *Iran Shielding Its Nuclear Efforts in Maze of Tunnels*, „New York Times", 5 stycznia 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

niedostępnej z powietrza ani w żaden inny sposób. Możliwe było też uszkodzenie wirówek nie tylko w znanych obiektach, ale też w *nieznanych*. Nie da się umieścić bomby w nieznanej fabryce, jednak cyberatak bombowy na nieznany obiekt jest możliwy. Gdyby w Iranie znajdowały się inne tajne zakłady wzbogacania uranu używające tych samych urządzeń i konfiguracji co w Natanzie, broń cyfrowa umieszczona na komputerach serwisujących je firm rozprzestrzeniłaby się ze znanych obiektów do nieznanych.

Cyfrowy sabotaż, choć na zdecydowanie mniej zaawansowanym poziomie, nie był niczym nowym. W latach 80. CIA, Departament Obrony i FBI przeprowadziły wspólną operację w celu sabotażu oprogramowania i sprzętu kierowanego do Związku Radzieckiego. Wszystko zaczęło się od tego, że ppłk Władimir Ippolitowicz Wietrow, 48-letni pracownik Pionu X Departamentu Technologii KGB, zaczął przekazywać Francuzom informacje na temat trwającej od dziesięciu lat radzieckiej operacji, której celem była kradzież zachodnich technologii.

Wietrow przekazał ok. 3000 dokumentów, nazwanych przez Francuzów Farewell Dossier (czyli „teczką Farewella"). W aktach znajdowała się długa lista technologii, które Sowieci już zdobyli, a także wykaz rozwiązań, które dopiero chcieli pozyskać. Gdy lista trafiła do dr. Gusa Weissa, doradcy ekonomicznego w Radzie Bezpieczeństwa Narodowego za rządów Ronalda Reagana, Weiss zaproponował ówczesnemu dyrektorowi CIA, Williamowi Caseyowi, przebiegły plan. CIA miała pozwolić Sowietom na pozyskiwanie potrzebnych im technologii, przy czym agencja szpiegowska miała dołączać zmodyfikowane projekty i schematy, aby zmylić wroga i sprawić, że jego prace badawcze doprowadzą tylko do straty pieniędzy. Weiss zaproponował też modyfikację produktów i komponentów przed przekazaniem ich za żelazną kurtynę, tak aby technologie przechodziły wszelkie testy zapewniania jakości, jakim mogą je poddać Sowieci. Problemy miały pojawiać się dopiero później. Plan prowadził do sytuacji wygrana – wygrana, ponieważ nawet gdyby Sowieci odkryli operację kontrwywiadu, w przyszłości stale byliby podejrzliwi względem informacji lub technologii pozyskanych z Zachodu. Nie byliby pewni, jak i czy w ogóle zostało coś zmienione lub kiedy coś przestanie działać. Byłaby to „rzadkość w świecie szpiegostwa" — napisał później Weiss w wewnętrznym newsletterze CIA,

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

gdzie opisał cały plan. „Operacja zakończyłaby się sukcesem nawet w przypadku jej wykrycia”[17].

Zgodnie z planem „zmodyfikowane układy komputerowe trafiały do wyposażenia wojskowego Sowietów, wadliwe turbiny były instalowane w gazociągach, a błędne plany zakłócały działanie zakładów chemicznych i fabryki traktorów” — pisał Weiss. Ponadto Sowieci otrzymali mylące informacje na temat myśliwców taktycznych, samolotów typu stealth i zachodnich programów obrony przestrzeni kosmicznej. Weiss ujawnił również, że sowiecki prom kosmiczny został zbudowany na podstawie przekazanego Sowietom „projektu odrzuconego przez NASA”[18].

Według Weissa operacja Farewell nigdy nie została wykryta, natomiast Wietrow miał mniej szczęścia. Został uwięziony w 1982 r. po dźgnięciu nożem swojej kochanki, zamężnej współpracowniczki z KGB, i ujawniono jego rolę podwójnego agenta. Jednak sabotaż prowadzony przez CIA pozostał tajemnicą[19]. W 1986 r. CIA zakończyła operację.

Weiss już nie żyje i nigdy nie ujawnił efektów działania zmodyfikowanych układów komputerowych i innych wadliwych części wprowadzonych w sowiecki łańcuch dostaw. Jednak w 2004 r. Thomas C. Reed, współpracownik Weissa w Radzie Bezpieczeństwa Narodowego, napisał książkę,

---

[17] Później ten newsletter został odtajniony. Zob. Gus Weiss, *The Farewell Dossier: Strategic Deception and Economic Warfare in the Cold War*, „Studies in Intelligence”, 1996 (*https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm*).

[18] Według Weissa CIA prowadziła też kampanię dezinformacyjną na temat broni laserowej, aby przekonać Sowietów, że ta niesprawdzona technologia jest czymś, w co powinni inwestować. Gdy CIA znalazła sowieckie dokumenty z opisem tej technologii, zaaranżowała publikację tekstów znanych fizyków w czasopiśmie „Nature” i innych poważanych magazynach, aby wywołać szum wokół laserów i wzbudzić wrażenie, że jest to obiecujące odkrycie. Potem nagle wstrzymano publikowanie takich prac, aby Sowieci zaczęli myśleć, że nowa technologia ma strategiczne znaczenie, dlatego zabroniono pisać na jej temat. Weiss mówił, że Sowieci musieli połknąć haczyk, ponieważ wiele lat później, po upadku Związku Radzieckiego, znaleziono dowody na to, że Sowieci prowadzili badania nad technologią laserową.

[19] Pełną historię życia Wietrowa i sprawy Farewell Dossier opisali Siergiej Kostin i Eric Raynaud w książce *Farewell: The Greatest Spy Story of the Twentieth Century*. Ta książka, opublikowana we Francji w 2009 r., została przetłumaczona na język angielski przez Catherine Cauvin-Higgins i wydana w 2011 r. przez wydawnictwo Amazon Crossing. Na jej podstawie nakręcony został francuski film z 2009 r. *L'affaire Farewell*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

w której wspomniał o sprawie Farewell Dossier i powiązał eksplozję rurociągu na Syberii w 1982 r. z planem CIA. Była to ta sama eksplozja, o której wspominali badacze Symanteca w poświęconym Stuxnetowi wpisie z bloga. Według Reeda jednym z komponentów z listy Pionu X było oprogramowanie do sterowania pompami, zaworami i turbinami rurociągu transsyberyjskiego, budowanego na potrzeby przesyłu gazu z syberyjskich pól gazu Urengoj do państw europejskich. Gdy CIA dowiedziała się, że Sowieci próbowali pozyskać oprogramowanie od kanadyjskiej firmy, agencja we współpracy z tą firmą umieściła w kodzie bombę logiczną. Kod miał zmieniać szybkość pracy pompy i ustawienia zaworów w rurociągu, aby „wytworzyć ciśnienie znacznie wykraczające ponad wartości dopuszczalne dla złączy i spawów" — napisał Reed[20]. Oprogramowanie „znakomicie sterowało rurociągiem — do czasu". Jednak później, w określonym momencie, prowadziło do rozregulowania pomp i zaworów oraz wytworzenia tak wysokiego ciśnienia gazu, że nastąpiła eksplozja o sile 3 kt (kiloton). Według Reeda była to „najbardziej monumentalna nienuklearna eksplozja i pożar widziane z przestrzeni kosmicznej".

Niektórzy autorzy uważają, że ta historia o eksplozji rurociągu jest nieprawdziwa. Były pracownik KGB zaprzeczył tym opowieściom i stwierdził, że Reed i Weiss mylą fakty[21]. Jednak Farewell Dossier istniała i posłużyła za inspirację dla późniejszych planów sabotażu irańskiego programu nuklearnego.

---

[20] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War*, Presidio Press, Nowy Jork 2004, s. 268 – 269.

[21] Opowieści Reeda o eksplozji rurociągu były pierwszą publikacją na ten temat, po czym zaczęły żyć własnym życiem i były wielokrotnie powtarzane jako fakt, choć żadnemu dziennikarzowi nie udało się ich potwierdzić. Istnieją powody, by wątpić w prawdziwość tej historii. Według Reeda eksplozja została zarejestrowana przez amerykańskie satelity wykonujące zdjęcia w podczerwieni i spowodowała wzburzenie wśród członków Rady Bezpieczeństwa Narodowego, którzy chcieli ustalić, czy Sowieci zdetonowali na Syberii urządzenie atomowe. Weiss powiedział im, by się nie martwili, nie wyjaśnił jednak, dlaczego. Gdy 20 lat później Reed pisał swoją książkę, Weiss poinformował go, że przyczyną niepokojącej eksplozji był sabotaż ze strony CIA. Jednak Wasilij Pczelincew, były szef KGB w okręgu, w którym według Reeda nastąpiła eksplozja, zaprzeczył tym słowom. Stwierdził, że Weiss musiał pomylić sprawę Farewell Dossier z eksplozją z kwietnia 1982 r. w innym regionie. Zdaniem Pczelincewa tamta eksplozja została spowodowana przez przesunięcie się rury w wyniku stopnienia śniegu, a nie przez sabotaż ze strony CIA. Zob. Anatoly Medetsky, *KGB Veteran Denies CIA Caused '82 Blast*, „Moscow Times", 18 marca 2004. Zapytany o to, czy wierzy

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jedna z takich operacji nastąpiła po tym, jak CIA ok. 2000 r. zinfiltrowała sieć dostaw A.Q. Khana i zaczęła wstawiać przerobione części do komponentów wysyłanych do Iranu i Libii (gdy Khan zaczął świadczyć nielegalne usługi nuklearne także drugiemu z tych państw). Ekspert ds. broni pracujący w Laboratorium Narodowym Los Alamos pomógł CIA zmodyfikować serię pomp próżniowych, tak by w losowych odstępach czasu popełniały błędy. Podobnie jak w operacji przeciw Sowietom, tak i tu plan polegał na wyrafinowanym sabotażu komponentów, aby przez pewien czas działały poprawnie, a następnie psuły się w taki sposób, żeby trudno było wykryć wzorzec lub ustalić źródło problemu.

Z siedmiu uszkodzonych przez CIA pomp sześć trafiło do Libii, jednak siódma znalazła się w Iranie. Inspektorzy MAEA później przypadkowo natrafili na nią w trakcie wizyty w Natanzie[22]. Irańczycy najwyraźniej nie wiedzieli, że pompa została zmodyfikowana.

Odkryli jednak inną akcję sabotażową, która została przeprowadzona w 2006 r. Dotyczyła ona zasilaczy UPS pozyskanych od Turcji. Takie zasilacze pomagają regulować przepływ prądu i są ważne dla działania wirówek,

---

w opowieści Weissa na temat rurociągu, Reed odpowiedział mi w wywiadzie telefonicznym z października 2010 r.: „Tak naprawdę nie wiem, co się stało. […] Najwyraźniej cała ta operacja Dossier miała miejsce. Agencja wkładała bardzo dużo wysiłku w modyfikowanie technologii w sprzęcie wysyłanym Rosjanom". Stwierdził też, że pamięta, iż eksplozja wydarzyła się w czasie, gdy pracował dla Rady Bezpieczeństwa Narodowego. „Zapamiętałem, że miało miejsce jakieś poważne zdarzenie, które zaniepokoiło wywiad". Jednak czy rzeczywiście chodziło o eksplozję rurociągu? „To było trzydzieści lat temu — powiedział, przyznając, że we wspomnieniach jego i Weissa przez lata mogły pojawić się nieścisłości. — Wierzę rosyjskim historykom, którzy twierdzą, że nie było eksplozji związanej ze sprawą Dossier. […] Możliwe więc, że nastąpiła eksplozja, ale nie była ona wynikiem działania konia trojańskiego. […] Nie wiem, jaka była prawda". Mimo wszystko nadzieja na to, że w przyszłych opisach historii rurociągu pojawią się odpowiednie zastrzeżenia, może okazać się płonna.

[22] Gdy inspektorzy MAEA zobaczyli pompę w Natanzie, zwrócili na nią uwagę, ponieważ była do niej przyczepiona plakietka informująca, że urządzenie jest własnością Narodowego Laboratorium Los Alamos. Inspektorzy uznali, że to dziwne. W trakcie śledztwa MAEA stwierdziła, że pompa miała numer seryjny następujący po numerach pomp, jakie agencja widziała w Libii. Wskazywało to na to, że wszystkie urządzenia pochodzą z tej samej partii. Inspektorzy prześledzili zamówienie na pompy prowadzące do wspomnianego amerykańskiego laboratorium. Nikt nigdy nie odkrył, w jaki sposób plakietka z Los Alamos znalazła się na pompie w Natanzie ani dlaczego nie wzbudziła ona podejrzeń Irańczyków. Zob. Collins, Frantz, *Fallout*, s. 138.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wymagających stabilnego i stałego dopływu energii, aby mogły obracać się przez długi czas z równomierną szybkością. Gdy napięcie się zmienia, wirówki przyspieszają lub zwalniają, co zakłóca proces wzbogacania uranu, a nawet może doprowadzić do destabilizacji wirówek.

Sieć Khana najwyraźniej zakupiła urządzenia od dwóch biznesmenów z Turcji i potajemnie sprzedała je Iranowi i Libii[23]. Jednak na początku 2006 r., gdy Iran próbował wzbogacić pierwszą porcję uranu w małej kaskadzie w zakładzie pilotażowym w Natanzie, wystąpiły poważne problemy. Kaskada działała prawidłowo ok. dziesięciu dni, a potem ujawniły się skutki sabotażu i wszystkie wirówki trzeba było zastąpić. Wówczas nie pojawiły się żadne doniesienia na ten temat. Dopiero rok później, w trakcie nagrywanego przez telewizję wywiadu, szef irańskiej Agencji Energii Atomowej opisał, co się stało. Technicy zainstalowali w kaskadzie 50 wirówek, jednak pewnej nocy „wszystkich 50 urządzeń eksplodowało". Zasilacz UPS kontrolujący przepływ prądu „nie zadziałał prawidłowo" i spowodował spięcie. „Później odkryliśmy, że zasilacze UPS, które zaimportowaliśmy za pośrednictwem Turcji, zostały zmodyfikowane". Powiedział też, że po tym incydencie Iran zaczął sprawdzać wszystkie importowane komponenty przed ich użyciem[24].

Były też inne plany modyfikacji komponentów do irańskiego programu nuklearnego, lecz przynajmniej jedna akcja została odwołana, a kolejne nie doprowadziły do oczekiwanych skutków[25]. Jednak to, co doradcy Busha zaproponowali w 2006 r., miało wznieść czarną sztukę sabotażu na zupełnie nowy poziom.

---

[23] Frantz, Collins, *Nuclear Jihadist*, s. 238.

[24] Wywiad z Gholamem Rezą Aghazadehem ze stycznia 2007 r. przeprowadzony przez *Ayande-ye* (czyli „nową przyszłość"). Wywiad nie jest dostępny w internecie, jednak wzmianki o nim znajdują się w: Sheila MacVicar, Farhan Bokhari, „Assessing Iran's Nuclear Program", CBS News, 4 kwietnia 2007 (*http://www.cbsnews.com/news/assessing-irans-nuclear-program/*).

[25] Jedna z nieskutecznych operacji planowanych przez Mosad i CIA (co opisuje James Risen w książce *State of War*) miała polegać na zastosowaniu impulsu elektromagnetycznego do uszkodzenia komputerów używanych w irańskich obiektach nuklearnych. Szpiedzy zamierzali przemycić do Iranu sprzęt, który wygeneruje impuls elektromagnetyczny przekazany później do linii przesyłowych przy obiektach nuklearnych. CIA zrezygnowała jednak z tego planu, gdy uznała, że potrzebny sprzęt jest zbyt duży, aby wwieźć go ciężarówkami do Iranu i umieścić w ukryciu. James Risen, *State of War: The Secret History of the CIA and the Bush Administration*, Free Press, Nowy Jork, s. 208 – 209.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Propozycja dotyczyła samodzielnego, przeprowadzonego z chirurgiczną precyzją ataku z użyciem kodu, który po wypuszczeniu zacznie działać niezależnie, będzie potrafił stwierdzić znalezienie celu i uwolni ładunek tylko wtedy, gdy warunki będą właściwe. Kod miał też ukrywać swoje istnienie, starannie monitorując próby wykrycia go, oraz uszkadzać urządzenia nie w wyniku gwałtownej eksplozji, ale w subtelny i stopniowy sposób.

Niektórzy urzędnicy z administracji Busha mieli wątpliwości, czy taki atak może zadziałać. Porównywali go do niepoprzedzonego testami eksperymentu naukowego[26]. Jednak osoby planujące akcję nie oczekiwały cudów. Celem nie było całkowite zniszczenie irańskiego programu wzbogacania uranu, tylko spowolnienie go i zyskanie dodatkowego czasu. Ponadto nawet gdyby Irańczycy wykryli atak i dowiedzieli się, że ich komputery zostały zainfekowane, dla Amerykanów nadal była to sytuacja typu wygrana – wygrana (jak nazwał ją Weiss w kontekście sprawy Farewell Dossier), ponieważ wzbudziłaby wątpliwości i paranoję wśród Irańczyków. Nawet jeśliby technicy sformatowali maszyny i zaprogramowali je od nowa, nigdy nie mogliby mieć pewności, że systemy nie zostaną ponownie zainfekowane lub że napastnicy nie spróbują innego ataku. Dlatego musieliby nieustannie zwracać uwagę na jakiekolwiek oznaki problemów, a po wystąpieniu kłopotów nie mieliby pewności, czy powodem są wady materiałowe, czy sabotaż. Ponadto Irańczycy musieliby zachować znacznie większą ostrożność w stosunku do sprzętu pozyskanego spoza Iranu, ponieważ mógł on być zainfekowany.

Ten odważny i zaawansowany plan, łączący tajne (ang. *clandestine*) i utajnione (ang. *covert*) działania, został podobno opracowany przez amerykańskie dowództwo strategiczne — jednostkę Departamentu Obrony odpowiedzialną za operacje z użyciem broni nuklearnej i nadzorowanie jej. Za jednego z architektów akcji uważany jest gen. James Cartwright[27]. Były wysoki

[26] Sanger, *U.S. Rejected Aid for Israeli Raid…*

[27] Operacje *tajne* (ang. *clandestine*) obejmują niejawne działania, które mają pozostać niewykryte i niezauważone. Chodzi tu np. o inwigilację i zbieranie danych w celu zdobycia informacji o celu, który może zostać później zaatakowany. Natomiast operacje *utajnione* (ang. *covert*) są zauważane, ponieważ ich celem jest zmiana sytuacji politycznej, ekonomicznej lub militarnej, jednak podmiot odpowiedzialny za takie akcje, np. CIA, pozostaje niejawny. Operacja Stuxnet obejmowała i tajne, i utajnione działania. Akcje tajne polegały na wstępnym rekonesansie w celu zdobycia informacji o obiekcie. Natomiast umieszczenie szkodliwego kodu w systemie kontroli w celu wytrącenia wirówek z ich osi było akcją utajnioną, ponieważ jej efekty miały zostać zauważone z zachowaniem w ukryciu źródła ataku.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

urzędnik amerykański stwierdził, że gen. Cartwright był twórcą koncepcji ataku, natomiast były dyrektor NSA Keith Alexander odpowiadał za realizację planu. „Rola Cartwrighta polegała na przedstawianiu zakresu możliwości, prezentowaniu wizji" — powiedział urzędnik gazecie „Washington Post". Alexander posiadał zaś „wiedzę techniczną i realizował konkretne zadania"[28]. Pisaniem kodu zajmował się, przynajmniej na początku, elitarny zespół programistów w NSA. W późniejszych wersjach podobno połączono kod z NSA z kodem Jednostki 8200 Sił Obronnych Izraela (był to izraelski odpowiednik NSA). Po zakończeniu prac kod miał być wręczony CIA, która miała nadzorować dostarczenie go do celu. Wynikało to z tego, że tylko CIA posiada uprawnienia do prowadzenia tajnych operacji.

Związane z operacją trudności techniczne były bardzo poważne. Do rozwiązania pozostawały też kwestie prawne, ponieważ propozycja dotyczyła ataku na infrastrukturę innego kraju bez wypowiedzenia mu wojny. Akcje utajnione wymagały autoryzacji w postaci aktu prawnego o nazwie *Presidential Finding*, a także powiadomienia Kongresu. Zanim Bush zatwierdził operację, przeprowadzone zostały długie analizy zagrożeń związanych z operacją[29].

Na szczęście sabotaż wirówek w kaskadzie nie groził katastrofą nuklearną. Sześciofluorek uranu w większych ilościach był szkodliwy dla płuc i nerek, jednak cała kaskada zawierała tylko kilkadziesiąt gramów tego gazu. Po uwolnieniu gaz szybko rozproszyłby się w powietrzu.

Nawet jeśli nie trzeba było przejmować się ewentualną katastrofą nuklearną, należało uwzględnić inne zagrożenia, w tym ryzyko uszkodzenia komputerów w Natanzie, gdyby kod zawierał błąd lub był niezgodny z używanymi tam systemami. Awaria komputerów mogła naprowadzić Irańczyków na atak i zaprzepaścić operację. Ponadto odkrycie przez Iran, że to Stany Zjednoczone stoją za atakiem, groziło odwetem. Ktoś mógł też zmodyfikować kod i zastosować go przeciwko infrastrukturze krytycznej Amerykanów.

Prawdopodobnie największą obawą było zagrożenie ujawnienia amerykańskich możliwości w zakresie cyberataków Iranowi i innym wrogom. Jeden z byłych agentów CIA powiedział, że problem z używaniem cyberbroni

[28] Ellen Nakashima, Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, „Washington Post", 2 czerwca 2012.

[29] Sanger, *U.S. Rejected Aid for Israeli Raid…*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

polega na tym, iż „gdy się ją zastosuje, jest tak jak z pierwszym wykorzystaniem myśliwców typu stealth. Karty zostają odkryte i nie można już udawać, że takie myśliwce nie istnieją. Pojawia się więc pytanie, na którym polu bitwy chcesz zastosować takie myśliwce”[30].

Czy operacja przeciw Iranowi była warta ujawnienia nowych możliwości? I co z utratą przewagi moralnej, gdy wszyscy się dowiedzą, że to Stany Zjednoczone są źródłem ataku? Cyfrowy atak, który uszkadza infrastrukturę krytyczną innego kraju — a Iran z pewnością stwierdzi, że jego wirówki *były* taką infrastrukturą — oznaczał działania wojenne. Bardzo trudno byłoby później Stanom Zjednoczonym oskarżać inne państwa przeprowadzające tego rodzaju ataki.

Nie wiadomo, jak dużo badań i pracy włożono w plan przed zaproponowaniem go przez doradców Busha w 2006 r. Jednak gdy prezydent wyraził zgodę na tę utajnioną operację, zrealizowanie planu zajęło podobno tylko osiem miesięcy[31].

Była to genialna intryga realizowana dokładnie zgodnie z planem.

Aż do momentu, w którym to się zmieniło.

[30] Z wywiadu przeprowadzonego przez autorkę w 2012 r.

[31] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Crown, Nowy Jork 2012, s. 193.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 12

NOWY FRONT WALK

Zanim doradcy Busha przedstawili mu pomysł zastosowania precyzyjnej broni cyfrowej w celu sabotażu irańskich wirówek, przez niemal dziesięć lat trwały prace w tym obszarze. Motywacją do nich było uświadomienie sobie, że sieci wojskowe są podatne na atak wroga.

Naukowcy i eksperci wojskowi zastanawiali się nad cyberwojnami i bronią cyfrową od jeszcze dłuższego czasu. Już w latach 70. rada naukowa Departamentu Obrony analizowała potencjał militarny ataków na sieci komputerowe, tak aby stawały się zawodne lub bezużyteczne tzw. wojnie informacyjnej. Jednak wówczas niewiele operacji było zinformatyzowanych, a internet jeszcze nie istniał. Dlatego tego rodzaju teoretyczne rozważania musiały poczekać na to, aż rzeczywistość je dogoni.

Stało się tak w latach 90. Mniej więcej w tym samym czasie powstała nazwa cyberwojna (ang. *cyberwar*), która pojawiła się w przełomowym artykule „Cyberwar Is Coming!" opublikowanym w 1993 r. przez RAND. „Przewidujemy, że cyberwojna może być dla XXI wieku tym, czym *blitzkrieg* był dla wieku XX" — napisali wówczas John Arquilla i jego współautor[1]. Arquilla, obecnie profesor w Naval Postgraduate School w Kalifornii i konsultant ds. wojskowych, dostrzegł możliwość cyfrowych ataków w trakcie pierwszej wojny w Zatoce Perskiej, kiedy Stany Zjednoczone zastosowały

[1] John Arquilla, David Ronfeldt, „Cyberwar Is Coming!"; artykuł został opublikowany przez RAND w 1993 r. i ponownie jako rozdział 2. w książce Arquilli i Ronfelda *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, 1997.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

specjalny system radarowy do wykrywania ruchomych celów w Iraku i zdały sobie sprawę, że mógł on zostać łatwo zablokowany, gdyby Irakijczycy znaleźli sposób na zakłócenie jego pracy. Arquillę uderzyło to, że technologie informatyczne stanowiące o sile nowoczesnej armii potencjalnie mogą okazać się jej słabym punktem. „Było to niepokojące tym bardziej, że niezbędna siła znajdowała się w rękach sporej grupy hakerów — powiedział później — a nie tylko w rękach armii". Ponadto niszczycielska moc drugoplanowych grup „błyskawicznie rosła"[2].

Wojsko po raz pierwszy zetknęło się z możliwościami hakerów w latach 80., kiedy to Niemiec Markus Hess, podobno zrekrutowany przez KGB, włamał się do setek systemów militarnych i jednostek badawczych, m.in. do Laboratorium Narodowego Lawrence'a w Berkeley, szukając danych na temat satelit i systemu obronnego Star Wars[3]. Później nastąpiły inne alarmujące sytuacje. W 1990 r., w okresie poprzedzającym pierwszą wojnę w Zatoce Perskiej, holenderscy nastolatkowie włamali się do ok. 30 amerykańskich komputerów wojskowych, szukając informacji o rakietach Patriot, broni nuklearnej i operacji przeciw Irakowi. Urzędnicy obawiali się, że nastolatkowie planowali sprzedać te dane Irakijczykom. Później, w 1994 r., 16-letni brytyjski haker, uczący się od 21-latka w Walii, złamał systemy Sił Powietrznych Stanów Zjednoczonych i wykorzystał je do włamania się do południowokoreańskiego instytutu badań jądrowych, a także do zaatakowania setek innych ofiar. Ponieważ wyglądało to tak, jakby źródłem włamań były komputery armii Stanów Zjednoczonych, stało się jasne, że potencjalne konsekwencje tego rodzaju ataków nie ograniczają się do kradzieży danych. Stany Zjednoczone prowadziły wówczas delikatne negocjacje w kwestii broni atomowej z Koreą Północną. Wojskowi obawiali się, że gdyby hakerzy obrali sobie za cel obiekt w Korei Północnej, mogłoby to postawić oba kraje na krawędzi wojny[4].

---

[2] Aquilla wypowiadał się w programie *CyberWar!* z serii *Frontline* stacji PBS w 2003 r. Wywiad jest dostępny na stronie: *http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html*.

[3] Operacja została powstrzymana przez Cliffa Stolla, administratora systemu, który natrafił na atak w trakcie szukania źródła 75-centowej rozbieżności w rozliczeniach. Stoll wspomina tę historię w swojej klasycznej już książce *The Cuckoo's Egg: Tracking a Spy Through a Maze of Computer Espionage*, Doubleday, Nowy Jork 1989.

[4] Jonathan Ungoed-Thomas, *How Datastream Cowboy Took U.S. to the Brink of War*, „Toronto Star", 1 stycznia 1998.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak sieci były obosiecznym mieczem. Skoro amerykańskie systemy okazały się podatne na atak, to samo dotyczyło też systemów ich wrogów. Ponieważ Stany Zjednoczone nie miały wówczas możliwości przeprowadzenia podobnych ataków, zostały rozpoczęte działania w tym kierunku.

Siły Powietrzne jako pierwsze podjęły prace w tym obszarze w 1993 r., kiedy to przekształciły Centrum ds. Wojny Elektronicznej (ang. *Electronic Warfare Center*) w Wojskowe Centrum Sił Powietrznych ds. Wojny Informacyjnej (ang. *Air Force Information Warfare Center*) i dwa lata później utworzyły Szwadron 609 do Działań Informacyjnych (ang. *609 Information Warfare Squadron*) — pierwszą wojskową jednostkę cyberwojenną[5]. Była ona zlokalizowana w Bazie Sił Powietrznych im. Shawa w Karolinie Południowej, a jej zadaniem było łączenie ofensywnych i defensywnych cyberoperacji na potrzeby wspierania jednostek bojowych[6]. Operacje ofensywne były wówczas tylko teoretyczne, dlatego jednostka koncentrowała się na działaniach defensywnych. Wojsko jednak szybko zauważyło, że korzystne jest łączenie operacji defensywnych i ofensywnych, ponieważ zabezpieczanie własnych sieci przed atakami wroga pozwalało zdobyć wiedzę i umiejętności potrzebne do ataku. W 1996 r. szwadron zorganizował ćwiczenia z udziałem drużyn czerwonych i niebieskich, aby przetestować ofensywne i defensywne umiejętności jednostki. W ciągu dwóch godzin drużyna czerwonych przejęła pełną kontrolę nad systemem lotniczych rozkazów bojowych niebieskich.

W 1997 r. wojsko przeprowadziło bardziej formalne ćwiczenia o nazwie Eligible Receiver, aby sprawdzić zdolność do obrony przed atakami wroga. W ramach ćwiczeń drużyna czerwonych, w skład której wchodzili hakerzy z NSA, miała zaatakować sieci amerykańskiego Dowództwa Pacyfiku na Hawajach. Napastnicy nie mogli wykorzystywać wewnętrznej wiedzy i niczego oprócz gotowych narzędzi dostępnych dla przeciętnych hakerów. Najpierw drużyna rozpoczęła ofensywę z użyciem komercyjnego konta internetowego z dostępem wdzwanianym i nie napotykając większego oporu,

[5] Działania w wojnie informacyjnej to nie tylko ofensywne i defensywne cyberoperacje, ale też działania psychologiczne, wojna elektroniczna i fizyczne niszczenie celów związanych z informacjami.

[6] Historia Szwadronu 609 jest opisana w 39-stronicowej książeczce. Egzemplarz tej książki, zatytułowanej *609 IWS: A Brief History Oct. 1995 – June 1999*, pozyskano na podstawie ustawy o wolności informacji. Obecnie książka jest dostępna na stronie: *http://securitycritics.org/wp-content/uploads/2006/03/hist-609.pdf*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

od razu włamała się do wojskowych sieci. Administratorzy systemu na Hawajach nie wiedzieli o ćwiczeniach i wykryli tylko dwie spośród wielu ingerencji, jakich napastnicy dopuścili się w ciągu 90 dni. Nawet wtedy nie pomyśleli o włamaniach, ponieważ incydenty przypominały standardowy ruch, jakiego można się było spodziewać w sieci. Sytuacja była podobna jak w trakcie ataku na Pearl Harbor w 1941 r., kiedy to operator stanowiska radarowego Opana na wyspie Oahu dostrzegł nadlatujące samoloty kierujące się w stronę wyspy, ale nie ogłosił alarmu, ponieważ jego przełożeni sądzili, że są to przyjazne jednostki.

Hakerzy z drużyny czerwonych umieścili w systemie specjalne pliki, aby wbić wirtualną flagę dowodzącą, że weszli do środka. Opracowali też zestaw symulowanych ataków pokazujących, w jaki sposób mogliby przejąć kontrolę nad sieciami zasilania i komunikacyjnymi w Oahu, Los Angeles, Chicago i Waszyngtonie. Gdyby chcieli, mogli uzyskać kontrolę nad systemem służącym do dowodzenia setkami tysięcy żołnierzy lub wywołać „długotrwałe awarie zasilania i inne sytuacje, które doprowadziłyby do niepokojów społecznych". Były to słowa trójgwiazdkowego gen. Johna H. Campbella, emerytowanego już generała Sił Powietrznych, który wówczas kierował operacjami informatycznymi w Pentagonie. Te ćwiczenia „przeraziły mnóstwo osób — powiedział później Campbell — ponieważ to, co drużynie udało się zrobić, miało daleko idące implikacje"[7].

Gdy później dowódcy wojskowi dowiedzieli się o ćwiczeniach, początkowo zakładali, że drużyna czerwonych wykorzystała tajne narzędzia i techniki. Byli zaskoczeni informacjami, że NSA zastosowała rozwiązania dostępne dla każdego nastoletniego hakera.

Rok później grupa nastolatków włamała się do sieci wojskowych za pomocą tego samego rodzaju prostych technik. Tę sprawę nazwano Operation Solar Sunrise. Napastnikami, którzy wykradli poufne dane z 500 systemów,

[7] John „Soup" Campbell wypowiadał się w ramach spotkania panelowego „Lessons from Our Cyber Past: The First Military Cyber Units" zorganizowanego przez Atlantic Council 5 marca 2012 r. Campbell w grudniu 1998 r. został pierwszym dowódcą grupy wojskowej Połączonych Sił Operacyjnych — Ochrona Sieci Komputerowych. Później był głównym doradcą ds. spraw wojskowych przy dyrektorze CIA. Zapis dyskusji ze wspomnianego spotkania znajdziesz na stronie: *http://www.atlanticcouncil.org/news/transcripts/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

okazali się dwaj nastolatkowie z Kalifornii, wychowankowie izraelskiego hakera Ehuda Tenebauma. Departament Obrony prowadził wówczas dwie kampanie wojskowe: w Iraku oraz w Bośni i Hercegowinie. Dla dowódców wojskowych opisany atak wyglądał tak, jakby został przeprowadzony przez wroga chcącego zyskać przewagę na polu walki. Zastępca sekretarza obrony John Hamre sądził, że te ataki „mogą być pierwszymi strzałami w prawdziwej cyberwojnie, a ich źródłem może być Irak"[8]. Była to przeniesiona w rzeczywistość sytuacja z filmu *Gry wojenne*, która podkreśliła trudność w odróżnieniu ataku ze strony innego państwa od działań nastolatków sprawdzających, na ile mogą sobie pozwolić. „Z wszystkiego, czego nauczyliśmy się w trakcie ćwiczeń Eligible Receiver, mieliśmy powtórkę w sprawie Solar Sunrise — powiedział później Hamre na temat włamania. — Nic lepiej niż rzeczywiste doświadczenia nie utrwala takich lekcji"[9].

Jednak prawdziwa lekcja nadeszła później, kiedy Hamre zwołał spotkanie w celu omówienia ataku, rozejrzał się po sali wypełnionej ponad 20 ludźmi, spytał: „Kto dowodzi? Kto odpowiada za nasze bezpieczeństwo?" i dowiedział się, że najwyraźniej nikt nie kieruje pracami związanymi z cyberatakami. Zaskoczenie tym faktem doprowadziło w grudniu 1998 r. do powstania grupy Połączonych Sił Operacyjnych — Ochrona Sieci Komputerowych. Była to pierwsza grupa wojskowa odpowiedzialna za ustalenie, jak chronić sieci wojskowe[10].

Ta grupa zadaniowa, dowodzona przez Campbella, była mieszaną jednostką składającą się z kilku pilotów myśliwców z Sił Powietrznych i Marynarki Wojennej, oficera Piechoty Morskiej, kilku ludzi z Desantu Powietrznego, nawigatora łodzi podwodnych, osób z wywiadu i kilku pracowników kontraktowych. Jeden z oficerów opisał tę grupę jako: „kilku

---

[8] Bradley Graham, *U.S. Studies a New Threat: Cyber Attack*, „Washington Post", 24 maja 1998.

[9] *Ibid.*

[10] Część informacji na temat pierwszej grupy zadaniowej i historii cyberdziałalności wojska pochodzi z przeprowadzonego w marcu 2012 r. wywiadu z Jasonem Healeyem, szefem programu Cyber Statecraft Initiative w Atlantic Council w Waszyngtonie i członkiem pierwotnego składu opisywanej grupy. Healey wspomina też historię cyberkonfliktów w zredagowanej przez niego książce, będącej jednym z pierwszych omówień tego tematu. Zob. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ludzi w kurtkach lotniczych [i] bandę cywili bez krawatów"[11]. W jednostce było niewielu geeków znających się na sieciach. Początkowo grupa nie miała biura ani personelu pomocniczego, dlatego jej członkowie musieli pracować w postawionych na parkingu przyczepach. Ostatecznie jednostka rozrosła się do ponad 150 ludzi.

Zadanie jednostki polegało na opracowaniu zasad i metod ochrony sieci Departamentu Obrony przed atakami. Zanim grupa rozpoczęła pracę, zadała dowództwu wojskowemu dwa pytania: Czy mają zbudować strukturę podobną do NORAD przeznaczoną także do ochrony cywilnej infrastruktury krytycznej? I co z akcjami ofensywnymi? „Wszyscy chcieliśmy zająć się atakiem — wspomina Marcus Sachs, inżynier wojskowy i jeden z członków pierwotnego składu grupy. — Wszyscy myśleli o potencjale wypuszczania cyfrowych kul. […] Chcieliśmy iść dalej i przekonać się, co oznaczałyby dla nas działania ofensywne"[12].

Była to era przeznaczonych dla hakerów konferencji takich jak Def Con i HOPE, dwie imprezy organizowane w Las Vegas i Nowym Jorku, które stały się popularnymi miejscami rozmów hakerów i badaczy na temat luk w zabezpieczeniach i narzędzi hakerskich[13]. FBI i wywiad każdego roku wysyłały tajnych agentów na konferencję Def Con, dlatego Sachs też zdecydował się wziąć w niej udział i zobaczyć, co wojsko mogłoby robić. Jednak grupa otrzymała polecenie, by zwolnić tempo. Usłyszała, że wojsko nie jest na razie gotowe do podejmowania akcji ofensywnych. „Kwestie prawne nie zostały jeszcze wyjaśnione" — tłumaczył Sachs.

Był też inny powód do zachowania ostrożności. Cyberbroń była „typem broni, która po wystrzeleniu nie ginie. Ktoś mógł ją podnieść i skierować przeciwko nam — powiedział Sachs. — Był to bardzo ważny powód, by jej nie stosować".

Sachs nie wiedział wówczas, że rok wcześniej sekretarz obrony uprawnił NSA do rozpoczęcia prac nad technikami ataków na sieci komputerowe. To zadanie agencja szpiegowska przyjęła jako rozszerzenie wcześniejszych

[11] Generał dywizji James D. Bryan, pierwszy dowódca jednostki Połączone Siły Operacyjne — Operacje na Sieciach Komputerowych. Wypowiedź w trakcie spotkania panelowego „Lessons from Our Cyber Past: The First Military Cyber Units".

[12] Te i inne słowa Sachsa pochodzą z wywiadu przeprowadzonego przez autorkę w marcu 2012 r.

[13] „HOPE" to akronim od *Hackers on Planet Earth*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

obowiązków z zakresu broni elektronicznej, które obejmowały zagłuszanie systemów radarowych i kanałów komunikacyjnych wroga[14]. NSA wierzyła, że jej techniczni geniusze mogą odegrać kluczową rolę także na powstającym cyfrowym polu bitwy.

Zalety walki cyfrowej w porównaniu z konwencjonalną były oczywiste, co NSA napisała w wewnętrznym newsletterze w 1997 r.[15]. W dobie transmisji telewizyjnych z pól bitwy, w której nagrania worków z ciałami obrazują gorzkie realia wojen, cyberbroń stanowi aseptyczną alternatywę, łatwiejszą do zaakceptowania przez opinię publiczną. W raporcie zwrócono też uwagę na inne korzyści: niskie koszty prowadzenia kampanii, „swobodny wybór rozmieszczenia oddziałów", ponieważ posiadanie celu „w zasięgu" nie jest koniecznością, a także różnorodny i wciąż zwiększający się zestaw celów z powodu informatyzacji coraz większej liczby systemów.

Agencje szpiegowskie już dziesięć lat przed powstaniem Stuxneta zaczęły rozważać ofensywne możliwości wynikające z rosnącej zależności świata od skomputeryzowanych systemów kontroli w infrastrukturze krytycznej. W innym artykule ze wspomnianego newslettera zaproponowane zostało przygotowanie planu analizy już dostępnych technologii, a także rozwiązań, które „są dopiero iskierką w oku jakiegoś inżyniera", pod kątem opracowania ataków na nie[16]. W newsletterze zaproponowano też przygotowanie listy publicznie dostępnych narzędzi hakerskich — wirusów,

[14] Broń elektroniczna, rozwijana już w czasie pierwszej wojny światowej, obejmuje zastosowanie skierowanej energii elektromagnetycznej do kontroli spektrum elektromagnetycznego w celu zakłócenia pracy systemów wroga. Natomiast ataki na sieci komputerowe są zdefiniowane jako operacje nakierowane na zakłócanie, blokowanie, uszkadzanie lub usuwanie informacji znajdujących się na komputerach i w sieciach komputerowych, a także samych komputerów i sieci (z Dyrektywy Departamentu Obrony nr 3600.1).

[15] Autor utajniony, *IO, IO, It's Off to Work We Go*, „Cryptolog: The Journal of Technical Health", wiosna 1997, s. 9. „Cryptolog" to wewnętrzny poufny cokwartalny newsletter pisany przez i dla pracowników NSA. Znajduje się w nim wszystko: od recenzji książek, przez informacje o pracownikach, po artykuły techniczne na odpowiednie tematy. W 2013 r. agencja odtajniła numery opublikowane między 1974 a 1999 r. i udostępniła je publicznie, choć część z nich nadal jest ocenzurowana. Archiwum numerów jest dostępne na stronie: *https://www.nsa.gov/news-features/declassified-documents/cryptologs/*.

[16] Autor utajniony, *Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium*, „Cryptolog: The Journal of Technical Health", wiosna 1997, s. 32.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

robaków, bomb logicznych, koni trojańskich i tylnych furtek. Te potężne narzędzia, „jeśli zostaną odpowiednio zastosowane", jak pisał autor, „[mogą być] niezwykle niszczycielskie dla infrastruktury informacyjnej społeczeństwa"[17]. Dotyczyło to jednak infrastruktury amerykańskiej. „Dlatego […] zanim zaczniecie się nadmiernie ekscytować bogatym w cele środowiskiem — przestrzegał autor newslettera potencjalnych cyberżołnierzy — pamiętajcie, że gen. Custer też działał w takim środowisku!"[18].

Mimo oczywistego zainteresowania prowadzeniem cyfrowych ataków problemem wciąż były kwestie prawne. Wiosną 1999 r., gdy siły NATO prowadziły bombardowania na terenie Jugosławii, organizacja AFA (ang. *Air Force Association*) zorganizowała w Teksasie zamknięte sympozjum, aby rozważyć możliwości z zakresu czegoś, co wciąż nazywano wojną informacyjną. Generał John Jumper, dowódca Sił Powietrznych Stanów Zjednoczonych w Europie, powiedział zgromadzonym, że choć wojna informacyjna może się kojarzyć z przejmowaniem „sekretnej infrastruktury" wroga, wojsko nie jest jeszcze do tego gotowe. Cyberbroń wciąż istniała głównie w laboratoriach, a jedyna wojna informacyjna, jaka się wówczas toczyła, była prowadzona między prawnikami, prawodawcami i dowódcami wojskowymi w Waszyngtonie spierającymi się w kwestii przydatności i legalności ataków na sieci[19]. Jumper powiedział: „Wyobrażam sobie wspólną odprawę na temat celów, na której znajdują się: pilot myśliwca, pilot bombowca, ludzie od operacji specjalnych i eksperci od informatyki. W trakcie omawiania listy celów każda osoba po kolei podnosi rękę i mówi: »Mogę zniszczyć ten cel«. Jednak ekspert od informatyki stwierdza: »Mogę zniszczyć ten cel, jednak najpierw muszę udać się do Waszyngtonu i uzyskać zgodę [od prezydenta]«"[20].

---

[17] William B. Black Jr., *Thinking Out Loud About Cyberspace*, „Cryptolog: The Journal of Technical Health", wiosna 1997, s. 4.

[18] Autor utajniony, *IO, IO, It's Off to Work We Go*.

[19] William M. Arkin, *A Mouse that Roars?*, „Washington Post", 7 czerwca 1999.

[20] W 1999 r. biuro głównego doradcy przy Departamencie Obrony przeanalizowało różne traktaty i prawa międzynarodowe, po czym stwierdziło, że nie istnieją międzynarodowe reguły ani prawa bezpośrednio dotyczące cyberoperacji proponowanych przez wojsko. Biuro głównego doradcy przy Departamencie Obrony, *An Assessment of International Legal Issues in Information Operations*, maj 1999 (*http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2000 r. coś zaczęło się zmieniać, gdy w Pentagonie grupa robocza ds. ochrony sieci usłyszała, że ma dodać do misji operacje ofensywne i opracować doktrynę ich przeprowadzania. Ta zmiana nastawienia doprowadziła też do zmiany nazwy jednostki z Połączone Siły Operacyjne — Ochrona Sieci Komputerowych na Połączone Siły Operacyjne — Operacje na Sieciach Komputerowych. Sachs powiedział, że zmiana była niewielka, aby uniknąć przyciągania uwagi, ale wewnętrznie sygnalizowała gotowość wojska do rozpoczęcia poważnego planowania operacji ofensywnych.

Informatyczna grupa robocza musiała teraz znaleźć odpowiedzi na wiele pytań. Czy atak na sieć to akcja wojskowa, czy utajniona operacja? Jakie były reguły przeprowadzania takich ataków? Eliminowanie skomputeryzowanych systemów komunikacyjnych wydawało się oczywistą operacją ofensywną, co jednak z sabotażem komputerowego systemu kontroli broni, by nakierować ogień na inny cel lub spowodować chybienie[21]? Ponadto kto miał odpowiadać za prowadzenie takich operacji? Wcześniej, gdy Siły Powietrzne chciały wyeliminować system radarowy wroga, współpracowały z zespołem ds. broni elektronicznej z NSA. Jednak NSA była jednostką wywiadu, której głównym zadaniem było przechwytywanie informacji. Eliminowanie komputerów kontrolujących systemy artylerii wydawało się raczej zadaniem dla jednostek bojowych.

Po dodaniu operacji ofensywnych do obowiązków informatycznej grupy zadaniowej jej nowym dowódcą został gen. dywizji James D. Bryan. Jednak zastępca sekretarza obrony Hamre jednoznacznie stwierdził, że priorytetem dla grupy nadal jest obrona, a działania ofensywne mają być dodatkiem do tradycyjnych operacji wojskowych, natomiast nie mają ich zastępować.

Było tak do czasu ataków terrorystycznych 11 września, które, jak wspomina Bryan, „zmieniły naszą sytuację". Operacje ofensywne nagle zyskały na znaczeniu i po raz pierwszy grupa zaczęła przygotowywać się do ofensywnych

[21] Przykładem tego, jak bardzo systemy sterowania bronią były zależne od oprogramowania, jest historia z operacji Pustynna Burza z 1991 r. Zainstalowany w Az-Zahranie w Arabii Saudyjskiej system obrony przeciwrakietowej Patriot nie przechwycił nadlatujących pocisków Scud z powodu problemu programowego w systemie kontroli. Błąd sprawił, że system szukał pocisków w złym miejscu. Pociski Scud zabiły wtedy 28 amerykańskich żołnierzy. Zob. „Software Problem Led to System Failure at Dhahran, Saudi Arabia", US Government Accountability Office, 4 lutego 1992 (*http://www.gao.gov/products/IMTEC-92-26*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

cyberataków w sposób, w jaki szykowano się do ataków kinetycznych. Cyberataki miały służyć eliminowaniu celów, a nie tylko wykorzystaniu komputerów na potrzeby zbierania danych lub zakłócania pracy systemów. „Zgłosiliśmy się do jednostek bojowych i poprosiliśmy o listę celów — wspominał Bryan. — Przechodziliśmy też przez proces oceny celów, analizowania ich i określania priorytetów w kontekście globalnym"[22].

Kolejny postęp w amerykańskich operacjach ofensywnych nastąpił w 2003 r., kiedy to Pentagon przygotował tajny raport „Plan Operacji Informacyjnych", który miał przekształcić wojnę informacyjną w jedną z podstawowych kompetencji armii na równi z operacjami powietrznymi, lądowymi, morskimi i specjalnymi[23]. W tym tajnym raporcie, ujawnionym kilka lat później z ocenzurowanymi fragmentami, napisano, że realizowany był już kompletny proces oceny możliwości w obszarze cyberbroni i narzędzi szpiegowskich oraz opracowywania polityki ich stosowania. W kwestii polityki próbowano ustalić, jaki poziom manipulacji danymi lub systemami stanowi atak lub wykorzystanie siły, a jaki można uznać za zwykłe pozyskiwanie danych. Należało też określić, jakie działania mogą być zgodnie z prawem podejmowane w ramach samoobrony i jakie warunki muszą być spełnione, aby Stany Zjednoczone mogły przeprowadzić atak odwetowy. Ważne było też to, czy Stany Zjednoczone mogą posłużyć się do przeprowadzenia ataku „nieświadomym pośrednikiem" (czyli prowadzić działania z użyciem innego systemu lub przejąć nad nim kontrolę w celu zaatakowania wroga), jeśli grozi to pośrednikowi odwetem.

W 2004 r. w celu uwzględnienia większego nacisku na operacje ofensywne Departament Obrony podzielił jednostkę odpowiedzialną za cyberoperacje na wydziały ofensywny i defensywny. Ten ruch dla wielu obserwatorów był sygnałem początku militaryzacji cyberprzestrzeni. Wydział defensywny nosił teraz nazwę Połączone Siły Operacyjne — Globalne Operacje Sieciowe (ang. *Joint Task Force — Global Network Operations*), a ofensywny nazwano: Połączona Jednostka Funkcjonalna — Wojenne Działania Sieciowe (ang. *Joint Functional Component Command — Network Warfare*).

[22] Bryan, „Lessons from Our Cyber Past".

[23] „The Information Operations Roadmap" z 30 października 2003 r. to odtajniony w 2006 r. 74-stronicowy raport, przy czym strony dotyczące ataków na sieci komputerowe są mocno ocenzurowane (raport znajdziesz na stronie: *http://information-retrieval.info/docs/DoD-IO.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Siedzibą tego ostatniego został Fort Meade, będący też placówką NSA. Jednostka ta podlegała Dowództwu Strategicznemu Stanów Zjednoczonych i gen. piechoty morskiej Jamesowi E. Cartwrightowi. Jednak zdaniem części obserwatorów to w następnym roku został zapoczątkowany „kult ofensywy". Stało się to, gdy gen. Keith Alexander przejął funkcję dyrektora NSA od gen. Michaela Haydena i jednostka zaczęła skupiać się na tworzeniu cyberbroni na potrzeby działań wojennych. To wtedy była realizowana operacja Olympic Games i powstał Stuxnet.

Sześć lat później, w maju 2010 r., gdy Stuxnet szybko rozprzestrzeniał się na komputerach na całym świecie i wkrótce miał zostać odkryty, Pentagon ponownie połączył wydziały odpowiedzialne za defensywne i ofensywne cyberoperacje w nowo utworzonym Cyberdowództwie Stanów Zjednoczonych. Nowy wydział nadal był częścią Dowództwa Strategicznego Stanów Zjednoczonych, ale podlegał dyrektorowi NSA gen. Alexandrowi, co dawało szefowi agencji szpiegowskiej bezprecedensową władzę nad operacjami wywiadu i działaniami cyberwojennymi. Trzy miesiące po utworzeniu Cyberdowództwa Stanów Zjednoczonych Pentagon oficjalnie uznał cyberprzestrzeń jako „piąty obszar" działań wojennych (obok powietrza, lądu, mórz i przestrzeni kosmicznej).

Wszystko to było jedynie formalnym uznaniem działań, które z różnym natężeniem realizowano już od dziesięciu lat. Jednak z powodu tajnego charakteru operacji ofensywnych opinia publiczna mogła się ich tylko domyślać na podstawie powstających przez lata przecieków.

Na przykład możliwe jest, że pod koniec lat 90. w Kosowie siły NATO zastosowały cybertechniki w celu „zniekształcania obrazów generowanych przez serbskie zintegrowane systemy obrony powietrznej", o czym wspomina John Arquilla, pracujący wówczas dla Dowództwa Strategicznego Stanów Zjednoczonych[24]. Prezydent Bill Clinton miał też zatwierdzić utajnioną cyberoperację wymierzoną w zdeponowane w europejskich bankach finansowe środki jugosłowiańskiego prezydenta Slobodana Miloševića, przy czym pojawiają się sprzeczne informacje na temat tego, czy ta operacja

[24] Wywiad z Arquillą, *Frontline*, *CyberWar!* Według artykułu z gazety „Washington Post" ataki na komputery kontrolujące systemy obrony powietrznej w Kosowie zostały przeprowadzone z samolotu zagłuszającego, a nie z naziemnych stanowisk z pośrednictwem sieci komputerowych. Bradley Graham, *Military Grappling with Rules for Cyber*, „Washington Post", 8 listopada 1999.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

rzeczywiście została zrealizowana[25]. Gdy w 2003 r. zaproponowano podobny cyberatak w celu zamrożenia aktywów finansowych Saddama Husajna, akcja została zablokowana przez sekretarza skarbu Stanów Zjednoczonych z powodu obaw przed jej lawinowym rozciągnięciem się na inne konta na Bliskim Wschodzie, w Europie i w Stanach Zjednoczonych[26].

W 2007 r. Stany Zjednoczone podobno wspomagały Izrael za pomocą cyberataku związanego z bombardowaniem kompleksu al-Kibar w Syrii. Stany miały udostępnić informacje na temat luk w syryjskich systemach obrony. Zanim izraelscy piloci dotarli do obiektu, wyeliminowali syryjską stację radarową w pobliżu tureckiej granicy, posługując się kombinacją elektronicznego sprzętu zagłuszającego i pocisków precyzyjnych. Jednak według analityków amerykańskiego wywiadu Izraelczycy włamali się do syryjskiego systemu obrony powietrznej, używając dostępnych na pokładzie samolotu technologii do „ataku elektronicznego powietrze – ziemia", i później spenetrowali ten system za pomocą łączy komputer – komputer[27]. W niedawnym raporcie Rządowego Biura ds. Odpowiedzialności Stanów Zjednoczonych opisano ataki powietrze – ziemia jako przydatne do docierania do „niedostępnych w inny sposób sieci", do których nie da się włamać za pomocą połączeń przewodowych[28].

---

[25] James Risen, *Crisis in the Balkans: Subversion; Covert Plan Said to Take Aim at Milosevic's Hold on Power*, „New York Times", 18 czerwca 1999. Według artykułu gazety „Washington Post" plan nigdy nie został zrealizowany. „Wykonywaliśmy ćwiczenia w celu ustalenia, jak przeprowadzać pewnego rodzaju cyberakcje, gdybyśmy kiedyś musieli je realizować — powiedział gazecie wysoki stopniem oficer armii. — Jednak nigdy do tego nie doszło". Graham, *Military Grappling with Rules for Cyber*.

[26] John Markoff, H. Sanker, *Halted '03 Iraq Plan Illustrates US Fear of Cyberwar Risk*, „New York Times", 1 sierpnia 2009. Według Richarda Clarke'a to sekretarz skarbu zawetował akcję. Zob. Richard Clarke, Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, Nowy Jork 2010, s. 202 – 203. Można zaobserwować niepisane porozumienie przeciw manipulowaniu systemem finansowym i kontami. Wynika ono z obaw przed destabilizacją globalnych rynków i ekonomii.

[27] David A. Fulghum, Robert Wall, Amy Butler, *Israel Shows Electronic Prowess*, „Aviation Week", 25 listopada 2007. Artykuł nie jest już dostępny w witrynie czasopisma „Aviation Week", jednak został zachowany w pełnej postaci na stronie: *https://warsclerotic.com/2010/09/28/israel-shows-electronic-prowess/*.

[28] „Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight", Rządowe Biuro ds. Odpowiedzialności, lipiec 2012.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2011 r., w trakcie powstania w Libii, prowadzone były rozmowy na temat zastosowania cyberataków w celu przerwania wojskowych łączy komunikacyjnych w tym kraju i uniemożliwienia systemom wczesnego ostrzegania wykrycia samolotów bojowych NATO. Plan został jednak odrzucony, ponieważ brakowało czasu na przygotowanie ataku. Długie przygotowania są jedną z głównych wad operacji cyfrowych. Zaprojektowanie ataku tak, aby nie uszkodził systemów cywilnych, które nie są jego celem, wymaga wcześniejszego rozpoznania i opracowania planów. Dlatego trudno jest przeprowadzać szybkie ataki tego rodzaju dostosowane do zmieniającej się sytuacji"[29].

W ostatnim okresie wycieki od Edwarda Snowdena, byłego administratora systemów w NSA, stały się jednym z najlepszych źródeł informacji o ciemnych rządowych cyberoperacjach w asymetrycznej wojnie z terrorem. W dokumentach Snowdena opisane są elitarne jednostki hakerów NSA w Forcie Meade i w oddziałach regionalnych w Georgii, Teksasie i Kolorado oraz na Hawajach. Jednostki te zapewniają Cyberdowództwu Stanów Zjednoczonych ofensywne narzędzia i techniki potrzebne do operacji antyterrorystycznych. Rządowi cyberżołnierze współpracowali też z FBI i CIA w ramach cyfrowych operacji szpiegowskich. Między innymi wspomagali CIA w śledzeniu celów na potrzeby dokonywania zabójstw za pomocą dronów.

Aby wyśledzić Hassana Ghula, zabitego z użyciem drona w 2012 r. współpracownika Osamy bin Ladena, NSA zastosowała „arsenał narzędzi cyberszpiegowskich" do przejęcia kontroli nad laptopami, przesyłania plików dźwiękowych i rejestrowania transmisji radiowych. Wszystko to miało służyć ustaleniu, gdzie Ghul może „pójść do łóżka". Informacje te pochodzą z dokumentów Snowdena zdobytych przez „Washington Post"[30]. Od 2001 r. NSA spenetrowała też wiele systemów używanych przez współpracowników Al-Kaidy w Jemenie, Afryce i w innych krajach, aby zdobyć informacje, których nie udało się uzyskać za pomocą programów masowego zbierania danych od firm internetowych (takich jak Google i Yahoo!) lub z podwodnych kabli i węzłów internetowych.

---

[29] Eric Shmitt, Thom Shanker, *US Debated Cyberwarfare in Attack Plan on Libya*, „New York Times", 17 października 2011.

[30] Greg Miller, Julie Tate, Barton Gellman, *Documents Reveal NSA's Extensive Involvement in Targeted Killing Program*, „Washington Post", 16 października 2013.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Osoby podejrzane o terroryzm nie są jedynym celem NSA. W ostatnich latach znacznie wzrosła także liczba operacji przeciw wrogim państwom. Według wspomnianych wcześniej dokumentów w 2011 r. NSA przeprowadziła 231 ofensywnych cyberoperacji przeciw innym krajom. Trzy czwarte z nich dotyczyły priorytetowych celów: Iranu, Rosji, Chin i Korei Północnej. W ramach kosztującego 652 mln dolarów tajnego programu GENIE NSA, CIA i siły specjalne zainstalowały tajne cyfrowe podsłuchy w dziesiątkach tysięcy komputerów, routerów i zapór na całym świecie na potrzeby penetracji sieci komputerowych. Niektóre podsłuchy zostały umieszczone zdalnie, jednak instalacja innych wymagała fizycznego dostępu — przechwycenia. CIA lub FBI przechwytuje przesyłki sprzętu od producentów i sprzedawców, aby umieścić w urządzeniach złośliwe oprogramowanie lub zainstalować zmodyfikowane układy przed dotarciem towaru do klienta. Takie podsłuchy lub implanty działają jak „uśpione komórki", które można zdalnie włączać i wyłączać w celu rozpoczęcia szpiegowania w dowolnym momencie[31]. Większość implantów została utworzona przez jednostkę TAO (ang. *Tailored Access Operations*) agencji NSA i otrzymała nazwy takie jak UNITEDDRAKE lub VALIDATOR. Te narzędzia zostały zaprojektowane do otwierania tylnej furtki, przez którą hakerzy z NSA mogą zdalnie badać zainfekowane systemy i podłączone do nich sprzęty, a także do instalowania dodatkowych narzędzi na potrzeby pobierania dużych ilości danych. Implanty były podobno instalowane w taki sposób, by mogły przez lata pozostać niewykryte w systemach i przetrwać aktualizacje oprogramowania i sprzętu, które standardowo powinny spowodować ich usunięcie[32]. W 2008 r. NSA miała zainstalowane 22 252 implanty w systemach z całego świata. Do 2011 r. ta liczba wzrosła do 68 975 implantów, do 2014 r. ma wynieść 85 tys., a w przyszłości mają ich być miliony. Jednak problem bogactwa spowodowany przez tak dużą liczbę implantów jest dla NSA kłopotem. Ponieważ w systemach znajduje się tak wiele implantów, agencja

[31] Barton Gellman, Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, „Washington Post", 30 sierpnia 2013.

[32] NSA robi to, instalując implant w BIOS-ie komputerów i w rekordzie MBR, czyli w podstawowych fragmentach dysku twardego, które nie są kasowane w momencie aktualizowania lub usuwania oprogramowania komputera. Zob. „Interactive Graphic: The NSA's Spy Catalog", *Spiegel Online*, *http://www.spiegel.de/international/world/a-941262.html*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

nie była w przeszłości w stanie użyć wszystkich kontrolowanych maszyn. Według dokumentów Snowdena w 2011 r. szpiedzy z NSA potrafili w pełni wykorzystać tylko 10% zainfekowanych maszyn. Aby rozwiązać ten problem, agencja planowała zautomatyzować procesy za pomocą nowego systemu o nazwie TURBINE, który miał radzić sobie z jednoczesnym zarządzaniem milionami implantów[33].

Jednak wszystkie opisane operacje — od Kosowa, przez Syrię i Libię, po działania z dokumentów Snowdena — koncentrowały się na wykradaniu lub zniekształcaniu danych oraz używaniu cybertechnik do wspomagania naprowadzania fizycznych bomb na cel. W żadnej z tych akcji cyfrowy atak nie *zastępował* tradycyjnych bomb. To sprawiało, że Stuxnet był tak odmiennym i nowatorskim narzędziem.

Stuxnet to jedyny znany cyberatak, który spowodował fizyczne szkody w systemie. Istnieją też poszlaki, że Stany Zjednoczone przygotowywały się do innych tego typu akcji. W październiku 2012 r. prezydent Obama nakazał wysokim urzędnikom agencji bezpieczeństwa narodowego i wywiadu przygotowanie listy zagranicznych celów („systemów, procesów i infrastruktury") na potrzeby możliwych cyberataków. Rozkaz ten pochodzi ze ściśle tajnej prezydenckiej dyrektywy ujawnionej przez Snowdena[34].

[33] W jednym przypadku NSA i brytyjska agencja szpiegowska GCHQ (ang. *Government Communications Headquarters*) zastosowały zaawansowaną metodę Quantum Insert do włamania się do maszyn pracowników belgijskiej firmy telekomunikacyjnej, aby uzyskać dostęp do sieci i routera używanego przez tę firmę do obsługi użytkowników telefonów komórkowych. Ten wyrafinowany atak obejmował wykorzystanie szybkich serwerów, które NSA umieściła w kluczowych punktach wymiany ruchu internetowego, aby przechwytywać dane o użytkowaniu internetu przez administratorów systemów pracujących dla wspomnianej firmy. Agencje szpiegowskie najpierw zebrały wiele informacji o pracownikach firmy: adresy e-mail, adresy IP i internetowe przyzwyczajenia. Następnie szybkie serwery obserwowały żądania kierowane z maszyn pracowników do określonych stron internetowych, np. strony z profilem ofiary w serwisie LinkedIn. Gdy ofiara próbowała otworzyć stronę w tym serwisie, serwer przechwytywał żądanie przed jego dotarciem do witryny LinkedIn i zwracał fałszywą stronę, która wstrzykiwała złośliwe oprogramowanie. Po uzyskaniu dostępu do maszyny administratora systemu agencje szpiegowskie mogły wykorzystać dane uwierzytelniające danej osoby do dostania się do innych części sieci firmy i przejęcia kontroli nad routerem.

[34] Glenn Greenwald, Ewen MacAskill, *Obama Orders US to Draw up Overseas Target List for Cyber-Attacks*, „Guardian", 7 czerwca 2013. Liczący 18 stron dokument *Presidential Policy Directive 20* został wydany w październiku 2012 r., a ofensywne cyberakcje są w nim nazywane ofensywnymi operacjami z cyberefektami.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nie wiadomo, czy Stany Zjednoczone rzeczywiście zamierzają zaatakować te cele, czy tylko chcą na wszelki wypadek opracować plany. Jednak w dyrektywie napisano, że tego rodzaju operacje mogą zapewniać „wyjątkowe i niekonwencjonalne" możliwości „realizacji narodowych celów Stanów Zjednoczonych na świecie, przy czym wróg lub cel będzie w tylko małym lub zerowym stopniu uprzedzony o ataku, a potencjalne efekty mogą wahać się od niewielkich uszkodzeń po poważne zniszczenia".

Wzrostowi liczby operacji ofensywnych i ich planów odpowiadał równy wzrost zapotrzebowania na doświadczonych hakerów i narzędzia potrzebne NSA do realizowania takich akcji. Choć większość implantów używanych przez NSA to narzędzia zaprojektowane wewnętrznie przez jednostkę TAO, w 2013 r. agencja przeznaczyła 25,1 mln dolarów na „utajnione zakupy luk w oprogramowaniu" od prywatnych dostawców, czyli od małych firm i dużych dostawców dla wojska, tworzących nową branżę przemysłu zbrojeniowego, napędzającą szary rynek narzędzi typu zero-day[35]. Trend w zlecaniu przez rząd ofensywnych cyberoperacji jednostkom zewnętrznym jest zauważalny w ogłoszeniach o pracę, które firmy z przemysłu zbrojeniowego zaczęły dawać w ostatnich latach, szukając np. „programistów ataków" na system Windows lub osób z umiejętnością „analizowania oprogramowania pod kątem luk i tworzenia kodu eksploitów". Jedna oferta, od niemieckiej firmy z przemysłu zbrojeniowego, Northrop Grumman, zawierała bezpośrednie informacje o „ekscytującym i dynamicznym projekcie z dziedziny badań i rozwoju" na potrzeby „ofensywnej cyberoperacji", nie pozostawiając wątpliwości co do charakteru stanowiska. Inne firmy w bardziej subtelny sposób piszą o swoich intencjach. Na przykład firma Booz Allen Hamilton, w której zatrudniony był Snowden w trakcie pracy dla NSA, szukała „analityka celów w postaci sieci cyfrowych" do opracowywania eksploitów „systemów operacyjnych komputerów osobistych i urządzeń mobilnych takich jak Android, BlackBerry, iPhone i iPad". W wielu ofertach na liście szukanych umiejętności pojawiają się określenia CND (ang. *Computer Network Defense* — obrona sieci komputerowych) i CNA (ang. *Computer Network Attack* — ataki na sieci komputerowe), co podkreśla dwojaki charakter badań nad lukami i eksploitami, które mogą służyć zarówno do zabezpieczania systemów, jak i ich atakowania.

[35] Gellman, Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations…*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Kim są osoby ubiegające się o takie stanowiska? Niektóre z nich to ludzie tacy jak Charlie Miller, wspomniany w rozdziale 7. matematyk zrekrutowany przez NSA w celu łamania kodu i komputerów. Czasem są to byli hakerzy, poszukiwani w równym stopniu przez organy ścigania za włamania do amerykańskich systemów rządowych, jak i przez agencje szpiegowskie ze względu na umiejętności w zakresie dokonywania podobnych włamań do systemów wroga. Niedobór wśród profesjonalistów kandydatów o odpowiednich umiejętnościach, którzy mogliby zasilić szeregi elitarnych cyberżołnierzy, sprawił, że wojsko i agencje wywiadu zaczęły rekrutować pracowników na przeznaczonych dla hakerów konferencjach takich jak Def Con. Rekruterzy, aby przyciągnąć najlepszych kandydatów, mogą wybaczyć hakerom dawne wykroczenia, obniżyć oczekiwania co do stroju biurowego lub zaakceptować kolczyki w różnych miejscach ciała. Jeden z informatycznych żołnierzy zatrudniony przez firmę pracującą dla rządu powiedział w wywiadzie, że martwił się, iż jego wcześniejsze włamanie do amerykańskich systemów rządowych uniemożliwi mu pracę dla agencji federalnych, na szczęście zatrudniająca go firma rekrutacyjna „najwyraźniej nie dbała o to, że przed laty zhakowałem nasz rząd lub że paliłem trawkę"[36].

Ten haker opisał pracę, jaką wykonywał w liczącym 5000 osób zespole zajmującym nieoznakowany budynek w nijakim kompleksie biurowym w Wirginii. Pracownicy nie mogli wnosić do budynku telefonów komórkowych ani innych urządzeń elektronicznych, ani nawet zostawiać ich w samochodach.

Wkrótce po zatrudnieniu haker otrzymał od firmy listę oprogramowania, które firma chciała, aby złamał. Szybko udało mu się znaleźć proste luki w zabezpieczeniach każdego z podanych programów. Powiedział, że jego zespół posiadał duży zbiór luk typu zero-day. Były to „dziesiątki tysięcy gotowych do wykorzystania błędów" w aplikacjach i systemach operacyjnych, pozwalających na dowolny atak. „Możesz podać nazwę dosłownie dowolnego oprogramowania lub sterownika, a my znamy sposoby na złamanie go" — powiedział. Załatane luki nie były problemem, ponieważ na każdy naprawiony przez producenta błąd przypadały inne, które pozwalały go zastąpić. „Jesteśmy nową armią. Może nie podobać ci się to, co armia robi, ale jest ona potrzebna"[37].

[36] Roger A. Grimes, „In His Own Words: Confessions of a Cyber Warrior", *InfoWorld*, 9 lipca 2013.

[37] *Ibid.*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Intensyfikacja poszukiwania błędów przez rząd zwraca uwagę na ważną kwestię, której poświęcono niewiele uwagi, gdy grupa robocza Departamentu Obrony dziesięć lat wcześniej opracowywała swoją ofensywną doktrynę (nawet dziś ten temat nie przyciąga uwagi opinii publicznej i w ogóle nie jest omawiany w Kongresie). Chodzi o etyczne i związane z bezpieczeństwem aspekty budowania zasobów luk i eksploitów typu zero-day na potrzeby operacji ofensywnych. Gromadzenie przez rząd eksploitów typu zero-day do stosowania w atakach (zamiast udostępniania informacji o lukach producentom, co pozwoliłoby rozwiązać problemy) narażało właścicieli infrastruktury krytycznej i użytkowników komputerów w Stanach Zjednoczonych na ryzyko ataków ze strony hakerów o przestępczych zamiarach, szpiegów korporacyjnych i zagranicznych agencji wywiadowczych — wszystkie te grupy bez wątpienia znajdą i zastosują te same luki na potrzeby swoich operacji.

Gdy badacze wykrywają luki, zwykle ujawniają je publicznie lub przekazują prywatnie producentowi oprogramowania, aby ten mógł udostępnić łatki użytkownikom komputerów. Jednak gdy wojsko i agencje wywiadowcze potrzebują luk typu zero-day do operacji ofensywnych, ostatnią rzeczą, na jakiej im zależy, jest powstanie łatek. Zamiast tego te jednostki trzymają kciuki, by nikt inny nie wykrył i nie ujawnił danej luki, zanim nie skończą z niej korzystać. „Jeśli wszystkie działania operacyjne zależą od istnienia danej luki, [jej załatanie] oznacza utratę systemu, którego utworzenie mogło kosztować miliony dolarów i tysiące roboczogodzin" — powiedział Andy Pennington, konsultant ds. cyberbezpieczeństwa w firmie K2Share na konferencji w 2011 r. Pennington to były oficer ds. systemów broni w Siłach Powietrznych. Przed przejściem w 1999 r. na emeryturę zajmował się oceną nowych technologii z obszaru cyberprzestrzeni i projektowaniem broni nowej generacji dla Sił Powietrznych[38]. „Nie po to zatrudniasz zespół badaczy, aby znajdowali lukę i później udostępniali ją w internecie, gdzie wszyscy mogą zobaczyć, że próbujesz opracować [atak na nią] — powiedział potem w wywiadzie[39]. — Inwestujemy miliony dolarów w wykrycie luk, abyśmy mogli je wykorzystać i zachować przewagę taktyczną".

[38] Pennington przemawiał na konferencji Systemy Kontroli Procesów Przemysłowych — Wspólna Grupa Robocza w 2011 r. Sponsorem tej konferencji był Departament Bezpieczeństwa Krajowego.

[39] Z wywiadu przeprowadzonego przez autorkę w listopadzie 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

To jednak model, w którym rząd utrzymuje podatność wszystkich na atak, dzięki czemu można przeprowadzić akcję przeciw wybranym jednostkom. Jest to odpowiednik zaprzestania szczepień całej populacji, aby wybrana grupa mogła zostać zainfekowana wirusem.

Możliwe, że gdy Stuxnet wykorzystywał cztery luki typu zero-day do zaatakowania systemów w Iranie, jakiś haker lub państwowy cyberżołnierz z innego kraju też to robił. „Gdy znajdujesz nową lukę typu zero-day, naiwnością jest wierzyć, że nie udało się to nikomu innemu na świecie — powiedział Howard Schmidt, były koordynator ds. cyberbezpieczeństwa przy Białym Domu i były dyrektor w Microsofcie. — Niezależnie od tego, czy będzie to inny rząd, badacz, czy handlarz eksploitami, będziesz miał tę lukę dla siebie może przez kilka godzin lub dni, jednak z pewnością nie na długo”[40].

Luka związana z plikami .LNK na pewno była znana atakującemu banki gangowi, który posługiwał się wirusem Zlob, już w 2008 r., czyli dwa lata przed zastosowaniem jej w Stuxnecie. Informacje o luce powiązanej z drukarką także były publicznie znane, dzięki czemu inni mogli ją znaleźć i wykorzystać[41]. Kto wie, jak długo inne luki typu zero-day używane w Stuxnecie były znane i stosowane w innych atakach? W 2007 r. Immunity, firma z Florydy działająca w branży zabezpieczeń, ustaliła, że przeciętny eksploit typu zero-day działał przez 348 dni do czasu wykrycia go w systemach. Eksploity o najdłuższym czasie życia mogły ukrywać się przez prawie trzy lata[42]. Obecne symulacje dają podobne wyniki. Średni czas życia eksploitów typu zero-day wynosi dziesięć miesięcy, a niektóre eksploity potrafią ukrywać się w systemach nawet przez dwa i pół roku[43].

---

[40] Joseph Menn, „Special Report: US Cyberwar Strategy Stokes Fear of Blowback”, Reuters, 10 maja 2013 (*http://www.reuters.com/article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510*).

[41] W rozdziale 6. znajdziesz inne informacje o wykryciu tych dwóch luk przez innych przed zastosowaniem ich przez twórców Stuxneta.

[42] Summer Lemon, „Average Zero-Day Bug Has 348-Day Lifespan, Exec Says”, IDG News Service, 9 lipca 2007 (*https://www.pcworld.idg.com.au/article/187491/average_zero-day_bug_has_348-day_lifespan_exec_says/*).

[43] Robert Lemos, „Zero-Day Attacks Long-Lived, Presage Mass Exploitation”, Dark Reading, 18 października 2012 (*http://www.darkreading.com/vulnerabilities---threats/zero-day-attacks-long-lived-presage-mass-exploitation/d/d-id/1138557?*). Badania zostały przeprowadzone przez firmę Symantec.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Krótko po objęciu urzędu w 2009 r. prezydent Obama ogłosił, że cyberbezpieczeństwo, a przede wszystkim zabezpieczanie infrastruktury krytycznej, należą do priorytetów jego administracji. Jednak ukrywanie informacji o lukach w amerykańskich systemach, aby możliwe było ich wykorzystanie za granicą, tworzy w rządzie rozłam i stawia agencje gromadzące i wykorzystujące luki typu zero-day w opozycji do innych, takich jak Departament Bezpieczeństwa Wewnętrznego, które mają chronić i zabezpieczać infrastrukturę krytyczną Stanów Zjednoczonych i systemy rządowe.

W komentarzach z konferencji z 2011 r. Andy Pennington przyznał, że w rządzie występował „konflikt interesów" w kwestii luk. Stwierdził jednak, że gdy rząd znajdował luki, które chciał wykorzystać, przeprowadzał „kontrolowane odtajnienie luki", aby „zwiększać obronność Stanów Zjednoczonych" w sposób umożliwiający rządowi zachowanie zdolności do ataku. Pennington powiedział, że Departament Obrony „bardzo ściśle współpracował z Microsoftem, wspomagając tę korporację", a także z producentami systemów kontroli, informując ich o znalezionych w ich systemach lukach. „Chciałbym jednak jeszcze raz podkreślić, że celem jest załatwianie tych spraw w taki sposób […] aby zachować możliwość prowadzenia operacji" — powiedział. Dlatego należy „bardzo rozważnie ujawniać luki i sposoby ich rozwiązania"[44]. Choć Pennington nie wyjaśnił dokładnie, na czym polegało częściowe ujawnianie luk, inne osoby sugerowały, że chodziło o przekazywanie informacji o lukach administratorom z Departamentu Obrony, dzięki czemu mogli oni podejmować kroki na rzecz ochrony systemów wojskowych przed atakami. Dane nie były przekazywane producentom i opinii publicznej, dzięki czemu nie trafiały do wrogów. Podobno Microsoft przekazuje z wyprzedzeniem rządowi i firmom prywatnym informacje o nowych lukach w zabezpieczeniach oprogramowania tej korporacji. Ma to ułatwić rządowi ochronę systemów tej firmy do czasu udostępnienia łatki, może się jednak okazać wygodną wskazówką dla NSA, pozwalającą agencji wycofać eksploity stosowane do ataku na te luki przed publicznym ujawnieniem ich przez Microsoft. NSA może też szybko zaatakować maszyny z wykorzystaniem tej luki przed jej załataniem[45].

[44] Pennington, konferencja Systemy Kontroli Procesów Przemysłowych — Wspólna Grupa Robocza, 2011.

[45] Michael Riley, „U.S. Agencies Said to Swap Data with Thousands of Firms", Bloomberg, 14 czerwca 2013 (*https://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Greg Schaffer, były zastępca sekretarza Departamentu Bezpieczeństwa Wewnętrznego, powiedział stacji NPR, że departament, pomagający chronić niemilitarne systemy rządowe, czasem otrzymuje pomoc „od organizacji pracujących nad misjami ofensywnymi". Nie wyjaśnił jednak, czy chodzi o udostępnianie departamentowi informacji o lukach, co pozwoliłoby na ich załatanie[46]. „To oni sami muszą zdecydować, czy przekażą [nam] wyniki swoich prac — powiedział. — Nie mamy na to wpływu".

Natomiast inny urzędnik z Departamentu Bezpieczeństwa Wewnętrznego stwierdził, że nie przypomina sobie „przekazania im kiedykolwiek informacji o luce przez Departament Obrony. […] Chcielibyśmy znać i kontrolować jak najwięcej luk, aby zapewnić sobie możliwie najlepsze pozycje obronne". Choć brak informacji o lukach był frustrujący, urzędnik rozumiał, że taka była „natura problemu", jeśli rząd chciał zachować możliwość ataku na wrogów. Niestety, nie widział sposobu na rozwiązanie tej kwestii[47].

Choć informacje o lukach mogły nie być przekazywane z jednostek ofensywnych do jednostek defensywnych, które mogłyby wyeliminować problemy, to czasem luki wykryte przez grupy defensywne trafiały do grup ofensywnych. Mogło to służyć np. upewnieniu się, że luka w systemie kontroli wykorzystywana już przez NSA lub inne agencje nie została zbyt wcześnie ujawniona i załatana. Były urzędnik Departamentu Bezpieczeństwa Wewnętrznego stwierdził, że ten „proces analizy zasobów w postaci luk" (ang. *vulnerabilities equities process*) w zakresie systemów kontroli, jak go nazywano, rozpoczął się niedługo po przeprowadzeniu w 2007 r. testu Aurora Generator. Od tego czasu luki znajdowane przez badaczy rządowych w innych systemach kontroli były sprawdzane przez panel ds. zasobów w celu upewnienia się, że ich ujawnienie nie zaszkodzi prowadzonym operacjom. „Jeśli ktoś wykorzystuje lukę […] zgodnie ze swoimi uprawnieniami i w uprawnionym celu […] no cóż, musimy wtedy zbilansować konieczność ujawnienia z korzyściami związanymi z tym, by przez pewien czas pozostała niezałatana" — powiedział były urzędnik.

---

[46] Tom Gjelten, „Stuxnet Raises »Blowback« Risk in Cyberwar", Morning Edition, NPR, 2 listopada 2011 (*http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar*).

[47] Z wywiadu przeprowadzonego przez autorkę w 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Analiza zasobów przez rząd ma długą tradycję. Podczas drugiej wojny światowej Brytyjczycy złamali niemiecką Enigmę. Gdy odkryli, że Niemcy szykują atak na konwoje aliantów, musieli uwzględnić korzyści płynące ze zmiany kursu statków i z uniknięcia napaści, co groziło domyśleniem się przez Niemców, że ich szyfr został złamany, oraz koszty związane z poświęceniem konwoju, co pozwalało nadal korzystać z kluczowego źródła informacji.

Amerykański proces analizy zasobów obejmuje centralną komisję składającą się z przedstawicieli różnych departamentów i agencji: Departamentu Obrony, Departamentu Sprawiedliwości, Departamentu Stanu, Departamentu Bezpieczeństwa Wewnętrznego, Białego Domu i agencji wywiadowczych. Prace te były wzorowane na modelu opracowanym przez amerykańską Komisję ds. Inwestycji Zagranicznych, znanym jako proces CFIUS, w którym analizowany był wpływ zagranicznych inwestycji w Stanach Zjednoczonych na bezpieczeństwo narodowe.

Jeśli chodzi o luki w oprogramowaniu, to gdy badacze rządowi wykryli lukę w zabezpieczeniach często używanego sterownika PLC, powiadamiali o tym odkryciu komisję, aby ustaliła, czy ktoś może być tym zainteresowany. „Każdy mógł wypowiedzieć się na temat możliwego wpływu [ujawnienia lub nieujawnienia luki] na firmy lub systemy — powiedział urzędnik. — Komunikacja odbywała się za pomocą e-maili w poufnej sieci i każdy mógł stwierdzić, czy jest zainteresowany daną luką. Jeśli ktoś był zainteresowany, omawialiśmy tę kwestię. Jeżeli nikt nie był zainteresowany, przechodziliśmy do standardowego procesu odpowiedzialnego ujawniania luki".

Zapytany o to, czy Departament Bezpieczeństwa Wewnętrznego przekazywał informacje na temat luk jednostkom ofensywnym, co umożliwiało ich wykorzystanie, urzędnik zaprzeczył. Przyznał jednak, że sam fakt omawiania luk w ramach komisji ds. zasobów mógł przypadkowo naprowadzać jej członków na pomysły na nowe luki. Sam nigdy nie słyszał, aby ktoś z komisji wymagał od przedstawiciela producenta systemu kontroli, by nie ujawniał publicznie luki, co pozwoli agencji ją wykorzystać, ale przyznał, że takie rzeczy prawdopodobnie nie były omawiane otwarcie. „Agencje zapewne po cichu robiły notatki i mogliśmy nigdy nie dowiedzieć się [czy zbudowały eksploit danej luki]" — powiedział.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 13

CYFROWE ŁADUNKI BOJOWE

Liam O'Murchu był coraz bardziej zmęczony i znudzony. Od dwóch godzin siedział przy biurku, starannie podłączając jeden po drugim wirtualne komponenty do emulatora systemu Step 7 w desperackiej próbie ustalenia, co jest celem ataków Stuxneta. Na razie nie przynosiło to jednak sukcesu.

Był początek października. Minęły tygodnie od czasu, gdy Ralph Langner zidentyfikował Stuxneta jako broń o wysokiej precyzji wymierzoną w jeden cel. Oba zespoły, w Hamburgu i Kalifornii, pracowały niezależnie (i nie wiedząc o sobie nawzajem) nad identyfikacją tego celu.

Jedną z rzeczy, jakie odkryli badacze z Symanteca, było to, że Stuxnet tuż przed wypuszczeniem niszczycielskiego ładunku w sterownikach PLC model 315 szukał w nich trzech „magicznych wartości" — kombinacji cyfr i liter umieszczonych w blokach danych sterowników. Gdy natrafiał na model 315, sprawdzał bloki danych pod kątem wartości CB 00 01, 7050h i 9500h. Znalezienie wszystkich trzech oznaczałoby dotarcie do celu.

Eric Chien szukał tych wartości w Google'u, ale nie znalazł niczego, co miało sens w kontekście Stuxneta. Badacze podejrzewali, że pierwsza z tych wartości była numerem sekwencyjnym komponentu podłączanego do sterownika PLC. O'Murchu przygotował więc z użyciem systemu Step 7 symulowane środowisko sterownika PLC, aby spróbować ustalić tożsamość tego komponentu. System Step 7 obejmował emulator do tworzenia wirtualnych sieci dla sterownika PLC na potrzeby przetestowania różnych

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

konfiguracji sprzętowych przed zbudowaniem prawdziwej sieci w zakładzie. Emulator obsługiwał długą listę komponentów, które inżynierowie mogli wirtualnie podłączać do konfiguracji jeden po drugim, klikając nazwy urządzeń w menu. Po wybraniu każdego elementu na ekranie pojawiał się jego identyfikator. O'Murchu miał nadzieję, że wśród nich znajdzie się tajemnicza wartość 2C CB 00 01. Jednak od dwóch godzin sumiennie podłączał jedno urządzenie po drugim i wciąż nie znalazł pasującego komponentu, choć sprawdził ich już ponad setkę. Zaczynał podejrzewać, że cała ta praca nie ma sensu, kiedy dotarł na liście do grupy kart Profibus i Profinet — urządzeń przesyłających dane między sterownikami PLC a kontrolowanymi przez nie urządzeniami. O'Murchu kliknął kartę Profibus CP 342-5 i pojawiła się szukana wartość.

Ale karta Profibus była tylko jednym z elementów układanki. Badacz wciąż nie wiedział, jakie urządzenia sterownik PLC miał kontrolować. Zachęcony przez swój mały sukces szybko zaczął podłączać pozostałe komponenty z listy. Wprawdzie nie pojawiła się żadna inna z magicznych wartości, nie miało to jednak znaczenia. Nowe odkrycie pozwoliło zespołowi zrobić duży krok naprzód. Teraz badacze wiedzieli, że Stuxnet szuka systemu z podłączonymi sześcioma kartami sieciowymi. Wiedzieli też, że rozwiązanie tajemnicy reszty konfiguracji jest tylko kwestią czasu.

TRZY MIESIĄCE PO wykryciu Stuxneta cały świat wiedział już o tajemniczym kodzie, który najwyraźniej miał zaatakować Iran. Lecz spekulacje na temat tego, że celem był program wzbogacania uranu w Natanzie, pozostawały wyłącznie spekulacjami. Inżynierowie z Symanteca byli blisko znalezienia potrzebnych dowodów w kodzie. Najpierw jednak potrzebowali szybkiego szkolenia dotyczącego sterowników PLC.

Odkrycie, że Stuxnet miał dokonać sabotażu sterowników PLC Siemensa, z pewnością było przełomem dla Falliere'a i jego współpracowników. Jednak Langner miał rację, zakładając, że zespół z Symanteca natrafił na przeszkodę w badaniach i utknął z powodu sterowników PLC. „Szybko dowiedzieliśmy się, że nic nie wiemy" — powiedział Chien[1].

[1] Te i inne słowa Chiena pochodzą z wywiadów przeprowadzonych przez autorkę książki w latach 2010 i 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ponadto po odkryciu, że Stuxnet wstrzykuje szkodliwy kod do sterowników PLC, Falliere stwierdził też, że robak używa nie jednego ładunku, ale *dwóch*. Stuxnet w ramach ataku na sterowniki PLC wysyłał dwa ładunki bojowe, tak jak komandosi z sił specjalnych. Jeden był przeznaczony dla sterowników PLC Siemens S7-315, a drugi dla modelu S7-417.

Do każdego sterownika PLC wstrzykiwanych było tylko kilka kilobajtów szkodliwego kodu. Złamanie tego kodu stanowiło klucz do rozwiązania największej zagadki związanej z robakiem. Był jednak pewien problem — kod został napisany w niezrozumiałym dla Falliere'a formacie i języku. Pocisk w Stuxnecie był napisany w językach C i C++ oraz skompilowany do języka asemblerowego dla procesorów Intel x86 (jest to najczęściej stosowany i powszechnie znany język asemblerowy). Natomiast w cyfrowych ładunkach zastosowano mało znany język programowania STL, przeznaczony dla sterowników PLC Siemensa[2]. W celu zaprogramowania sterowników PLC Siemensa inżynierowie pisali polecenia w języku STL, następnie przetwarzali je na język asemblerowy MC7, po czym kompilowali do postaci binarnej zrozumiałej dla sterowników PLC. To oznaczało, że nawet jeśli Falliere'owi uda się przekształcić zera i jedynki z kodu binarnego z powrotem na język STL, nadal nie będzie wiedział, co ten kod oznacza. Przypominało to odszyfrowywanie zakodowanej wiadomości ze słynnej rzeźby *Kryptos* z siedziby CIA: po odkodowaniu tekstu okazuje się, że jest on napisany po grecku. Symantec wydał 17 sierpnia komunikat, w którym prosił o kontakt osoby znające sterowniki PLC i język STL, nikt się jednak nie zgłosił.

Firma nie musiałaby publicznie szukać wsparcia, gdyby otrzymała pomoc od Siemensa, ale jej nie uzyskała. Chien w początkowym okresie analiz i w miesiącach pracy nad Stuxnetem kontaktował się z Siemensem. Jednak gdy przesyłał niemieckiej firmie pytania na temat działania systemu Step 7, Siemens odpowiadał po upływie dni lub tygodni. Do tego czasu badacze z Symanteca zwykle sami znaleźli już odpowiedź i przygotowali nowy zestaw pytań[3].

---

[2] STL to akronim od *Statement List*.

[3] Chien nie miał pojęcia, dlaczego Siemens nie odpowiadał szybciej. Możliwe, że dla tej firmy omawiany problem nie był pilny. Tylko kilkunastu klientów Siemensa zgłosiło zainfekowanie Stuxnetem. Inną możliwością było to, że Siemens nie był przyzwyczajony odpowiadać na szczegółowe pytania na temat jego oprogramowania. Badacze z Symanteca nie zadawali pytań, na które może łatwo odpowiedzieć opiekun produktu. Pytania dotyczyły kwestii inżynieryjnych związanych z działaniem kodu Siemensa.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Była też inna grupa osób mogąca im udzielić pomocy. Langner i jego zespół byli ekspertami w obszarach, które stanowiły trudność dla Symanteca. Taka współpraca byłaby doskonałym połączeniem umiejętności. Badacze z Symanteca świetnie znali się na systemach Windows i inżynierii odwrotnej szkodliwego kodu, a zespół Langnera posiadał bogatą wiedzę na temat oprogramowania i sterowników PLC Siemensa. Jednak jakiekolwiek nadzieje na współpracę zostały szybko rozwiane po krótkiej wymianie e-maili między tymi grupami i wpisach na blogu, co doprowadziło do nieporozumień i urazy po obu stronach. Powodem były niejasności w komunikacji, które można było łatwo wyeliminować w trakcie krótkiej rozmowy telefonicznej. Niestety, obu stronom zabrakło motywacji, aby wykonać potrzebny telefon.

W obliczu braku wsparcia badacze z Symanteca zrobili jedyną możliwą rzecz: kupili w internecie kilka książek na temat języka STL i zaczęli się uczyć, jak działa kod w tym języku. Uznali, że najlepszym sposobem na inżynierię odwrotną kodu w STL-u jest nauczenie się pisania w tym języku.

Falliere każdego dnia w trakcie porannych i wieczornych dojazdów metrem zagłębiał się w książkach, starając się zrozumieć kod. Przed wiele dni robił tylko niewielkie postępy, aż trafił na otwarte internetowe narzędzie utworzone przez kogoś na potrzeby programowania sterowników PLC Siemensa. Ten program był bezpłatną alternatywą dla systemu Step 7.

Dlatego firma musiała znaleźć programistów pracujących nad systemem Step 7. Jeszcze inną możliwością było to, że Siemens nie chciał nagłaśniać sprawy Stuxneta, aby nie wzbudzać dyskusji na temat interesów tej firmy w Iranie. Firma niedawno wpadła w tarapaty, gdy w Dubaju została zatrzymana dostawa jej sterowników dla irańskiego programu wzbogacania uranu. Ponadto w Hamburgu organy kontroli eksportu przechwyciły dostawę szybkich procesów Siemensa przeznaczonych dla Iranu. Obie te transakcje naruszały obowiązujący w Unii Europejskiej zakaz eksportu bez pozwolenia sprzętu o podwójnym zastosowaniu do Iranu. Siemens stwierdził, że nie wiedział, iż przesyłki były przeznaczone dla Irańczyków. Jednak te incydenty sprawiły, że CEO firmy w styczniu 2010 r. poinformował, iż Siemens od połowy 2010 r. nie będzie zawierał żadnych nowych kontraktów z Iranem. Gdy kilka miesięcy później w Iranie wykryto Stuxneta, względny brak informacji od Siemensa na temat kodu mógł po części wynikać z chęci uniknięcia dyskusji o tym, w jaki sposób sterowniki w ogóle trafiły do zakładu wzbogacania uranu. Niektórzy pracownicy Siemensa zachęcali firmę do bardziej aktywnego udziału w analizowaniu Stuxneta, lecz zostali zignorowani. W efekcie Siemens chciał, aby sprawa ucichła, i miał nadzieję, że badacze z Symanteca i innych firm zrezygnują z dalszych prac.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Falliere zapoznał się ze znalezionym narzędziem, aby zobaczyć, jak kod w STL-u wygląda po skompilowaniu do języka MC7, i na tej podstawie przystąpił do inżynierii odwrotnej kodu MC7 Stuxneta.

Praca nad inżynierią odwrotną kodu zajęła tygodnie. Po jej ukończeniu okazało się, że kilka kilobajtów kodu binarnego wstrzykiwanego przez Stuxneta do sterowników PLC rozrosło się do ponad 4000 wierszy instrukcji w ataku na model 315 i ponad 13 tys. wierszy kodu w ataku na model 417. Kod był zbyt długi i chaotyczny, aby Falliere mógł go odczytać w tym formacie. Był też zbyt skomplikowany, by badacz potrafił go zrozumieć. Dlatego Falliere zdecydował się przekształcić go na postać przypominającą kod w języku C, dzięki czemu liczba instrukcji zmalała i stały się one prostsze. To jednak pozwoliło mu tylko zapoznać się ze statycznym kodem. Bez sterownika PLC nie mógł zobaczyć przebiegu ataku. Dlatego napisał prosty program symulujący pracę sterownika w systemie Windows i wypuścił robaka. Dzięki temu oraz lekturze statycznego kodu uzyskanego za pomocą inżynierii odwrotnej mógł wreszcie zrozumieć atak.

Jedną z pierwszych rzeczy, na jakie zwrócił uwagę, było to, że atak przebiegał w sześciu powtarzanych tygodniami i miesiącami etapach. Po zakończeniu ataku robak rozpoczynał go od nowa. To oznaczało, że Stuxnet nie zadawał jednego prowadzącego do katastrofy ciosu, jak badacze początkowo zakładali. Zamiast tego w wyrafinowany sposób dokonywał rozciągniętego w czasie sabotażu. To, w połączeniu z atakiem *man in the middle*, który ukrywał sabotaż przed operatorami, sprawiało, że trudno było wykryć i precyzyjnie ustalić źródło problemów. Falliere zdał sobie sprawę, że napastnicy oczekiwali, iż atak pozostanie niewykryty przez wiele miesięcy. I rzeczywiście tak się stało.

Pierwsza część ataku, rekonesans, trwała ok. 13 dni. W tym czasie Stuxnet spokojnie ukrywał się w sterowniku PLC i rejestrował jego standardowe działanie, aby odtwarzać zapisane dane operatorom po rozpoczęciu sabotażu. Stuxnet rejestrował dane przynajmniej raz na minutę i przechodził do następnego etapu dopiero po zapisaniu danych przynajmniej 1,1 mln razy.

Po zarejestrowaniu wystarczającej ilości danych następowało dwugodzinne odliczanie. Gdy licznik dochodził do zera, rozpoczynał się sabotaż. Trwał on tylko ok. 15 min, a po jego zakończeniu wznawiana była normalna praca sterownika PLC i kontrolowanych przez niego urządzeń. Następnie, po upływie pięciu godzin, cała sekwencja zaczynała się od nowa. Tym razem

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Stuxnet odczekiwał przed atakiem ok. 26 dni i rejestrował dwa razy więcej danych niż przy pierwszym podejściu. Ponadto następna akcja sabotażowa trwała 50 min zamiast 15. Tak jak wcześniej po zakończeniu ataku działanie urządzeń wracało do normy na 26 dni i cały cykl powtarzał się jeszcze raz. Kolejne akcje trwały na zmianę po 15 i 50 min, natomiast etap rekonesansu zajmował 26 dni.

Falliere nie wiedział, dlaczego długość akcji sabotażowej się zmieniała i czym różniły się obie sekwencje. Bez informacji na temat atakowanych urządzeń nie mógł ustalić natury ataku. Przypominało to obserwowanie pocisków samonaprowadzających na nocnym niebie bez wiedzy o tym, w co mają trafić.

OSTATECZNY PRZEŁOM W STUXNETOWEJ łamigłówce nastąpił na początku listopada, kiedy to holenderski programista Rob Hulsebos, ekspert od protokołu kart Profibus, wysłał e-mail do Chiena. Hulsebos zareagował, choć z opóźnieniem, na drugą prośbę o pomoc zamieszczoną na blogu przez badaczy z Symanteca. Badacze prosili o kontakt osoby z wiedzą na temat kart Profibus i infrastruktury krytycznej. E-mail od Hulsebosa zawierał tylko dwa akapity. Większość z nich zajmowały znane już Chienowi informacje o kartach Profibus. Jednak pewne zdanie zwróciło uwagę badacza. Hulsebos napisał, że każde urządzenie peryferyjne podłączone do kart sieciowych Profibus ma przypisany mu przez kartę unikatowy numer identyfikacyjny. Każdy identyfikator był długości 2 B (16 b).

Chien przypomniał sobie, że dwie tajemnicze wartości, które badacze starali się zrozumieć — 7050h i 9500h — miały dokładnie po 16 b (bitów).

Podszedł do boksu O'Murchu i na swoim telefonie BlackBerry pokazał współpracownikowi wspomniany e-mail. Gdy Chien z niecierpliwością zaglądał koledze przez ramię, O'Murchu poszukał w Google'u identyfikatorów urządzeń łączących się z kartami Profibus. Pojawiła się seria odsyłaczy do instrukcji obsługi urządzeń. Chien wskazał jedną z nich — plik PDF z listą urządzeń często używanych razem z kartami sieciowymi Profibus. O'Murchu otworzył ten plik. Przy nazwie każdego urządzenia znajdował się opisany w e-mailu unikatowy identyfikator. Badacz przewinął listę i natrafił na jedną z szukanych przez siebie (i Stuxneta) magicznych wartości — 9500h. Według instrukcji był to identyfikator konwertera częstotliwości produkowanego przez pewną fińską firmę. Chien poszukał informacji

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

o drugim tajemniczym identyfikatorze, ale niczego nie znalazł. Dlatego napisał do firmy Profibus e-mail z prośbą o zidentyfikowanie urządzenia o identyfikatorze 7050h. Nie oczekiwał odpowiedzi i był zaskoczony, gdy firma poinformowała go, że jest to identyfikator konwertera częstotliwości produkowanego w Iranie.

Konwertery częstotliwości to zasilacze kontrolujące prąd przekazywany do silników i wirników w celu modulowania ich szybkości. Zwiększenie częstotliwości skutkuje przyspieszeniem pracy silnika. Identyfikator 9500h dotyczył konwertera częstotliwości produkowanego przez fińską firmę Vacon. Identyfikator 7050h oznaczał nieokreślony model wytwarzany przez irańską firmę Fararo Paya. O'Murchu podejrzewał, że konwertery firmy Fararo Paya były irańską kopią fińskich urządzeń[4]. Oznaczało to, że zapewne żaden zakład poza Iranem nie używał konwerterów tej firmy.

Badacze pobrali wszystkie znalezione informacje na temat konwerterów częstotliwości, w tym podręczniki użytkownika różnych modeli. Żaden z nich nie dotyczył urządzeń firm Vacon i Fararo Paya, jednak w niektórych dokumentach znajdowały się służące do sterowania konwerterami instrukcje, które były takie same dla sprzętu różnych marek. Jedno z poleceń w języku STL znalezione przez Falliere'a w kodzie Stuxneta brzmiało „47F i 1". Gdy badacze zajrzeli do jednego z podręczników, znaleźli następujące słowa: „Aby uruchomić konwerter częstotliwości, prześlij słowo 47F i ustaw wartość 1". O'Murchu zawiesił palce nad klawiaturą, gdy na głos czytał ten fragment. Nie mógł w to uwierzyć. Od czterech miesięcy starali się odkryć, co było celem Stuxneta. Pracowali wieczorami i w weekendy, aby zrozumieć, co jest grane. A teraz, wpisując kilka prostych zapytań w Google'u, znaleźli odpowiedź. Było to równie ekscytujące i satysfakcjonujące jak przygnębiające.

Zbliżał się koniec dnia i obaj badacze byli zmęczeni, dlatego wysłali do Falliere'a krótki e-mail z informacją o swoim odkryciu, a także kilka plików PDF z podręcznikami użytkownika i znalezionymi poleceniami. „Zajrzyj do nich i sprawdź, czy znajdziesz coś, co zadziała" — napisał Chien Falliere'owi.

[4] Ponieważ w 2006 r. Iran padł ofiarą sabotażu, gdy zakupił z Turcji rzekomo uszkodzone części (zob. s. 209), irańscy urzędnicy mogli uznać, że kraj musi samodzielnie wyprodukować konwertery częstotliwości, by uniknąć sabotażystów atakujących łańcuch dostaw i manipulujących przy urządzeniach zakupionych przez Iran za granicą.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy Falliere obudził się i zobaczył e-mail, szybko pojechał do biura. Wyszukał listę wszystkich danych konfiguracyjnych i instrukcji znalezionych w Stuxnecie, po czym zaczął porównywać je z informacjami z podręczników użytkownika. Szybko dopasował wszystkie instrukcje. Już wcześniej podejrzewał, że Stuxnet może zmieniać częstotliwość urządzeń kontrolowanych przez sterownik PLC. Kod zawierał liczby takie jak 10640. Badacz podejrzewał, że chodzi o 1064 Hz wyrażone w decyhercach. Nowe informacje to potwierdzały.

Falliere posłużył się podręcznikami użytkownika do przetłumaczenia wszystkich instrukcji ze Stuxneta. W ciągu godziny lub dwóch uzyskał kompletny schemat ataku, który przesłał do O'Murchu i Chiena.

Stuxnet przed rozpoczęciem ataku na sterowniki PLC S7-315 upewniał się, że w systemie działają konwertery częstotliwości firm Vacon lub Fararo Paya, a także że konwertery używają częstotliwości z przedziału od 807 do 1210 Hz. Robak szukał zakładu, w którym pracowało do 186 tych konwerterów i wszystkie używały częstotliwości powyżej 800 Hz. Takie konwertery są używane w wielu miejscach, jednak modele z częstotliwościami od 600 Hz wzwyż są stosowane rzadko — na tyle rzadko, że gdy Chien poszukiwał informacji w internecie, dowiedział się, że w Stanach Zjednoczonych eksport takich urządzeń jest regulowany przez Komisję ds. Energii Atomowej. Nie było wątpliwości, że celem Stuxneta był obiekt jądrowy. Langner zaryzykował stwierdzenie, że Stuxnet atakował irański program nuklearny. Teraz badacze znaleźli w kodzie potwierdzające to dowody.

Chien był zdumiony tym, jak pięknie wszystko do siebie pasowało.

Zespół miesiącami starał się odszyfrować kod, jednak postępy mierzył raczej w centymetrach niż kilometrach. Badacze martwili się, że nigdy nie dotrą do celu. Z perspektywy czasu cały proces wydał im się elegancki i kompletny. Po wyjaśnieniu ostatnich szczegółów Falliere przedstawił opis ataku od początku do końca.

Gdy Stuxnet znalazł maszynę z systemem Step 7, zastępował plik .DLL z tego systemu wypakowanym sobowtórem. Następnie cierpliwie czekał na uruchomienie programu Step 7 przez programistę, który chciał przejrzeć lub napisać bloki kodu dla sterownika PLC S7-315. Wtedy robak wstrzykiwał do bloków kodu szkodliwy kod i czekał, aż programista podłączy laptopa do sterownika lub skopiuje instrukcje na pendrive'a, aby przenieść je do sterownika. Dotarcie szkodliwych poleceń do sterownika

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PLC mogło zająć dni lub tygodnie, jednak od tego momentu atak rozwijał się bez przeszkód.

Po fazie rekonesansu, polegającej na rejestrowaniu przez 13 dni danych, Stuxnet najpierw zwiększał częstotliwość w konwerterach do 1410 Hz na 15 min, a następnie na ok. 26 dni zmniejszał ją do 1064 Hz (co prawdopodobnie było standardowym poziomem). Gdy Stuxnet przez te trzy tygodnie zarejestrował wszystkie potrzebne dane, na 50 min zdecydowanie obniżał częstotliwość, do 2 Hz, po czym ponownie przywracał poziom 1064 Hz. Po kolejnych 26 dniach atak był powtarzany. W trakcie każdej akcji sabotażowej atak typu *man in the middle* przekazywał fałszywe odczyty częstotliwości operatorom i systemowi bezpieczeństwa, przez co nikt nie wiedział, co się dzieje.

SYMANTEC OSTATECZNIE DOKŁADNIE ustalił, co Stuxnet robił ze sterownikami PLC S7-315. Jednak atak na sterowniki PLC S7-417 wciąż pozostawał tajemnicą. Obie cyfrowe bronie znajdowały się w jednym pocisku, jednak działały w pełni niezależnie od siebie. Model S7-417 był zaawansowanym sterownikiem PLC Siemensa z 30 MB pamięci RAM i ceną powyżej 10 tys. dolarów (w porównaniu z 500 dolarami za model S7-315). Jakby dostosowując się do wyższego poziomu urządzenia, także kod ataku na nie był dużo bardziej rozbudowany. Obejmował więcej bloków kodu (40 w porównaniu do 15 z ataku na model 315), a niektóre z nich były generowane „w locie" na podstawie warunków odkrytych przez Stuxneta w atakowanym systemie.

Atak na model 417 był też dużo bardziej złożony zarówno ze względu na wykonywane kroki, jak również na warunki, w jakich był przeprowadzany sabotaż. Ponadto w kodzie zostały użyte dziwaczne konstrukcje, przez co jego inżynieria odwrotna była bardzo kłopotliwa. Kod zawierał wskaźniki prowadzące do innych wskaźników, które prowadziły do jeszcze innych wskaźników, dlatego trudno było prześledzić sekwencję wydarzeń. Z powodu różnic w strukturze obu ataków można było podejrzewać, że został napisany przez dwa zupełnie inne zespoły posługujące się innymi narzędziami.

Napastnicy najwyraźniej włożyli dużo inwencji i wysiłku w kod atakujący model 417, dlatego Falliere był zaskoczony, gdy odkrył, że atak nie działał. Napastnicy celowo wyłączyli ten kod. We fragmencie odpowiedzialnym za sprawdzanie, czy konfiguracja sterownika PLC S7-417 pasuje

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

do ustawień szukanych przez Stuxneta, napastnicy umieścili wyjątek. Jest to technika programistyczna polegająca na celowym zgłaszaniu błędu w kodzie. Tu powodowało to zakończenie misji jeszcze przed jej rozpoczęciem. Co więcej, nic nie wskazywało na to, że atak kiedykolwiek był aktywny. Stuxnet musiał wygenerować „w locie" kluczowy blok kodu, aby atak zadziałał, jednak fragment generujący ten blok był niekompletny.

Nie było jasne, czy napastnicy wyłączyli ten kod, ponieważ wciąż trwały prace nad nim, czy został on wcześniej ukończony, jednak z nieznanych przyczyn później go zdezaktywowano. Falliere przypomniał sobie opublikowany niedawno artykuł, w którym irański urzędnik twierdził, że w Iranie znaleziono *pięć* wersji Stuxneta[5]. Symantec i inni badacze zetknęli się na razie z trzema wersjami. Czy jednak istniała inna wersja Stuxneta, zawierająca kompletny atak na model 417?

Na podstawie poszlak znalezionych przez Falliere'a i jego współpracowników w trzech wersjach Stuxneta wydawało się, że rzeczywiście może istnieć jeszcze jedna wersja. Numery trzech znanych wersji nie tworzyły sekwencji. Napastnicy kod z czerwca 2009 r. opatrzyli numerem 1.001, natomiast kod z marca i kwietnia 2010 r. numerami 1.100 i 1.101. Luki w numeracji wskazują na to, że przynajmniej opracowano też inne odmiany Stuxneta, w tym poprzedzającą zidentyfikowane warianty wersję 1.00, choć mogły one nie zostać wypuszczone.

Niezależnie od tego, co atakował kod dla modelu 417, jego cel był inny niż kodu dla modelu 315. Kod dla modelu 417 szukał systemu obejmującego 984 urządzenia w sześciu grupach po 164 sztuki. W trakcie tego ataku sabotaż dotyczył tylko 110 ze 164 urządzeń. Niestety, kod dla modelu 417 nie zawierał magicznych wartości (podobnych do tych, które pozwoliły dotrzeć do konwerterów częstotliwości), które pomogłyby zespołowi z Symanteca zidentyfikować cel. Langner i jego zespół analizowali ten kod równolegle z badaczami z Symanteca i podejrzewali, że celem jest sama kaskada, a nie pojedyncze wirówki. Sądzili, że mogło chodzić o rury i zawory sterujące przepływem gazu w ramach kaskady. Jednak bez dodatkowych szczegółów zapewniających ostateczny dowód ani Langner, ani zespół z Symanteca nie mogli z całkowitą pewnością stwierdzić, jak działał kod dla modelu 417. Po miesiącach pracy i licznych postępach w innych obszarach

[5] Zob. s. 191.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

badacze musieli zaakceptować fakt, że nic więcej nie zdołają osiągnąć. Wyglądało na to, że Stuxnet zachowa przynajmniej jedną ze swoich tajemnic.

Ponieważ badacze z Symanteca nie potrafili w pełni zrozumieć kodu ataku na model 417, zdecydowali się opublikować to, co *wiedzieli*, czyli ostateczny szczegółowy opis ataku na model 315.

Tak więc 12 listopada 2010 r., dokładnie cztery miesiące po pierwszym ogłoszeniu odkrycia kodu Stuxneta przez firmę VirusBlokAda, Symantec opublikował na blogu wpis z informacją, że Stuxnet atakował konkretne konwertery częstotliwości skonfigurowane w ściśle określony sposób. „To, że Stuxnet wymaga konkretnych napędów i określonego sposobu działania konwerterów częstotliwości, zawęża liczbę potencjalnych celów do ograniczonego zbioru możliwości" — pisał Chien w typowym dla zespołu Symanteca tajemniczym i ostrożnym stylu[6]. Chien nigdy nie napisał bezpośrednio o irańskim programie nuklearnym ani nawet o wirówkach, jednak przekaz płynący z jego słów był jasny.

Cztery dni po opublikowaniu wpisu przez Symantec technicy w Natanzie zatrzymali wszystkie aktywne wirówki w zakładzie. Na sześć dni, do 22 listopada, wstrzymane zostały wszelkie prace związane ze wzbogacaniem uranu. Irańscy urzędnicy nie wyjaśnili tego nagłego przerwania prac, jednak badacze z Symanteca podejrzewali, że administratorzy w zakładzie dokładnie sprawdzali komputery pod kątem kryjących się w nich pozostałości po Stuxnecie. Choć informacje o robaku były publicznie dostępne od miesięcy, do tego czasu nie ujawniono, jakie urządzenia były celem Stuxneta ani jak przebiegała operacja. Ponadto Stuxnet został starannie zaprojektowany w taki sposób, aby utrudnić znalezienie jego szkodliwego kodu w sterownikach PLC lub wyśledzenie źródła sabotażu. Jednak najnowszy raport Symanteca zawierał wszystkie dowody, jakich potrzebowali operatorzy, aby powiązać problemy w Natanzie z opisaną przez badaczy bronią cyfrową. Choć firmy antywirusowe już dawno udostępniły sygnatury do wykrywania plików Stuxneta, pozwalało to wykryć wyłącznie pliki w komputerach z systemem Windows, a nie szkodliwy kod wstrzyknięty przez Stuxneta do sterowników PLC. Ponieważ Stuxnet działał jak ośmiornica i miał wiele pomagających mu się rozprzestrzeniać macek, technicy w Natanzie musieli

[6] Eric Chien, „Stuxnet: A Breakthrough", blog Symanteca, 12 listopada 2010 (*https://www.symantec.com/connect/blogs/stuxnet-breakthrough*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wyczyścić i odtworzyć system w każdej maszynie w zakładzie, aby całkowicie usunąć uporczywy kod ze swojego środowiska.

Teraz było już jasne, że czas Stuxneta dobiegł końca. Nie tylko nie mógł on już zaszkodzić wirówkom w Natanzie, ale też wszelkie późniejsze problemy z systemami w zakładzie natychmiast wzbudziłyby podejrzenia, że ich przyczyną jest szkodliwy kod. W przyszłości znacznie trudniej byłoby przeprowadzić podobny ukryty atak i uniknąć szybkich analiz systemów kontroli.

Po rozwiązaniu prawie wszystkich zagadek Stuxneta badacze z Symanteca skupili się na dopracowaniu szczegółów i zakończeniu obszernej dokumentacji kodu, po czym planowali zająć się innymi sprawami.

Jednak tydzień po tym, jak zatrzymane wirówki w Natanzie wznowiły pracę, historia Stuxneta przyjęła bardziej złowrogi bieg. Wskazywało to na to, że twórcy robaka nie zaprzestali jeszcze wysiłków na rzecz wstrzymania programu wzbogacania uranu. Choć zastosowanie szkodliwego kodu nie było już możliwe, napastnicy wciąż mieli do dyspozycji inne środki.

RANKIEM 29 LISTOPADA 2010 r. w godzinach szczytu ruch na Artesh Boulevard w północnym Teheranie był wyjątkowo wzmożony. Majid Shahriari, szczupły 40-letni profesor fizyki nuklearnej manewrował swoim sedanem marki Peugeot w korku w drodze do pracy. Była dopiero 7:45 poniedziałkowego poranka, jednak warstwa smogu unosiła się już w powietrzu. Shahriari powoli dojeżdżał do Shahid Beheshti University, gdzie był wykładowcą. Razem z nim w samochodzie znajdowała się jego żona, także profesor fizyki nuklearnej, a ponadto matka dwójki dzieci, i ochroniarz.

Gdy sedan zbliżał się do ruchliwego skrzyżowania, do samochodu Shahriariego nagle podjechali napastnicy na motocyklu, którzy, nie kryjąc się, przyczepili do drzwi po stronie kierowcy bombę „samoprzylepną". Zaraz po tym, jak zamachowcy pospiesznie odjechali, bomba eksplodowała, rozbijając tylne okno samochodu i zmieniając drzwi kierowcy w bezkształtną masę stopionego metalu. Shahriari zginął na miejscu, jego żona i ochroniarz odnieśli obrażenia, ale przeżyli. Mała wyrwa w asfalcie obok samochodu była dowodem na siłę wybuchu[7].

[7] „Iranian Nuclear Scientist Killed in Motorbike Attack", BBC, 29 listopada 2010 (*http://www.bbc.com/news/world-middle-east-11860928*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Niewiele później w innej części miasta Fereydoon Abbasi, 52-letni ekspert od separacji izotopów atomowych, przebijał się przez korki na tę samą uczelnię, gdy kątem oka spostrzegł zbliżający się motocykl. Sekundę później usłyszał charakterystyczny dźwięk spowodowany przyczepieniem czegoś do drzwi. Abbasi był członkiem irańskiej gwardii rewolucyjnej, dlatego miał silniejszy instynkt samozachowawczy niż Shahriari. Szybko wyskoczył z samochodu i wyciągnął żonę z fotela. Choć oboje zostali ranni, przeżyli atak.

W serwisach informacyjnych podano, że obaj naukowcy zostali zaatakowani, ponieważ pełnili ważne funkcje w irańskim programie nuklearnym. „To źli ludzie — powiedział później anonimowy amerykański urzędnik — i wykonują pracę potrzebną do zbudowania bomby”[8].

Shahriari był ekspertem od transportu neutronów (dziedzina ta jest związana z generowaniem atomowych reakcji łańcuchowych w reaktorach i bombach), a zachodnie serwisy informacyjne podały, że w irańskim programie nuklearnym wyżej od niego stały tylko osoby mianowane z przyczyn politycznych. Szef tego programu, Ali Akbar Salehi, powiedział dziennikarzom, że Shahriari pracował nad „bardzo ważnym projektem” irańskiej Agencji Energii Atomowej, nie podał jednak szczegółów[9].

Abbasi był jeszcze ważniejszy dla programu nuklearnego. Był jednym z niewielu specjalistów w Iranie z wiedzą na temat separacji izotopów uranu, co jest podstawą procesu wzbogacania uranu. Znajdował się też na liście osób poddanych sankcjom przez Radę Bezpieczeństwa ONZ-etu, co wynikało z pełnionej przez Abbasiego funkcji starszego doradcy naukowego przy irańskim ministerstwie obrony i ze ścisłej współpracy z Mohsenem Fakhrizadehem-Mahabadim, oficerem irańskiej gwardii rewolucyjnej. Jeśli Iran rzeczywiście realizował program budowy broni atomowej, to uważano, że właśnie Fakhrizadeh-Mahabadi jest jego architektem.

Prezydent Ahmadineżad nie tracił czasu i oskarżył o atak „reżim syjonistyczny i rządy Zachodu”[10]. Saeed Jalili, sekretarz generalny irańskiej Najwyższej Rady Bezpieczeństwa Narodowego, nazwał ataki „aktem desperacji bezsilnych wrogów”[11].

---

[8] William Yong, Robert F. Worth, *Bombings Hit Atomic Experts in Iran Streets*, „New York Times”, 29 listopada 2010.

[9] *Ibid.*

[10] *Ibid.*

[11] Dieter Bednarz, Ronen Bergman, „Israel's Shadowy War on Iran: Mossad Zeros in on Tehran's Nuclear Program”, Spiegel Online, 17 stycznia 2011 (*http://www.spiegel.de/international/world/israel-s-shadowy-war-on-iran-mossad-zeros-in-on-tehran-s-nuclear-program-a-739883.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Gdy wróg nie widzi innych możliwości, ucieka się do terroru — powiedział. — Nie jest to oznaką siły, tylko słabości”[12]. Po dojściu do zdrowia Abbasi został mianowany szefem irańskiej Agencji Energii Atomowej, jakby w celu udowodnienia determinacji kraju w realizowaniu celów nuklearnych mimo intryg wrogów. Podobno trzymał w gabinecie zdjęcie Shahriariego, aby przypominało mu o tym nastawieniu[13].

Jednak dwa ataki na zatłoczonych ulicach w świetle dnia wywarły zamierzony efekt i były komunikatem dla wszystkich osób zaangażowanych w irański program nuklearny, że nikt nie jest bezpieczny i nikt nie znajduje się poza zasięgiem zamachowców. Podobno inni irańscy naukowcy na kilka dni po zamachach poszli na chorobowe, aby uniknąć losu współpracowników[14].

---

[12] *Iran's Chief Nuclear Negotiator: „We Have to Be Constantly on Guard”*, „Der Spiegel”, 18 stycznia 2011.

[13] Shahriari i Abbasi nie byli pierwszymi zaatakowanymi irańskimi naukowcami. W 2007 r. Ardeshir Hosseinpour, fizyk nuklearny pracujący w zakładzie przetwarzania uranu w Isfahanie, zginął w tajemniczych okolicznościach, choć jako przyczynę jego śmierci podano wypadek przemysłowy. Później, dziesięć miesięcy przed śmiercią Shahriariego, jego współpracownik, Masoud Alimohammadi, został zabity w ataku bombowym na samochód. Iran oskarżył Mosad o przeprowadzenie ataku na Alimohammadiego, jednak później pojawiły się wątpliwości, gdy w serwisach informacyjnych poinformowano, że ofiara nie była fizykiem nuklearnym, tylko teoretykiem pola kwantowego. W grudniu tego roku oskarżony o to zabójstwo został 26-letni kickbokser Majid Jamali Fashi, który potem opowiadał w irańskiej telewizji dziwaczne historie o tym, że został zrekrutowany i przeszkolony przez Mosad po wizycie w Turcji w 2007 r. Fashi stwierdził, że otrzymał za zabójstwo 30 tys. dolarów z góry, a po ataku miał dostać jeszcze 20 tys. Irańskie serwisy informacyjne doniosły, że w maju 2012 r. Fashi został stracony przez powieszenie. W wywiadzie z 2014 r. wdowa po Alimohammadim powiedziała, że jej mąż rzeczywiście pracował potajemnie nad irańskim programem nuklearnym. Zob. Scott Peterson, *Covert War Against Iran's Nuclear Scientists: A Widow Remembers*, „Christian Science Monitor”, 17 lipca 2014.

[14] Irański urzędnik w wywiadzie z 2014 r. opisał też inną strategię zastraszania. Mosad pewnego razu zamówił w irańskiej kwiaciarni wysyłkę bukietu do rodziny irańskiego inżyniera nuklearnego. Do bukietu dołączona była karteczka z wyrazami ubolewania z powodu śmierci inżyniera, który jednak był żywy i miał się dobrze. Irański urzędnik powiedział też, że Mosad nakręcił filmy z fikcyjnymi fragmentami irańskich serwisów informacyjnych, na których znalazły się zdjęcia rzekomo zamordowanych irańskich naukowców. Filmy te zostały wysłane jako ostrzeżenie do wciąż żyjących naukowców. Zob. „How West Infiltrated Iran's Nuclear Program, Ex-Top Nuclear Official Explains”, *Iran's View*, 28 marca 2014 (*http://www.iransview.com/west-infiltrated-irans-nuclear-program-ex-top-nuclear-official-explains/1451/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W odpowiedzi na oskarżenia Ahmadineżada Departament Stanu USA wystosował krótkie oświadczenie. „Mogę powiedzieć tylko tyle, że potępiamy akty terroryzmu niezależnie od tego, gdzie mają miejsce. Poza tym nie mamy żadnych informacji na temat tego zdarzenia" — powiedział rzecznik Philip J. Crowley[15]. Izrael odmówił odpowiedzi na oskarżenia, przynajmniej bezpośrednio. Ale w dniu ataków premier Izraela Beniamin Netanjahu poinformował o przejściu na emeryturę szefa Mosadu, Meira Dagana, po ośmiu latach służby na stanowisku dowódcy tej agencji szpiegowskiej. Moment wydania tego ogłoszenia mógł sugerować, że ataki na naukowców i wirówki w Natanzie były łabędzim śpiewem Dagana. Izraelczyk był znany z tego, że chętnie posługiwał się zabójstwami jako bronią polityczną[16]. Po jego mianowaniu w 2002 r. na szefa Mosadu ówczesny premier Ariel Szaron w prymitywny sposób pochwalił go za umiejętność oddzielania Arabów od ich głów.

W dniu zamachów na naukowców prezydent Ahmadineżad najwyraźniej powiązał te ataki ze Stuxnetem i wydał pierwszy oficjalny komunikat potwierdzający, że cyfrowa broń uderzyła w Natanz. Oskarżając Izrael i Zachód o zamachy bombowe, oskarżył ich też o atak z użyciem wirusa przeprowadzony na irański program nuklearny rok wcześniej. Wirus został umieszczony w oprogramowaniu „zainstalowanym w częściach elektronicznych" i uszkodził część irańskich wirówek. Prezydent zbagatelizował jednak skutki ataku i stwierdził, że robak spowodował problemy w tylko „ograniczonej liczbie wirówek", zanim pracownicy wykryli go i unieszkodliwili[17]. Choć Ahmadineżad nie podał nazwy robaka ani zakładu, w którym działały uszkodzone wirówki, dla wszystkich było oczywiste, że chodziło o Stuxneta i Natanz.

Gdy wiadomości o atakach na naukowców dotarły do Ralpha Langnera, bardzo go poruszyły. Niemiec zastanawiał się, czy ujawnienie szczegółów Stuxneta przez jego zespół nie popchnęło napastników do podjęcia bardziej drastycznych kroków. Dotarł do niego fakt, że praca nad Stuxnetem wciągnęła jego zespół w bardzo mroczną i krwawą dziedzinę.

---

[15] Yong, Worth, *Bombings Hit Atomic Experts in Iran Streets*.

[16] Dagan został podobno zwolniony przez premiera Netanjahu i ministra obrony Ehuda Baraka, ponieważ sprzeciwiał się nalotom na Iran.

[17] Yong, Worth, *Bombings Hit Atomic Experts in Iran Streets*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Badacze z Symanteca byli równie wstrząśnięci wiadomościami. W trakcie miesięcy pracy nad Stuxnetem czarny humor i paranoiczne myśli wisiały w powietrzu, co było efektem ubocznym niepewności dotyczącej tego, kto stoi za atakami i do czego jest gotów się posunąć. O'Murchu zaczął słyszeć dziwne kliknięcia w telefonie, przez co podejrzewał, że jest nagrywany. Pewnego piątkowego popołudnia, gdy wychodził z biura do domu, w rozmowie z Chienem i Falliere'em zażartował, że gdyby nie przeżył weekendu, chce, aby wiedzieli, że nie ma skłonności samobójczych. Natomiast Chien zaczął każdego poranka po wyjściu z domu rozglądać się po okolicy, aby sprawdzić, czy ktoś go nie obserwuje. Nigdy jednak nie wierzył, że grozi mu niebezpieczeństwo. W dniu, w którym rozniosły się informacje o zamachach na naukowców, Chien zażartował do O'Murchu, że gdyby motocyklista podjechał do jego samochodu, natychmiast by go przejechał. Ale gdy tego dnia jechał do domu i zatrzymał się przy pierwszych światłach, przeraził się, kiedy we wstecznym lusterku zobaczył podjeżdżającego do niego motocyklistę.

Żaden z badaczy nie sądził, że zamachowcy będą chcieli zaatakować ich za pracę nad Stuxnetem. Było jednak jasne, że Stuxnet zmienił środowisko łowców wirusów. Od tego czasu firmy takie jak Symantec musiały opracować nowy sposób określania ryzyka w związku z ujawnianymi informacjami.

W różnych momentach pracy nad Stuxnetem badacze rozmawiali czasem o tym, czy nie zatrzymać odkryć dla siebie lub nie ujawnić ich anonimowo. Ostatecznie ukryli niektóre szczegóły, np. tożsamość pięciu pierwszych ofiar Stuxneta, jednak zdecydowali się ujawnić całą sprawę. Uznali, że im więcej informacji przedstawią, tym łatwiej będzie wszystkim zabezpieczyć się przed Stuxnetem i atakami naśladowców. Doszli przy tym do wniosku, że jedną rzecz powinni zachować dla siebie. Była nią tożsamość napastników. W tej sprawie nie miało to jednak znaczenia, ponieważ badacze nigdy nie znaleźli oczywistych dowodów na to, kto stał za atakiem.

Zespół nigdy nie znalazł też niezaprzeczalnych dowodów na to, że celem Stuxneta był zakład w Natanzie. Choć informacje o konwerterach częstotliwości stanowiły ważny fragment układanki, badacze nie mieli dowodów na to, że określona konfiguracja szukana przez Stuxneta znajdowała się w Natanzie. To David Albright i jego współpracownicy z ISIS musieli zapewnić tę ostatnią porcję informacji.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

SYMANTEC OPUBLIKOWAŁ OSTATNI raport na temat konwerterów częstotliwości w połowie listopada. Dwa tygodnie później Albright połączył ze sobą wszystkie informacje. Było to pewnego grudniowego dnia, gdy uczestniczył w spotkaniu z pracownikami z ISIS i grupą ekspertów od wirówek, których zaprosił do biura w celu omówienia kwestii irańskiego programu nuklearnego. Grupa zaczęła zastanawiać się nad zagadką, która nurtowała ich od ponad roku.

ISIS w 2002 r. opublikowała zdjęcia satelitarne zakładu w Natanzie. Miało to wywrzeć na Iran presję, aby kraj pozwolił inspektorom ONZ-etu zbadać zakład wzbogacania uranu. Od tego czasu Albright i jego pracownicy śledzili postępy Irańczyków, czasem zdobywając informacje od źródeł rządowych, ale głównie znajdując je w publikowanych przez MAEA cokwartalnych raportach na temat przeprowadzonych inspekcji. Dla większości obserwatorów Iranu te raporty były jedyną okazją do przyjrzenia się temu, co dzieje się w Natanzie.

Przez 18 miesięcy Albright i jego zespół zastanawiali się nad znacznymi zmianami liczb w raportach. Co trzy miesiące inspektorzy podawali liczbę wirówek i kaskad zainstalowanych przez Irańczyków w Natanzie, a także liczbę wirówek wzbogacających w danym momencie gaz (inne stały w tym czasie puste). Kontrolerzy podawali też ilość gazu wprowadzonego przez irańskich techników do wirówek i ilość wyprodukowanego wzbogaconego gazu.

Przez dużą część lat 2007 i 2008 te liczby rosły w dość stabilnym tempie. Jednak od połowy do końca 2009 r. nastąpiły nagłe zmiany. Ilość wzbogaconego gazu znacznie spadła, a wirówki pracujące w 11 z 18 kaskad w jednej z hal w Natanzie zostały ostatecznie wyłączone. W raportach zabrakło informacji o przyczynie takiego stanu rzeczy, było jednak oczywiste, że wystąpiły jakieś problemy.

Albright i jego współpracownicy miesiącami głowili się nad tymi zmianami. Analizowali dane z różnych perspektyw. Myśleli, że problemy były spowodowane nieprawidłowo skonstruowanymi komponentami lub materiałami niskiej jakości albo że technicy błędnie zainstalowali rury i zawory w kaskadach, co doprowadziło do wycieku gazu. Żadne z wyjaśnień nie tłumaczyło jednak wszystkich zaobserwowanych w raportach zmian. W grudniu 2010 r. na spotkaniu z ekspertami zespół omawiał anomalie, gdy nagle ktoś wspomniał o Stuxnecie i nowym raporcie Symanteca dotyczącym konwerterów częstotliwości. Albright nie czytał tego raportu, wiedział

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

jednak, że Iran stosował konwertery Vacon, fińskiej firmy wymienionej przez Symantec, oraz że w przeszłości kupował tego typu urządzenia w Turcji i w Niemczech. Nigdy wcześniej nie słyszał jednak o konwerterach Fararo Paya. Była to ważna kwestia. Albright i jego współpracownicy uważnie monitorowali towary zamawiane i wytwarzane przez Iran, ale nie wiedzieli, że ten kraj sam produkował konwertery. Jeśli Iran rzeczywiście używał tych konwerterów w Natanzie, to napastnicy posiadali informacje o programie wzbogacania uranu, których nie mieli nawet najbardziej uważni obserwatorzy.

Po zakończeniu spotkania Albright wrócił do biurka i pobrał raport Symanteca, aby dokładnie się z nim zapoznać. Znalazł też raport, w którym Langner napisał o zdezaktywowanym kodzie ataku na model 417. Przez kilka następnych tygodni Albright analizował techniczne szczegóły ataków, a nawet skontaktował się z Chienem, aby uzyskać wyjaśnienia w kwestiach, których nie rozumiał. Gdy pewnego dnia rozmawiał z Chienem, zwrócił uwagę na coś, czego wcześniej nie dostrzegał. Stuxnet po zakończeniu każdej akcji sabotażowej ustawiał częstotliwość w konwerterach na wartość 1064 Hz. Ta liczba przykuła uwagę Albrighta. Badacz wiedział, że silniki wirówek miały określoną optymalną częstotliwość działania zależną od modelu i materiałów, z jakich było wykonane urządzenie. Optymalna częstotliwość dla wirówek IR-1 z Natanzu wynosiła 1064 Hz.

Co więcej, częstotliwość ta była bardzo specyficzną cechą tych wirówek. Żadne inne wirówki nie miały takiej nominalnej częstotliwości. Ponadto żaden inny kraj oprócz Iranu nie korzystał z tego modelu. Choć wirówki IR-1 były wzorowane na projekcie wirówek P-1, używanych przez Pakistan w początkowych latach programu wzbogacania uranu w tym państwie, później Pakistan zaczął stosować bardziej zaawansowane urządzenia, działające z inną częstotliwością.

Optymalna częstotliwość wirówek IR-1 nie była powszechnie znana. Albright znał ją, ponieważ dowiedział się o tym ze źródeł rządowych w 2008 r. Jednak choć optymalna częstotliwość wynosiła 1064 Hz, informator stwierdził, że Iran uruchamiał urządzenia z niższą częstotliwością (Albright i jego współpracownicy ustalili, że wynosi ona 1007 Hz), ponieważ przy wyższych wartościach często się psuły. Albright przez pewien czas zastanawiał się nad tymi rozbieżnościami. Albo twórcy Stuxneta nie wiedzieli, że Iran wprowadził tę zmianę, albo Irańczycy zmienili częstotliwość pracy wirówek już po napisaniu przez napastników kodu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nie był to jedyny szczegół, który przykuł uwagę Albrighta. Badacz zauważył też, że gdy Stuxnet przeprowadzał atak, zwiększał częstotliwość w konwerterach do 1410 Hz na 15 min. Była to prawie maksymalna częstotliwość, jaką wirniki w modelu IR-1 mogły znieść przed rozpadnięciem się z przeciążenia.

Następnie zapoznał się z podanymi przez Symantec i Langnera informacjami o ataku na model 417. Choć badacze mieli niepełne dane na temat tego ataku, wiedzieli, że był on wymierzony w urządzenia skonfigurowane w sześć grup po 164 sztuki. Albright wiedział, że kaskady w Natanzie liczyły po 164 wirówki. Wskazywało to na to, że atak na model 417 dotyczył sześciu kaskad złożonych z 984 wirówek.

Chien powiedział też Albrightowi, że w ataku na model 417 kod zamiast zmieniać częstotliwości (co robił w przypadku modelu 315), tylko włączał i wyłączał urządzenia. Albright i jego współpracownicy przejrzeli listę komponentów z zakładu wzbogacania uranu, które pasowały do tego scenariusza. Za jedyny sensowny cel uznali zawory.

Każda wirówka w Natanzie miała trzy zawory kontrolujące pobieranie i wysyłanie gazu, a także zawory pomocnicze sterujące przesyłem gazu do kaskady i poza nią oraz między rzędami wirówek w kaskadzie. Zespół Albrighta przeanalizował różne scenariusze, aby ustalić, co by się stało po otwarciu lub zamknięciu określonych zaworów na dłuższy czas w celu wyrządzenia szkód. W każdym scenariuszu doprowadziłoby to do uszkodzenia lub zniszczenia wirówek.

Dla Albrighta było oczywiste, że wreszcie znaleźli wytłumaczenie dla zaskakujących liczb z raportów MAEA. W oświadczeniach dla prasy Ahmadineżad utrzymywał, że szkody spowodowane wysłanym przez Zachód wirusem były niewielkie. Jednak zdaniem Albrighta liczby z raportów MAEA z okresu, w którym według Irańczyków zaatakował wirus, wskazywały na to, że w tym czasie uszkodzonych lub wymienionych zostało 1000 wirówek.

Albright opublikował artykuł ze swoimi przemyśleniami, który miał raz na zawsze rozwiązać zagadkę zakładu w Natanzie. Krótko potem w gazecie „New York Times" ukazał się tekst, który ujawniał największą tajemnicę Stuxneta — to, kto go stworzył i uruchomił. Wnioski z tego artykułu nikogo nie zaskoczyły. Gazeta donosiła, że Stuxnet był wspólną operacją Izraela i Stanów Zjednoczonych ze świadomym lub nieświadomym udziałem Niemców i Brytyjczyków[18].

[18] William J. Broad, John Markoff, David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, „New York Times", 15 stycznia 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Według autora artykułu, polegającego na anonimowych źródłach, robak został napisany przez amerykańskich i izraelskich programistów oraz przetestowany w izraelskim kompleksie Dimona na pustyni Negew. Było to miejsce, w którym w latach 60. Izrael realizował własny tajny program budowy broni atomowej. W ośrodku Dimona skonfigurowano stanowisko badawcze z kontrolerami Siemensa i wirówkami identyczne z systemem wirówek IR-1 w Natanzie, aby zbadać skuteczność robaka w niszczeniu atakowanych urządzeń. W testach istotne było też laboratorium amerykańskie. W 2004 r. Laboratorium Narodowe Oak Ridge w Tennessee pozyskało wirówki P-1, na których wzorowany był irański model IR-1. Pewną rolę mogli odegrać w tym Brytyjczycy, którzy byli partnerami w konsorcjum Urenco — twórcy pierwotnych planów wirówek. Po zakończeniu testów Amerykanie i Izraelczycy wspólnie brali udział w ataku na maszyny w Iranie.

Gary Samore, główny doradca prezydenta Obamy ds. broni masowego rażenia i kontroli zbrojeń, zapytany o rolę Stanów Zjednoczonych w powstaniu Stuxneta, uśmiechnął się do reportera „Timesa" i powiedział: „Cieszę się na wieść o ich problemach z wirówkami. Stany Zjednoczone razem z sojusznikami robią wszystko, co w ich mocy, aby utrudnić [Iranowi] pracę"[19].

Informacje o zaangażowaniu Stanów Zjednoczonych w tworzenie i stosowanie broni cyfrowej powinno wzbudzić zamieszanie w Waszyngtonie i kręgach rządowych. Lecz reakcją na wiadomości była cisza, choć wywołały one wiele niepokojących pytań, związanych nie tylko z zagrożeniem amerykańskiej infrastruktury krytycznej, podatnej na tego samego rodzaju ataki, ale też z etycznymi i prawnymi kwestiami stosowania niszczycielskich ataków cyfrowych, które w zasadzie były działaniami wojennymi. Ralph Langner miał rację, kończąc swój wpis na temat Stuxneta takimi, a nie innymi słowami. Potwierdzenie (choć nieoficjalne), że za atakiem stały Izrael i Stany Zjednoczone, oznaczało wkroczenie świata w erę cyberwojen.

[19] *Ibid.*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 14

SYN STUXNETA

Wraz z nadejściem wiosny 2011 r. historia Stuxneta zaczęła tracić na popularności. Symantec rozwiązał tajemnicę urządzeń będących celem tej cyfrowej broni, Albright ostatecznie powiązał Stuxneta z wirówkami z Natanzie, a choć rząd Stanów Zjednoczonych wciąż nie wziął formalnie odpowiedzialności za atak, „New York Times" potwierdził to, co wszyscy podejrzewali — że za operacją stały Stany Zjednoczone i Izrael.

Badacze z Symanteca byli gotowi zająć się innymi zadaniami. Poświęcili pół roku na analizę kodu i przygotowali 72-stronicowy raport ze swoimi odkryciami. Poczuli ulgę, że wreszcie zakończyli tę sprawę. Ledwie jednak odłożyli ten projekt na bok, w Europie pojawiły się nowe, zaskakujące dowody. Wskazywały one na to, że Stuxnet był tylko jednym z wielu narzędzi w arsenale, jaki napastnicy zastosowali przeciw Iranowi i innym celom.

BOLDIZSÁR BENCSÁTH UGRYZŁ kanapkę i zapatrzył się w ekran komputera. Pobieranie oprogramowania, które próbował zainstalować na maszynie, trwało wieki, a Bencsáth miał jeszcze mnóstwo rzeczy do zrobienia przed rozpoczęciem jesiennego semestru 2011 r. na Budapeszteńskim Uniwersytecie Techniczno-Ekonomicznym, gdzie wykładał nauki komputerowe. Mimo długiej listy zadań do wykonania był zadowolony i zrelaksowany. Był pierwszy dzień września, jedno z tych doskonałych popołudni późnego lata, kiedy ciepłe powietrze i czyste niebo pozwalają zapomnieć o zimnej jesiennej pogodzie, która czai się za rogiem.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bencsáth, przez przyjaciół nazywany Boldim, siedział przy swoim biurku w Laboratorium Kryptografii i Bezpieczeństwa Systemów (ang. *Laboratory of Cryptography and System Security* — CrySyS), gdy telefon przerwał mu lunch. Dzwonił Jóska Bartos, CEO firmy, dla której laboratorium świadczyło czasami usługi z zakresu konsultingu[1].

„Boldi, miałbyś czas zrobić coś dla nas?" — zapytał Bartos.

„Chodzi o tę sprawę, o której wcześniej rozmawialiśmy?" — Bencsáth nawiązał do poprzedniej rozmowy o testowaniu nowych usług, jakie firma zamierzała zaoferować klientom.

„Nie, to coś innego — odpowiedział Bartos. — Mógłbyś do nas podejść? To ważne. Tylko nie mów nikomu, gdzie idziesz".

Bencsáth szybko pochłonął resztę lunchu i powiedział współpracownikom w laboratorium, że zdarzył się „czerwony alarm" i że musi iść. „Nawet nie pytajcie" — zawołał, wybiegając przez drzwi.

Niedługo potem był w biurze Bartosa, gdzie zebrał się już zespół oceny sytuacji odpowiedzialny za analizę problemu, o którym chcieli pomówić z Bencsáthem. „Uważamy, że zaatakowali nas hakerzy" — powiedział Bartos.

Zespół oceny sytuacji na komputerze programisty znalazł podejrzany plik utworzony późno w nocy, gdy nikt nie pracował. Plik był zaszyfrowany i skompresowany, dlatego nikt nie wiedział, co znajdowało się w środku. Zespół podejrzewał jednak, że były to dane, które napastnicy skopiowali z maszyny i zamierzali później pobrać. W firmowej sieci znalezionych zostało więcej zainfekowanych maszyn. Zespół był przekonany, że pliki służyły do ataku, i potrzebował pomocy Bencsátha w ustaleniu, jak intruzi się włamali i czego szukali. Firma korzystała z odpowiednich zabezpieczeń: zapory, programu antywirusowego, systemów wykrywania włamań i zapobiegania im. Mimo to napastnicy zdołali się przez nie przedostać.

Bencsáth był wykładowcą, a nie łowcą złośliwego oprogramowania, i nigdy wcześniej nie przeprowadzał podobnych analiz. W laboratorium CrySyS, gdzie był jednym z czterech doradców pracujących z grupką doktorantów, prowadził badania naukowe dla Unii Europejskiej i niekiedy udzielał konsultacji innym klientom. To ostatnie zadanie polegało jednak

[1] Jóska Bartos to pseudonim. Firma prosiła Bencsátha, aby nie ujawniał jej nazwy ani tożsamości pracujących dla niej osób. Opis wydarzeń pochodzi z wywiadu przeprowadzonego z Bencsáthem, chyba że jest napisane inaczej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

głównie na standardowym czyszczeniu systemów — porządkowaniu i przywracaniu systemów po infekcjach przypadkowymi wirusami. Bencsáth nigdy wcześniej nie badał celowego włamania, a tym bardziej w czasie, gdy akcja wciąż trwała, i był podekscytowany taką możliwością. Jedyny kruczek polegał na tym, że wykładowca nie mógł nikomu powiedzieć, czym się zajmuje. Firma Bartosa potrzebowała zaufania klientów. Gdyby się rozniosło, że nastąpiło włamanie, firma mogłaby stracić odbiorców.

Zespół oceny sytuacji wykonał kopie lustrzane zainfekowanych dysków twardych, po czym razem z Bencsáthem spędził resztę popołudnia, szukając na dyskach czegoś podejrzanego. Pod koniec dnia znaleźli to, czego szukali — keylogger (rejestrator wciśniętych klawiszy) i program do wykradania informacji. Narzędzia te rejestrowały hasła i inne słowa wpisane na zainfekowanych maszynach, a także wykradały dokumenty i robiły zrzuty ekranu. Spisywały też wszystkie urządzenia i systemy podłączone do komputerów, dzięki czemu napastnicy mogli ustalić schemat architektury sieci firmy. Zainstalowane złośliwe oprogramowanie nie przesyłało wykradzionych danych natychmiast, tylko zapisywało je w plikach tymczasowych, takich, jakie znalazł zespół oceny sytuacji. Te pliki stawały się większe za każdym razem, gdy program do wykradania informacji pobierał nowe dane. W pewnym momencie napastnicy mieli połączyć się z maszyną ze zlokalizowanego w Indiach serwera C&C, aby pobrać plik[2].

Zbliżał się koniec dnia, więc Bencsáth wziął ze sobą kopie lustrzane dysków i logi systemowe firmy (po usunięciu z nich poufnych danych klientów). Przez kilka kolejnych dni szukał w nich dalszych szkodliwych

[2] Badacze sprawdzili keylogger w serwisie VirusTotal, bezpłatnym internetowym narzędziu antywirusowym, stosowanym do analizowania szkodliwych plików w celu ustalenia, czy nie są one znanym złośliwym oprogramowaniem. VirusTotal do wykrywania szkodliwych plików stosuje ok. 40 silników antywirusowych różnych firm. Dwa skanery oznaczyły plik jako podejrzany, jednak nie było jasne, czy jest on znanym keyloggerem, czy nowym zagrożeniem. Tymi skanerami były BitDefender i AVIRA. Plik został wskazany też przez skanery F-Secure i G-DATA, ale tylko dlatego, że w obu używany jest silnik z BitDefendera. VirusTotal jest czasem używany przez napastników do testowania złośliwego oprogramowania przed jego zastosowaniem, ponieważ w ten sposób można się upewnić, że silniki antywirusowe nie wykryją ataku. Jednak wskazanie keyloggera przez dwa silniki mogło oznaczać, że napastnicy albo nie przetestowali ataku z użyciem tych skanerów, albo nie oczekiwali, że ich ofiary będą się nimi posługiwać.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

plików, unikając rozmów ze współpracownikami z biura na temat tego, czym się zajmuje. Zespół oceny sytuacji pracował równolegle z nim. Po kilku dniach badacze znaleźli trzy nowe podejrzane pliki, w tym sterownik działający w trybie jądra i inny sterownik, występujący tylko w niektórych zainfekowanych systemach.

Gdy Bencsáth zbadał sterownik z jądra, serce zaczęło mu szybciej bić. Plik był podpisany poprawnym certyfikatem cyfrowym tajwańskiej firmy. „Chwileczkę" — pomyślał. Stuxnet używał sterownika podpisanego certyfikatem firmy z Tajwanu. Była to firma RealTek Semiconductor, natomiast ten certyfikat należał do innej firmy, C-Media Electronics. Sterownik podpisano w sierpniu 2009 r., mniej więcej w tym samym czasie, kiedy Stuxnet został zastosowany w komputerach w Iranie.

Bencsáth zastanawiał się, czy oba ataki były ze sobą powiązane. Rozważał tę myśl przez chwilę, a potem uznał, że to niemożliwe. Stwierdził, że każdy mógł wykraść klucz i certyfikat firmy C-Media; nie musieli to być napastnicy stojący za Stuxnetem.

Później członek zespołu oceny sytuacji zauważył jeszcze coś znajomego w znalezionym sterowniku. Chodziło o sposób wstrzykiwania kodu do określonego procesu w zainfekowanej maszynie. „Znam tylko jednego robaka, który tak działa" — powiedział Bencsáthowi. Nie musiał podawać jego nazwy. Bencsáth wiedział, że chodzi o Stuxneta. Szybko jednak odrzucił także to podobieństwo, ponieważ miał pewność, że zastosowana technika była używana nie tylko w Stuxnecie.

W ciągu następnych dni Bencsáth i zespół oceny sytuacji jeszcze dwukrotnie natrafili na rozwiązania przypominające Stuxneta. Jednak w obu przypadkach przekonywali samych siebie, że to tylko zbieg okoliczności. Zakładali, że żaden piorun nie uderza dwa razy. Ponadto nic nie wskazywało na to, że celem nowego ataku są sterowniki PLC.

Po tygodniu pracy nad tym projektem Bencsáth zaczął się zastanawiać, czy inne firmy też zostały zainfekowane znalezionymi plikami. Zdecydował się sprawdzić, czy uda mu się wywabić inne ofiary — lub samych napastników — za pomocą przebiegłego testu. Ósmego września w swojej prywatnej witrynie, *http://boldi.phishing.hu/*, zamieścił skróty szkodliwych plików wraz z tajemniczym opisem: „Szukam przyjaciół [lub] wrogów 9749d38ae9b9ddd8ab50aad679ee87ec, aby porozmawiać na ten temat. Wiecie, co mam na myśli. Wiecie, dlaczego". Witryna badacza była dziwnym

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

kompendium przepisów na dania rybne i recenzji ryb z puszki (nazwa domeny, phishing, to gra słowna wykorzystująca określenie szkodliwych e-maili i podobnie wymawiane angielskie słowo *fishing* oznaczające łowienie ryb). Dlatego doskonale nadawała się na przykrywkę do umieszczania zagadkowych wiadomości, ponieważ jedynym sposobem, aby znaleźć opublikowane skróty, było wyszukanie ich w Google'u. Mogła to zrobić inna ofiara, która znalazła na swoim komputerze te same pliki i poszukiwała w internecie informacji na ten temat. Mogli to zrobić także napastnicy, chcący sprawdzić, czy któraś z ofiar znalazła pliki i pisze coś o nich w sieci. Bencsáth mógł sprawdzić adresy IP osób, które odwiedzały jego witrynę w poszukiwaniu zamieszczonych skrótów.

Niestety, nikt nie złapał się na tę przynętę, dlatego po kilku dniach Bencsáth usunął skróty.

W tym czasie rozpoczął się już semestr jesienny i Bencsáth był zajęty innymi sprawami. Musiał wykładać na zajęciach i prowadzić dyżury dla studentów. Miał też przygotować pracę naukową na konferencję w Dubrowniku. Nie mógł jednak przestać myśleć o badanym ataku. Gdy po konferencji wrócił do Budapesztu, razem z zespołem oceny sytuacji zdecydował się porównać kod jednego ze sterowników znalezionych w komputerach firmy ze sterownikiem używanym w Stuxnecie. Badacze chcieli w ten sposób raz na zawsze ustalić, że oba ataki nie są ze sobą powiązane. Ale gdy umieścili kody obu ataków w edytorze heksadecymalnym, by zbadać je jeden obok drugiego, czekała ich duża niespodzianka. Jedyną różnicą okazały się certyfikaty cyfrowe użyte do podpisania plików.

Bencsáth natychmiast zadzwonił do Bartosa, CEO firmy, i poinformował go, że musi włączyć w analizy innych członków laboratorium CrySyS. Nie chodziło już o proste włamanie. Wyglądało na to, że mógł to być atak na skalę państwową ze skutkami dla bezpieczeństwa narodowego. Bartos zgodził się, ale postawił warunek, że Bencsáth ma nie ujawniać swoim współpracownikom nazwy firmy. Jedynymi oprócz Bencsátha ludźmi, którzy wiedzieli o włamaniu, był lokalny rządowy Informatyczny Zespół Reagowania Kryzysowego (ang. *Computer Emergency Response Team* — CERT), powiadomiony tylko z powodu charakteru działalności zaatakowanej firmy[3].

[3] Charakter działalności firmy nie został ujawniony przez Bencsátha ani przez jego laboratorium. Opisują go inne źródła mające informacje na temat włamania i ofiary.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bencsáth zamierzał opowiedzieć współpracownikom o sprawie w następny poniedziałek. W weekend zebrał całą literaturę techniczną na temat Stuxneta, jaką udało mu się znaleźć (w tym długi raport przygotowany przez Symantec), i ponownie ją przeczytał, aby odświeżyć sobie pamięć. Gdy dotarł do fragmentu z omówieniem procedur szyfrowania stosowanych w Stuxnecie do ukrycia jego kodu, sprawdził takie procedury w nowym ataku i czekała go następna niespodzianka — użyte techniki były prawie identyczne. W nowym ataku napastnicy zastosowali nawet jeden z kluczy deszyfrujących używanych w Stuxnecie[4].

Następnie zbadał sześć użytych w nowym kodzie hooków jądra (są to określone funkcje komputera, które złośliwe oprogramowanie przejmuje, aby przeprowadzić atak), aby porównać je z podobnymi funkcjami z innych znanych ataków. W niektórych atakach stosowane były dwie lub trzy te same funkcje, jednak w żadnym nie posłużono się wszystkimi sześcioma. Później Bencsáth poszukał w literaturze poświęconej Stuxnetowi przejmowanych funkcji. Okazało się, że nowa cyfrowa broń przejmowała sześć tych samych funkcji. Badacz nie miał już wątpliwości, że ataki są ze sobą powiązane.

Nie oznaczało to, że kod został napisany przez tych samych ludzi. Było jednak jasne, że autorzy nowego kodu opracowali swój atak na podstawie kodu źródłowego i schematu zastosowanego w Stuxnecie. Stuxnet służył do sabotażu irańskiego programu wzbogacania uranu. Jaki jednak był cel nowego ataku i ile systemów zostało zainfekowanych?

Bencsáth od razu napisał do Bartosa e-mail, w którym omówił swoje odkrycia. Do tej chwili badacz pracował niespiesznie, analizując kod w wolnych chwilach. Teraz jednak zrozumiał, że musi szybko ustalić cel ataku i upublicznić te informacje, zanim ktoś zdąży mu w tym przeszkodzić. Po ujawnieniu przez Symantec raportu na temat Stuxneta część osób zastanawiała się, dlaczego rząd amerykański nie próbował temu zapobiec. Bencsáth obawiał się, że tym razem ktoś może spróbować zainterweniować.

[4] W nowym ataku pojawiła się też wartość zastosowana w Stuxnecie jako „szczepionka", 0x19790509 (zinterpretowana przez badaczy z Symanteca jako data — 9 maja 1979 r.). W Stuxnecie miała ona zapobiegać infekowaniu maszyn, w których wartość ta była zapisana w rejestrze. Tu była używana w ramach szyfrowania.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Następnego dnia powiedział o ataku swoim współpracownikom: Lavantemu Buttyánowi i Gáborowi Pékowi. Ta trójka wiedziała, że nie ma wiedzy potrzebnej do tego, by samodzielnie dokładnie zbadać znalezione pliki. Żaden z nich nie przeprowadzał wcześniej tego rodzaju analiz. Badacze mieli też niewielkie doświadczenie w posługiwaniu się narzędziami do debugowania potrzebnymi w inżynierii odwrotnej. Wiedzieli jednak, że muszą zbadać kod na tyle, by przekonać do zajęcia się nim innych, bardziej doświadczonych badaczy. Laboratorium CrySyS (podobnie jak firma VirusBlokAda) nie było powszechnie znane w branży zabezpieczeń komputerów. Dlatego jego pracownicy potrzebowali solidnych dowodów, aby powiązać atak ze Stuxnetem. Wiedzieli, że w przeciwnym razie nikt się nim nie zainteresuje.

Badacze przeznaczyli na badania dziesięć dni. W tym czasie zdecydowali się skupić tylko na tych aspektach ataku, które były podobne do Stuxneta. Ku zaskoczeniu badaczy podobieństw było niespodziewanie dużo. Po dziesięciu dniach grupa przygotowała 60-stronicowy raport. Bartos zgodził się, by Bencsáth udostępnił dokument Symantecowi. Postawił jednak warunek, że jeśli raport zostanie upubliczniony, nie pojawi się w nim nazwa laboratorium CrySyS. Bartos obawiał się, że gdy ktokolwiek się dowie, że laboratorium działa na Węgrzech, szybko zidentyfikuje ofiarę.

Badacze przesłali raport do rządowej agencji CERT, do Chiena i jego zespołu z Symanteca i do kilku innych osób: Pétera Szőra, węgierskiego analityka z firmy McAfee, do organizacji VeriSign, ponieważ powinna ona wycofać certyfikat cyfrowy używany przez złośliwe oprogramowanie, a także do pracownika Microsoftu[5]. Serce Bencsátha waliło, gdy badacz kliknął przycisk *Wyślij* w celu przesłania raportu. „Byłem bardzo podekscytowany — powiedział. — Zrzuciłem coś z góry i nie wiedziałem, jakiego rodzaju lawina powstanie [z tego powodu]".

[5] Ten pracownik, Tareq Saade, znalazł się na liście, ponieważ rządowa agencja CERT przesłała już do Microsoftu kopię keyloggera po jego wykryciu. Dlatego Bencsáth uznał, że także Microsoft powinien zapoznać się z raportem laboratorium CrySyS.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

GDY CHIEN OBUDZIŁ się w piątek 14 października, natychmiast sięgnął po telefon, aby sprawdzić pocztę. Jego uwagę przykuł temat jednej z wiadomości: „ważne złośliwe oprogramowanie". E-mail przyszedł z załącznikiem, a wysłany został przez dwóch informatyków z nieznanego laboratorium uniwersyteckiego na Węgrzech, którzy łamanym angielskim napisali, że wykryli nowy atak o widocznych „silnych podobieństwach" do Stuxneta. Nazwali go Duqu, ponieważ pliki tymczasowe generowane przez złośliwe oprogramowanie na zainfekowanych maszynach miały nazwy rozpoczynające się od członu *~DQ*. Badacze byli pewni, że ten atak „otworzy nowy rozdział w historii Stuxneta".

„Ponieważ jeszcze [*sic*] nie mamy doświadczenia w radzeniu sobie z tego rodzaju incydentami, nie jesteśmy pewni, jakie dalsze kroki powinniśmy podjąć — napisali. — Jesteśmy gotowi współpracować z innymi jednostkami, w tym z waszą, zapewniając dostęp do złośliwego oprogramowania i uczestnicząc w dalszych analizach".

Chien przesłał e-mail do pozostałych członków zespołu reagowania na incydenty w Symantecu. Wysłał też wiadomość tekstową do O'Murchu z prośbą, aby jak najszybciej przeczytał e-mail. Potem, z poczuciem ostrożnej ekscytacji, ruszył do biura.

W ciągu ostatniego roku Chien nauczył się z dystansem traktować osoby kontaktujące się z nim w sprawie rzekomych nowych przypadków napotkania Stuxneta. Ponieważ pracował dla firmy antywirusowej, był przyzwyczajony do tego, że znajomi i sąsiedzi korzystali z jego wiedzy, gdy uważali, że ich komputery zostały zainfekowane. Jednak gdy praca jego zespołu nad Stuxnetem została powszechnie upubliczniona, zaczęły się z nim kontaktować przypadkowe, nieznane mu osoby, utrzymujące, że rząd szpieguje je z użyciem Stuxneta. Jeden człowiek przesłał nawet kopertę z 50 stronami wydrukowanych zrzutów i plików dziennika z zakreślonymi na żółto fragmentami. Na jednej ze stron człowiek ten zakreślił adres URL odwiedzonej witryny, obejmujący fragmenty „en/us". Zdaniem tej osoby był to dowód na to, że rząd amerykański obserwuje jego komputer[6]. Inna osoba, autorka książek kucharskich, przesłała Chienowi kilka e-maili za pośrednictwem serwisu Hushmail (pozwala on wysyłać anonimowo szyfrowane

[6] Fragmenty „en/us" w adresie URL świadczą tylko o tym, że użytkownik odwiedził witrynę dostosowaną do anglojęzycznych czytelników ze Stanów Zjednoczonych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wiadomości i jest używany przez aktywistów oraz przestępców do ukrywania swojej tożsamości). Gdy zignorował te e-maile, kobieta znalazła jego numer telefonu i nagrała wiadomość. Także ta osoba była przekonana, że ktoś szpieguje ją za pomocą Stuxneta. Uważała tak, ponieważ za każdym razem, gdy w trakcie wizyty w bibliotece wkładała pendrive'a do komputera tej instytucji, jej domowy komputer był infekowany przez wirusa z tego właśnie pendrive'a.

Mimo zdystansowanego stosunku Chiena do wszystkich nowych informacji o Stuxnecie, które trafiały na jego biurko, badaczowi wystarczyło zapoznać się z dwiema pierwszymi stronami raportu z Węgier, aby stwierdził, że tym razem sytuacja wygląda inaczej. „To Stuxnet" — powiedział z przekonaniem.

Mimo braku doświadczenia w analizowaniu szkodliwego kodu Węgrzy przygotowali świetny raport, choć przepraszali, że „wiele pytań i kwestii pozostało bez odpowiedzi lub nierozwiązanych". Dołączyli też fragmenty zdekompilowanego kodu ilustrującego podobieństwo Duqu do Stuxneta oraz opracowali listę z kilkunastoma punktami, w których oba ataki były identyczne lub zbliżone do siebie. Nowy kod nie obejmował ataku na sterowniki PLC. Co więcej, w ogóle nie zawierał ładunku, chyba że uznać za niego keylogger. Jednak wszędzie w kodzie widoczne były „odciski palców" autorów Stuxneta. Duqu albo został napisany przez zespół, który stworzył Stuxneta, albo przynajmniej przez osoby mające dostęp do tego samego kodu źródłowego i tych samych narzędzi.

Chien wysłał do Bencsátha e-mail z informacją o otrzymaniu raportu, a następnie czekał niecierpliwie na przybycie O'Murchu. Odczuwał mieszane emocje. Jego zespół od dawna miał nadzieję, że ktoś odkryje dodatkowe wskazówki, które pomogą rozwiązać ostatnie kwestie dotyczące Stuxneta. Wyglądało na to, że Duqu może pomóc w uzyskaniu szukanych odpowiedzi. Jednak analizy Stuxneta zajęły miesiące pracy — także wieczorami i w weekendy. Dlatego Chien obawiał się, że nowy kod może wymagać podobnej ilości czasu i energii.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

O'MURCHU WCIĄŻ BYŁ pogrążony w półśnie, gdy przeczytał wiadomość tekstową od Chiena. Ale gdy otworzył załącznik i przejrzał raport, szybko oprzytomniał. Spojrzenie w lufę potencjalnej cyberbroni okazało się świetnym sposobem na rozjaśnienie umysłu. „Muszę lecieć do biura" — powiedział swojej dziewczynie, narzucając na siebie ubranie i wybiegając przez drzwi.

W drodze do pracy próbował poukładać sobie w głowie to, co właśnie zobaczył. Nie mógł uwierzyć, że gang odpowiedzialny za Stuxneta wciąż jest aktywny. Był przekonany, że po nagłośnieniu operacji przez media i wskazaniu jako winnych Izraela i Stanów Zjednoczonych napastnicy przez pewien czas nie będą się wychylać, aby pozwolić sprawie przycichnąć. Sądził, że przynajmniej zmienią metody i kod, by mieć pewność, że późniejsze ataki — jeśli zostaną wykryte — nie zostaną z nimi powiązane. Jednak z raportu Węgrów wynikało, że napastnicy nie próbowali nawet zmienić specyficznych dla siebie technik. Uznał, że „mają jaja". Byli zdeterminowani, aby zrobić, co mieli do zrobienia, i nie obchodziło ich, kto się dowie, że to oni stoją za atakiem. Inną możliwością było to, że napastnicy tak dużo zainwestowali w kod Duqu, iż nie chcieli z niego rezygnować nawet mimo wykrycia Stuxneta.

Gdy O'Murchu dotarł do biura, Chien i jego współpracownicy rozmawiali już o nowym ataku. Skontaktowali się z Falliere'em, który został przeniesiony z Paryża do Stanów i obecnie pracował w biurze Symanteca w północnej Kalifornii. Badacze pobrali przesłane przez Węgrów pliki binarne z kodem Duqu i pracowali nad nimi przez resztę dnia oraz weekend. Z radością odkryli, że kod Duqu jest znacznie krótszy niż kod Stuxneta i składa się z tylko kilku plików, których odszyfrowanie okazało się stosunkowo proste. Do poniedziałku zespół wiedział prawie wszystko o nowym kodzie.

Duqu był koniem trojańskim ze zdalnym dostępem (ang. *Remote Access Trojan* — RAT), działającym jako prosta tylna furtka zapewniająca napastnikom trwały punkt oparcia w zainfekowanych maszynach. Po zainstalowaniu tylnej furtki Duqu kontaktował się z serwerem C&C, z którego napastnicy mogli pobrać dodatkowe moduły, aby rozbudować atak — np. o keylogger lub narzędzie do wykradania informacji znalezione przez Węgrów w ich systemach.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jeśli chodzi o przeznaczenie Duqu, było oczywiste, że kod (w odróżnieniu od Stuxneta) nie służy do sabotażu, tylko jest narzędziem szpiegowskim. Stuxnet był używany w tajnej operacji nastawionej na zniszczenie celu, natomiast Duqu wydawał się zwiadowcą wysłanym w celu zebrania informacji na potrzeby późniejszych ataków. Badacze z Symanteca podejrzewali, że to wstęp do innego ataku podobnego do Stuxneta. Czas życia Duqu był ograniczony. Data zakończenia operacji w kodzie sprawiała, że kod usuwał sam siebie po 36 dniach, kasując wszystkie ślady swojego istnienia z zainfekowanej maszyny[7].

Wszystko to wydawało się proste, jednak gdy badacze przyjrzeli się plikom Duqu, odkryli niespodziankę łączącą ten atak z inną tajemniczą operacją, która zastanawiała ich od jakiegoś czasu. Sześć miesięcy wcześniej urzędnicy irańscy poinformowali, że komputery zostały dotknięte przez drugi atak cyfrowy podobny do Stuxneta. Komunikat w tej sprawie został wydany kilka miesięcy po tym, jak Irańczycy ostatecznie przyznali, że ich komputery sterujące wirówkami zostały zaatakowane. Choć nigdy nie podali nazwy wirusa, który zaatakował wirówki, nowemu atakowi nadali nazwę Stars. Gholam Reza Jalali, dowódca irańskiej Obrony Cywilnej, nie wyjaśnił, skąd wzięła się ta nazwa. Nie przedstawił też szczegółowych informacji o ataku. Powiedział tylko, że miał on na celu kradzież danych. Powiedział też, że zapewne „został błędnie wzięty [w komputerach] za rządowe pliki wykonywalne". Wyglądało na to, że złośliwe oprogramowanie zostało pobrane w ramach phishingu, a szkodliwy plik znajdował się w załączniku udającym dokument od źródeł rządowych[8].

Symantec i inni badacze z branży zabezpieczeń nie wiedzieli wówczas, jak potraktować ten raport, ponieważ Irańczycy nie udostępnili osobom z zewnątrz próbek złośliwego oprogramowania do przeanalizowania. To, że nigdzie indziej na świecie nie zgłaszano infekcji wirusem Stars, spowodowało, że niektórzy badacze podważali prawdziwość raportu.

---

[7] Później badacze znaleźli kilka wersji Duqu, każdą o innym czasie usuwania plików. Niektóre odmiany kasowały pliki po 30 dniach, inne po 36. Przynajmniej jedna ze znalezionych wersji działała przez 120 dni do czasu usunięcia.

[8] Dugald McConnel, „Iranian Official: New Computer Worm Discovered", CNN, 27 kwietnia 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Uważali, że Iran albo sfabrykował całą historię, by oskarżyć Zachód o kolejne cyberataki, albo pomylił zwykłego wirusa z atakiem sponsorowanym przez inne państwa.

Jednak pewne aspekty Duqu pozwalały podejrzewać, że właśnie on jest wirusem Stars. Gdy autorzy Duqu przesłali na zainfekowane maszyny keylogger, umieścili go w pliku .JPEG (czyli w zwykłym pliku graficznym), aby mógł niezauważony przejść przez zaporę. Zawartość większości grafiki z pliku została usunięta, dzięki czemu można było umieścić w pliku kod keyloggera. Dlatego gdy O'Murchu otworzył plik, zobaczył na ekranie tylko kilka centymetrów rysunku. Widoczny fragment przedstawiał biały tekst na ciemnym tle. Słowa były przycięte i widoczna pozostała tylko ich górna część, ale można było odczytać tekst: „Interacting Galaxy System NGC 6745". Po wpisaniu tych słów w wyszukiwarce Google udało się odnaleźć cały rysunek. Było to zdjęcie wykonane przez teleskop Hubble'a w marcu 1996 r. Ta poruszająca fotografia przedstawiała dużą grupę błękitnych i białych gwiazd otoczonych delikatnym welonem złotawej materii i gazu. Z podpisu wynikało, że jest to efekt „zderzenia" dwóch galaktyk, w którym mniejsza galaktyka musnęła górną część większej. Czy było możliwe, że Duqu to tajemniczy wirus Stars, który zaatakował Iran[9]? Dla badaczy z Symanteca i z laboratorium CrySyS była to sensowna hipoteza.

Symantec chciał upublicznić informacje o Duqu, jednak zanim badacze się na to zdecydowali, razem z Bencsáthem usunęli z przykładowych plików i z raportu laboratorium CrySyS wszystkie informacje, które pozwalały

[9] Po pojawieniu się informacji o Duqu użytkownik Twittera podający się za irańskiego badacza złośliwego oprogramowania z Wirginii opublikował wpis, w którym stwierdził, że według badań irańskiego zespołu CERT „#Duqu to zaktualizowana wersja złośliwego oprogramowania #Stars". Użytkownik bardzo szybko usunął wpis, a niedługo potem skasował też konto na Twitterze. Nie wiadomo, czy zdjęcie galaktyk w Duqu miało jakieś znaczenie, czy też napastnicy wybrali przypadkową grafikę. Zdaniem Bencsátha zdjęcie mogło być ukrytym przekazem pozwalającym zidentyfikować Duqu jako „przyjacielski ogień". Czasem różne jednostki wywiadowcze tego samego rządu atakują te same komputery. Jeśli to Stany Zjednoczone lub Izrael stały za Duqu, zdjęcie mogło być informacją dla „przyjaciół", którzy trafili na keylogger na zainfekowanej maszynie, próbując się do niej włamać, że dana maszyna została już zainfekowana przez sojusznika.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

zidentyfikować ofiarę lub samo laboratorium[10]. Osiemnastego października zespół z Symanteca opublikował poddany anonimizacji raport laboratorium CrySyS, a także własne analizy Duqu. Ofiarę opisano jako „organizację z siedzibą w Europie", a laboratorium CrySyS jako „laboratorium badawcze o szerokich powiązaniach międzynarodowych"[11].

W ciągu godziny od upublicznienia komunikatu Bencsáth wyśledził w swojej prywatnej witrynie pierwszą osobę szukającą skrótów, które opublikował tydzień wcześniej. Choć badacz usunął je z witryny, pamięć podręczna wyszukiwarki Google zachowała jego wpis, a na forach poświęconych zabezpieczeniom pojawiły się pytania dotyczące usuniętych informacji. Następnego dnia witrynę Bencsátha odwiedziło ponad 400 osób, ponieważ szybko rozeszły się wieści, że dziwna węgierska witryna o rybach w puszce była w jakiś sposób powiązana z Duqu. W witrynie nie było danych kontaktowych Bencsátha, jednak szybko ktoś sprawdził, na kogo zarejestrowana jest domena, i znalazł jego nazwisko. Później wystarczyło wpisać odpowiednie zapytanie w Google'u, aby powiązać badacza z laboratorium CrySyS.

---

[10] Pojawiły się głosy krytykujące decyzję Symanteca o tak szybkim opublikowaniu danych. Bardziej strategicznym podejściem byłoby zachowanie milczenia na czas zbierania dodatkowych informacji o ataku. Symantec mógł np. najpierw poprosić firmy hostingowe, u których działały serwery C&C, o wykonanie kopii lustrzanej tych serwerów, aby zbadać, co napastnicy na nich robią, a dopiero później zasygnalizować napastnikom, że zostali wykryci. Występowała stała rozbieżność między potrzebami badaczy i śledczych a interesami klientów, którzy chcieli jak najwcześniej dowiedzieć się, czy zostali zainfekowani, aby móc zabezpieczyć swoje sieci przed innymi atakami i ustalić, czy intruzi czegoś nie ukradli. Jednak laboratorium CrySyS wysłało już raport do pracownika firmy McAfee, konkurencyjnego producenta oprogramowania antywirusowego, który mógł opublikować te informacje lub przypadkowo ostrzec napastników, że zostali odkryci. Zwlekanie z udostępnieniem danych miało też inne wady. Bez zwiększenia grupy osób wiedzących o tym złośliwym oprogramowaniu trudno było uzyskać inne próbki Duqu, które pomogłyby lepiej zrozumieć atak. Wykryte złośliwe oprogramowanie było silnie ukierunkowane. Infekowało tylko niewielką liczbę ofiar, a każdy związany z Duqu plik uzyskany od ofiar zapewniał badaczom dodatkowe informacje o ataku.

[11] Raport Symanteca na temat Duqu jest dostępny na stronie: *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W tym momencie ukrywanie tożsamości laboratorium nie miało już sensu, dlatego 21 października Bencsáth opublikował w witrynie organizacji krótkie oświadczenie, potwierdzając rolę zespołu w odkryciu Duqu i prosząc wszystkich o zaprzestanie spekulacji na temat ofiary. Na to było już jednak za późno. Rozeszły się wieści, że Duqu zaatakował europejską jednostkę certyfikacyjną. Stało się to po tym, jak Péter Szőr, badacz z firmy McAfee, który otrzymał pierwotny raport Bencsátha, napisał na blogu artykuł zatytułowany „Dzień złotego szakala". Stwierdził w nim, że Duqu atakował jednostki certyfikacyjne, i zalecił takim organizacjom sprawdzenie swoich systemów w celu upewnienia się, że nie zostały zainfekowane. Ponieważ laboratorium CrySyS działało na Węgrzech, wiele osób zakładało, że też zostało zaatakowane. A że w tym kraju znajdowało się niewiele jednostek certyfikacyjnych (najważniejsze z nich to NetLock i Mikrosec e-Szigno), kilku badaczy szybko ustaliło, że ofiarą była firma NetLock. Żaden z nich nie upublicznił jednak tej informacji[12].

Wnioski płynące z ataku były alarmujące. Jednostki certyfikacyjne są podstawą opartych na zaufaniu relacji, dzięki którym działa internet. Wydają certyfikaty, za pomocą których rządy, instytucje finansowe i firmy podpisują swoje oprogramowanie i witryny. Stanowi to dla użytkowników gwarancję, że pobierają legalny program Microsoftu lub wprowadzają dane uwierzytelniające w oficjalnej witrynie Bank of America albo poczty Gmail. Atak na takie jednostki umożliwiłby napastnikom wydawanie sobie poprawnych certyfikatów na dowolną nazwę i używanie ich do podpisywania złośliwego oprogramowania. Był to dodatkowy krok w porównaniu z zastosowaną w Stuxnecie strategią atakowania poszczególnych firm takich jak RealTek, JMicron i C-Media. Jeśli Duqu był efektem prac Stanów Zjednoczonych lub Izraela, oznaczało to, że kraj NATO lub jego sojusznik zaatakował fundamentalną część zaufanej infrastruktury umożliwiającej realizowanie transakcji w internecie. Zostało to zrobione w celu przeprowadzenia tajnej kampanii. Jeśli za atakiem stały Stany Zjednoczone, oznaczało to też, że choć niektóre jednostki rządowe zwracały uwagę na znaczenie zabezpieczania infrastruktury krytycznej w kraju i opracowywanie norm działania w internecie, inne były zajęte włamaniami do należących

[12] To, że ofiarą była firma NetLock, udało się autorce ustalić na podstawie kilku źródeł niepowiązanych z laboratorium CrySyS.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

do sojusznika z NATO krytycznych systemów ważnych dla bezpieczeństwa internetu i ustanawiały wątpliwe normy zachowania, które mogły być naśladowane przez inne kraje. A ponieważ w czasie, gdy ujawniono Duqu, tożsamość ofiary nie została podana, opinia publiczna nie miała okazji do dyskusji na te tematy.

Mimo pominięcia tego ważnego szczegółu ujawnienie informacji o Duqu wywołało w społeczności zajmującej się zabezpieczeniami zupełnie inną reakcję niż Stuxnet. Zespoły badaczy, które biernie się przyglądały, gdy Symantec miesiącami pracował nad analizą ładunku Stuxneta, szybko zajęły się kodem Duqu. Po części wynikało to z tego, że był on prostszy niż kod Stuxneta, a także nie obejmował ładunku wymierzonego w sterowniki PLC. Inną przyczyną było to, że badacze zobaczyli, do czego prowadzi przyglądanie się sytuacji z boku. Stuxnet sygnalizował nastanie nowej ery, a wielu analityków zdecydowało się przeczekać przejściowy okres[13].

Jedną z firm zdeterminowanych, aby tym razem nie zostać w tyle, była rosyjska Kaspersky Lab. Pracujący w niej badacze nie pozostali bezczynni po wykryciu Stuxneta. Włożyli dużo pracy w analizę części ataku związanej z systemem Windows i jako pierwsi badacze z firmy prywatnej wykryli dodatkowe eksploity typu zero-day oraz zgłosili je Microsoftowi. Jednak poza zestawem eksploitów Stuxnet nie wydał im się specjalnie interesujący. Niezrozumiały kod do ataku na sterownik PLC okazał się przeszkodą w analizie ładunku. Ostatecznie firma stwierdziła, że odszyfrowywanie tego kodu przyniesie niewielkie korzyści, dlatego po zakończeniu analiz pocisku zajęła się innymi zadaniami. Badacze nie zamierzali jednak po raz drugi popełnić tego samego błędu.

[13] Nie tylko firmy zajmujące się bezpieczeństwem zareagowały inaczej. Zrobił to także rząd. Z niewiadomych przyczyn w trakcie wielu miesięcy, przez jakie badacze z Symanteca analizowali Stuxneta i publikowali prośby o pomoc do ekspertów od sterowników PLC, zespół ICS-CERT nie reagował, choć zatrudniał analityków posiadających wiedzę potrzebną Symantecowi. Pracownik Departamentu Bezpieczeństwa Wewnętrznego przyznał później w przeprowadzonym przez autorkę książki wywiadzie, że jednostka ta popełniła błąd, nie odpowiadając na prośby Symanteca. Tym razem zespół ICS-CERT postąpił inaczej i skontaktował się z Symantekiem w celu porównania odkryć dotyczących Duqu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

COSTIN RAIU, DYREKTOR globalnego zespołu ds. badań i analiz w firmie Kaspersky, znajdował się w Pekinie, gdy pojawiły się informacje o Duqu. Przygotowywał się właśnie do odprawy na poranny lot do Hongkongu, gdzie był umówiony na spotkanie. Najpierw chciał zadzwonić do współpracowników z Moskwy, ale ci jeszcze spali. Dlatego przed wejściem do samolotu szybko pobrał pliki Duqu udostępnione badaczom przez Symantec i przyjrzał się im w trakcie lotu.

Zaraz po wylądowaniu w Hongkongu skontaktował się z Aleksandrem Gostiewem z Moskwy — młodym, uzdolnionym specjalistą od inżynierii odwrotnej i głównym badaczem złośliwego oprogramowania w firmie. Symantec i laboratorium CrySyS dokładnie przebadały pliki Duqu, jednak Raiu i Gostiew podejrzewali, że można w nich znaleźć znacznie więcej informacji. Mieli rację.

Od początku było dla nich jasne, że Duqu jest dziełem doskonałych programistów. Kod znacznie różnił się od innego oprogramowania szpiegującego, z jakim się zetknęli. Raiu porównał to do różnicy między *Gwieździstą nocą* Vincenta van Gogha a amatorskim malunkiem rozgwieżdżonego nocnego nieba wykonanym przez ucznia szkoły plastycznej. Mistrzowskie pociągnięcia i geniusz kryjące się w kodzie były ewidentne dla wprawnego oka.

Raiu był 33-letnim Rumunem pracującym dla firmy Kaspersky w malutkim biurze w Bukareszcie, które zajmował razem z jeszcze jednym badaczem i grupką marketingowców. Miał ciemne, krótko przycięte, siwiejące włosy oraz dojrzałość i mądrość znacznie starszej osoby. Te ostatnie cechy sprawiały, że w naturalny sposób nadawał się na mentora młodszych członków zespołu. Ponadto miał spokojny, podobny Buddzie sposób bycia, co pomagało mu w stresujących momentach, gdy jednocześnie pracował nad wieloma złożonymi projektami. Ta cecha okazała się nieoceniona w trakcie wielu kolejnych miesięcy, kiedy jego zespół dokładnie badał sprawę Stuxneta i Duqu oraz zaczął przyciągać uwagę agencji wywiadowczych.

Raiu dołączył do firmy w 2000 r. Miał wtedy 23 lata, a firma zatrudniała tylko kilkudziesięciu pracowników. Zrekrutowano go do pracy nad projektem Praga — budowanym przez firmę silnikiem antywirusowym nowej generacji.

Badacz dorastał w komunistycznej Rumunii, a w dzieciństwie jego pasją były nie komputery, tylko chemia. Fascynowały go reakcje wybuchowe mieszanek określonych chemikaliów oraz wnioski o naturze i strukturze świata płynące z podstawowej wiedzy chemicznej. Jednak gdy jeden z eksperymentów

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

prawie doprowadził do wysadzenia mieszkania jego rodziców w powietrze, Raiu otrzymał lokalnie wyprodukowaną kopię komputera PC, aby zajął się czymś mniej niebezpiecznym. Szybko nauczył się programować i jeszcze jako nastolatek napisał od podstaw silnik antywirusowy, który nazwał RAV.

Prace nad tym narzędziem rozpoczął, gdy sieć jego liceum została zainfekowana wirusem, którego nie wykrył szkolny skaner antywirusowy. Raiu przez całą noc pisał sygnatury i dopracowywał narzędzie do wykrywania zagrożenia. Z czasem dodał więcej kodu i funkcji, po czym zaczął udostępniać swój program bezpłatnie pod nazwą MSCAN. Gdy wieści o tym silniku się rozniosły, Raiu został zatrudniony przez rumuńskiego przedsiębiorcę do pracy w firmie GeCAD Software, która zaczęła sprzedawać program Raiu pod nazwą RAV (od słów *Romanian Anti-Virus*). Szybko został on najlepiej się sprzedającym produktem firmy i w kolejnych testach okazywał się lepszy od konkurencyjnych rozwiązań. Przyciągnęło to uwagę Microsoftu. W 2003 r. gigant zakupił program RAV od firmy GeCAD, jednak wtedy Raiu pracował już dla firmy Kaspersky[14].

W tym czasie Kaspersky Lab była firmą stosunkowo mało znaną w Stanach Zjednoczonych. Na rynku oprogramowania antywirusowego dominowały tam Symantec i McAfee. Ponieważ Kaspersky była firmą rosyjską, zmagała się z brakiem zaufania na Zachodzie — tym bardziej, że jej założyciel, Eugene Kaspersky, został wyszkolony w instytucie wspieranym przez KGB i służył w rosyjskim wywiadzie wojskowym. Jednak firma powoli wyrabiała sobie markę w Europie Wschodniej i w innych miejscach świata, głównie na Bliskim Wschodzie, gdzie podobny brak zaufania dotyczył Stanów Zjednoczonych i amerykańskich firm.

Raiu początkowo był zatrudniony jako programista. W 2004 r., gdy firma utworzyła zespół odpowiedzialny za analizowanie i inżynierię odwrotną złośliwego oprogramowania, dołączył do tej grupy. W 2010 r. został jej dyrektorem i nadzorował zespoły badawcze na kilku kontynentach. Obecnie, po odkryciu Duqu, kilka z tych zespołów przystąpiło do działania.

Pracami technicznymi kierował Gostiew, chudy analityk z krótkimi jasnobrązowymi włosami i nieco przygarbionymi plecami, które wskazywały na pełne koncentracji godziny spędzone przed komputerem. Gdy Gostiew i jego współpracownicy analizowali kod, ich uwagę zwróciło kilka kwestii.

[14] Program Security Essentials Microsoftu jest oparty na opracowanym przez Raiu silniku antywirusowym RAV.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wyjątkowo interesującym aspektem był komponent użyty przez napastników do pobierania na maszyny ofiary dodatkowych modułów z ładunkiem w celu wykradania danych. Ten komponent, w odróżnieniu od innych modułów Duqu i Stuxneta, nie był napisany w C lub C++, ale w języku, z którym ani Gostiew, ani Raiu nigdy wcześniej się nie zetknęli. Badacze tygodniami próbowali zidentyfikować ten język i nawet konsultowali się z ekspertami od języków programowania, ale wciąż nie mogli znaleźć odpowiedzi. Dlatego umieścili na blogu prośbę o pomoc i w końcu, po połączeniu różnych drobnych wskazówek, udało im się stwierdzić, że napastnicy zastosowali bardzo rzadki, niestandardowy dialekt języka C razem ze specjalnymi rozszerzeniami przekształcającymi kod, zmniejszającymi jego wielkość i umożliwiającymi jego pracę w różnych systemach[15]. Styl programowania był typowy dla komercyjnego oprogramowania sprzed dziesięciu lat, a nie dla nowoczesnych programów i z pewnością nie dla złośliwego oprogramowania. Było jasne, że autorami nie byli czołowi koderzy posługujący się najnowszymi technikami, tylko programiści starej daty, ostrożni i konserwatywni. C++ mógł czasem prowadzić do powstania w wyniku kompilacji nieprzewidywalnego kodu, który był wykonywany niezgodnie z intencjami autora. Raiu doszedł więc do wniosku, że napastnicy wybrali język C, ponieważ zapewniał im największą kontrolę nad szkodliwym kodem. Następnie zmodyfikowali kod w trakcie kompilacji, by zmniejszyć jego wielkość i ułatwić przesłanie go do ofiar[16].

[15] Napastnicy posługiwali się niestandardowym obiektowym dialektem języka C, OO-C.

[16] Choć ten komponent był dziełem bardzo zaawansowanych programistów, niektóre aspekty ataku były niższej jakości. Dotyczyło to np. szyfrowania. Duqu był zbudowany jak eleganckie chińskie pudełeczko — napastnicy zastosowali wiele warstw szyfrowania ukrywających komponenty i zapobiegających wykryciu ataku. Jednak rozwiązanie to zostało słabo zaimplementowane. W jednej części znajdował się zaszyfrowany blok z konfiguracją, w którym znajdował się klucz do odszyfrowania rejestru. W tym rejestrze zapisany był inny klucz, odszyfrowujący główny plik .DLL Duqu. Ten projekt miał utrudniać osobom, które znalazły plik .DLL, odszyfrowanie go bez znalezienia obu kluczy. Jednak programiści osłabili to zabezpieczenie, stosując identyczne klucze dla rejestru i pliku .DLL oraz używając klucza 0 dla bloku z konfiguracją. Odszyfrowanie bloku z konfiguracją zapewniało więc klucz potrzebny do odszyfrowania głównego pliku .DLL (dodatkowy klucz z rejestru nie był już potrzebny). W Stuxnecie na każdym etapie szyfrowania używany był inny klucz. Ponadto w Stuxnecie zastosowano szyfr czterokrotny, natomiast w Duqu słabszy, jednokrotny. Najwyraźniej więc to różne, choć powiązane zespoły zaprojektowały Duqu i Stuxneta. Jednak choć oba miały do dyspozycji silne i zaawansowane metody szyfrowania, zespół odpowiedzialny za Duqu nie zadbał o ich zastosowanie.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ograniczenia związane z Duqu dotyczyły też mechanizmów rozprzestrzeniania. Stuxnet działał w pełni niezależnie, natomiast Duqu był ściśle kontrolowany. Do rozprzestrzeniania Duqu najwyraźniej nie zastosowano żadnych eksploitów typu zero-day. Duqu nie potrafił też sam się rozprzestrzeniać (w odróżnieniu od Stuxneta). Nawet gdy już znalazł się w maszynie, infekował inne komputery tylko po otrzymaniu od napastników ręcznie przesłanych instrukcji z serwera C&C[17]. Duqu komunikował się z serwerami C&C bardziej dyskretnie niż Stuxnet[18]. Komunikacja była szyfrowana silnym algorytmem AES, aby zapobiec jej odczytaniu, oraz umieszczana w pliku graficznym .JPEG, co pomagało w jej ukryciu. Ponadto inaczej niż w przypadku Stuxneta, który zaatakował ponad 100 tys. maszyn, badacze ostatecznie odkryli niewiele ponad 30 infekcji Duqu[19].

Ofiary znajdowały się w różnych państwach i były różnymi organizacjami: od jednostek wojskowych po producentów sprzętu przemysłowego (np. rur i zaworów). Wszystkie te firmy były starannie dobrane pod kątem „zasobów strategicznych" — wytwarzanych produktów lub świadczonych usług[20]. Nie było zaskoczeniem, że wiele ofiar znalezionych przez firmę Kaspersky miało powiązania z Iranem. Były to firmy albo mające biura w tym kraju, albo handlujące z nim. Jedyną do tej pory ofiarą, która wydawała się nie być powiązana z Iranem, była węgierska organizacja, gdzie po raz pierwszy wykryto atak.

---

[17] W tym celu napastnicy musieli najpierw przejąć kontrolę nad kontem administratora na zainfekowanej maszynie, a następnie skonfigurować zadanie pozwalające złośliwemu oprogramowaniu rozprzestrzeniać się za pomocą udziałów sieciowych.

[18] Twórcy Duqu umieścili niektóre skrypty do sterowania operacją w innych lokalizacjach, a nie na serwerach C&C, dlatego jednostka, która przejęłaby kontrolę nad tymi serwerami, nie mogłaby zdobyć i zbadać tych skryptów, aby ustalić działania podejmowane przez Duqu.

[19] Przez lata ofiarami Duqu mogło paść więcej firm, jednak tylko tyle zostało znalezionych po odkryciu ataku. Symantec natrafił na ofiary w 8 państwach: po jednej we Francji, w Indiach, Holandii, Szwajcarii, Sudanie, Wietnamie i na Ukrainie oraz przynajmniej dwie w Iranie. Kaspersky odkrył 11 dalszych infekcji w Iranie, trzy w Europie i cztery w Sudanie. Inni producenci oprogramowania antywirusowego znaleźli ofiary w Austrii, Indonezji i Wielkiej Brytanii.

[20] Kelly Jackson Higgins, „Same Toolkit Spawned Stuxnet, Duqu, and Other Campaigns", Dark Reading, 3 stycznia 2012 (*http://www.darkreading.com/attacks-breaches/same-toolkit-spawned-stuxnet-duqu-and-other-campaigns/d/d-id/1136876*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Na podstawie informacji znalezionych w plikach dziennika udostępnionych przez niektóre ofiary udało się stwierdzić, że napastnicy byli zainteresowani przede wszystkim wykradaniem plików z programu AutoCAD, a zwłaszcza dokumentów związanych z systemami kontroli procesów przemysłowych używanymi w różnych branżach w Iranie. AutoCAD (CAD to skrót od *computer aided design*, czyli projektowanie wspomagane komputerowo) to oprogramowanie służące do rysowania dwu- i trójwymiarowych projektów architektonicznych oraz projektowania układów komputerowych i produktów konsumpcyjnych. Używa się go też do planowania układów sieci komputerowych i maszyn w halach fabrycznych. Te ostatnie plany byłyby przydatne komuś, kto chciałby zbombardować fabrykę lub przeprowadzić atak podobny do Stuxneta.

Napastnicy w systematyczny sposób prowadzili akcje przeciw ofiarom. Dla każdego celu przygotowywali nowe pliki i odrębne serwery C&C w Europie i Azji, tak aby z jednym serwerem komunikowały się tylko dwie lub trzy zainfekowane maszyny. Taki podział bez wątpienia pomagał w śledzeniu różnych operacji i grup ofiar, a dodatkowo sprawiał, że gdy ktoś z zewnątrz uzyskał dostęp do jednego z serwerów, miał bardzo ograniczony wgląd w całość operacji. Wspomniane serwery okazały się pośrednikami — stacjami przekaźnikowymi, przez które napastnicy kierowali wykradzione dane na inne maszyny. Było to dodatkowe zabezpieczenie przed ujawnieniem całej operacji lub prześledzeniem drogi skradzionych danych do napastników. Na przykład dane ofiary z Węgier były najpierw przesyłane na serwer w Indiach, następnie na serwer na Filipinach, a potem jeszcze gdzieś indziej. Dane z Iranu trafiały na serwer w Wietnamie, później na serwer w Niemczech, a następnie jeszcze dalej. Badacze próbowali podążać za tym śladem, jednak po natrafieniu za każdym razem na trzy kolejne serwery pośredniczące stwierdzili, że nigdy nie dotrą do celu. Dlatego dali za wygraną.

Na szczęście dzięki pomocy firm hostingowych, gdzie działały te serwery, firma Kaspersky uzyskała kopie lustrzane pięciu takich maszyn, w tym serwera z Wietnamu, który kontrolował infekcje z Iranu. Badacze odkryli, że 20 października, dwa dni po upublicznieniu przez Symantec informacji o Duqu, napastnicy przeprowadzili szeroko zakrojoną akcję usuwania danych

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

w panicznej próbie wyczyszczenia informacji z serwerów[21]. Jednak starając się w pośpiechu usunąć dowody, pozostawili ślady dzienników, które dały firmie Kaspersky wskazówki dotyczące działań napastników[22]. Z dzienników wynikało np., że napastnicy zarejestrowali jeden z serwerów C&C w Niemczech w listopadzie 2009 r., czyli dwa lata przed wykryciem Duqu. To sugerowało, że Duqu działał przynajmniej tak długo. Badacze z firmy Kaspersky zaproponowali hipotezę, że Duqu był w rzeczywistości *prekursorem* Stuxneta, a nie, jak zakładali analitycy Symanteca, jego następcą. Niedługo później znaleźli dowody potwierdzające te podejrzenia.

POCZĄTKOWO NIE BYŁO jasne, w jaki sposób Duqu infekował maszyny. W Stuxnecie do rozprzestrzeniania szkodliwych plików zastosowano pendrive'y z eksploitem wykorzystującym pliki .LNK. Jednak laboratorium CrySyS nie znalazło droppera na komputerach firmy Bartosa. Nie wykryło też żadnych eksploitów typu zero-day. Gdy Symantec opublikował raport na temat Duqu, Chien poprosił Bencsátha, aby zaatakowana węgierska

[21] Jeśli to Izrael stworzył Duqu, opóźnienie mogło wynikać z tego, że 18 października (kiedy to Symantec opublikował swój raport) wypadał w izraelskie święto Sukkot, trwające tego roku od 13 do 19 października. Sukkot upamiętnia 40 lat spędzonych przez Izraelczyków na pustyni Synaj po ucieczce z egipskiej niewoli. W Izraelu pierwszy dzień tego święta jest wolny od pracy. Pozostałe sześć dni nie jest ustawowo świętem, jednak wielu Izraelczyków bierze wtedy urlop, ponieważ szkoły są zamknięte. Sukkot kończył się w tym roku 19 października, a pracownicy wracali do zadań 20. Mogło to dotyczyć także zespołu odpowiedzialnego za serwery Duqu.

[22] Napastnicy pozostawili też inne ślady. W nocy przed ujawnieniem informacji o Duqu zmienili klucze szyfrujące i skompilowali Duqu z użyciem nowych kluczy. Następnie przesłali nowe pliki na zainfekowane maszyny. Zapewne zamierzali w ten sposób zastąpić starsze wersje Duqu nowszymi w opanowanych systemach, jednak nie uwzględnili nietypowego działania systemu operacyjnego Windows, co spowodowało pozostawienie śladów dawnych plików. Badacze odkryli je później po przeskanowaniu systemów programami antywirusowymi. Napastnicy mogli zmienić klucze szyfrujące, ponieważ podejrzewali, że ich złośliwe oprogramowanie zostało wykryte, i chcieli zdążyć z tym przed ujawnieniem akcji. Skoro jednak zakładali, że zostali zauważeni, najwyraźniej nie rozumieli, w jakim stopniu ich misja zostanie ujawniona. W aktualizacji wydłużyli czas życia swojego złośliwego oprogramowania do więcej niż 36 dni, tak jakby oczekiwali, że będą mogli prowadzić akcję bez zakłóceń. Po ujawnieniu informacji zrozumieli jednak, że cała operacja została zaprzepaszczona, i przystąpili do usuwania wszystkich danych z serwerów.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

firma przeszukała systemy pod kątem podejrzanych operacji w okolicach 11 sierpnia (był to dzień infekcji). W efekcie udało się znaleźć e-mail z załączonym dokumentem w Wordzie. Załącznik miał ok. 700 kB — znacznie więcej niż dokumenty standardowo otrzymywane przez firmę. Zainteresowało to pracowników firmy. Gdy zespół z laboratorium CrySyS otworzył e-mail w systemie testowym, rzeczywiście doprowadziło to do umieszczenia w nim szkodliwych plików Duqu[23].

Ponieważ kod ataku do tej pory pozostał niewykryty, badacze z laboratorium podejrzewali, że napastnicy posłużyli się eksploitem typu zero-day. Bencsáth przesłał dropper do zespołu z Symanteca, gdzie ustalono, że kod faktycznie wykorzystywał lukę typu zero-day związaną z przepełnieniem bufora w silniku obsługi czcionek TrueType w systemie Windows. Ten silnik odpowiada za wyświetlanie znaków na ekranie. Gdy w dokumencie Worda pojawia się kod znaku, silnik sprawdza odpowiedni plik czcionki, aby ustalić, jak dany znak powinien wyglądać. W omawianej sytuacji, gdy silnik próbował wczytać kod czcionki, z powodu luki uruchamiany był eksploit.

Ten eksploit był prawdziwym „kozakiem", jak nazwał go jeden z badaczy. Normalny eksploit atakujący lukę związaną z przepełnieniem bufora zapewnia hakerom zwykle tylko dostęp do maszyny z poziomu użytkownika. Oznacza to, że napastnik potrzebuje drugiej luki i drugiego eksploita, aby zdobyć uprawnienia z poziomu administratora i bez przeszkód zainstalować szkodliwy kod[24]. Jednak wykryty eksploit potrafił pokonać warstwy zabezpieczeń, co pozwoliło na niezakłóconą instalację i wykonywanie szkodliwego kodu na poziomie jądra maszyny. Luki związane z przepełnieniem bufora, które umożliwiają atak na poziomie jądra, są rzadkie i trudne do wykorzystania bez spowodowania awarii maszyny. Ale eksploit z Duqu działał bezbłędnie. Był zdecydowanie bardziej zaawansowany

[23] Wykryty dropper nie instalował natychmiast swojego szkodliwego ładunku. Zamiast tego odczekiwał, aż komputer będzie bezczynny przez przynajmniej 10 min, i dopiero wtedy przystępował do działania. Ponadto data w komputerze musiała wypadać w ośmiodniowym oknie w sierpniu. W przeciwnym razie Duqu nie instalował swoich plików. Był to kolejny dowód na ostrożność napastników i zachowywaną przez nich kontrolę nad kodem.

[24] Bloger z fińskiej firmy antywirusowej F-Secure określił go mianem „kozaka wśród eksploitów". „Duqu Attack's Installer Discovered", 2 listopada 2011 (*https://f-secure.com/weblog/archives/00002263.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

niż eksploit plików .LNK ze Stuxneta. Eksploit ze Stuxneta został błyskawicznie skopiowany przez cyberprzestępców po ujawnieniu go w lipcu 2010 r. Natomiast udane skopiowanie eksploita z Duqu wymagało miesięcy pracy[25].

Ten eksploit sam w sobie był godny uwagi. Ponadto napastnicy ukryli w kodzie także kilka „jaj wielkanocnych" — prawdopodobnie po to, aby zadrwić z ofiar. Fałszywej czcionce używanej w ataku nadali nazwę Dexter Regular, a w informacjach o prawach autorskich do niej napisali: „Copyright © 2003 Showtime Inc. All rights reserved. Dexter Regular"[26].

Było oczywiste, że nawiązywali do popularnego serialu telewizyjnego *Dexter*, emitowanego wówczas w sieci Showtime. Tylko że emisję serialu rozpoczęto dopiero 1 października 2006 r., dlatego data praw autorskich, 2003, wydawała się dziwna. Nie było jasne, czy to „jajo wielkanocne" miało

[25] Badacze w czerwcu 2012 r., osiem miesięcy po opublikowaniu informacji o luce przez Symantec, znaleźli ślady wskazujące na to, że cyberprzestępcy bez powodzenia próbowali skopiować eksploit z Duqu. Udało im się to dopiero w październiku 2012 r. W grudniu tego roku firma Kaspersky odnotowała wzrost liczby ataków z użyciem kopii omawianego eksploita. Jednak w grudniu 2011 r. Microsoft załatał lukę, dlatego napastnicy mogli wykorzystać eksploit tylko przeciw niezaktualizowanym maszynom.

[26] Badacze z firmy Kaspersky znaleźli w kodzie coś jeszcze, co mogło być „jajem wielkanocnym". Wartość klucza deszyfrującego w jednej z wersji sterownika z Duqu wynosiła 0xAE240682 i wyglądała na datę 24 czerwca 1982 r. Raiu dowiedział się, że była to data słynnego wydarzenia w historii lotnictwa. W tym dniu samolot o numerze lotu 09 linii British Airways wleciał w chmurę pyłów wulkanicznych w trasie z Londynu do Nowej Zelandii. Samolot właśnie wystartował po międzylądowaniu w Malezji, gdy gęsty pył z wulkanu Galunggung zadławił wszystkie cztery silniki maszyny 747, przez co maszyna pozostała bez napędu w powietrzu. Piloci próbowali szybować i w ten sposób podejść do lądowania. Gdy samolot obniżył pułap z ponad 11 km do ok. 3,6 km, z sufitu wyrzucone zostały maski tlenowe. Wtedy brytyjski kapitan Eric Moody wsławił się jednym z najsłynniejszych niedomówień w historii lotnictwa. „Panie i panowie — powiedział pasażerom — mówi kapitan. Mamy niewielki problem. Wszystkie cztery silniki przestały działać. Robimy wszystko co w naszej mocy, aby je uruchomić. Mam nadzieję, że nie jesteście państwo zanadto zestresowani". Zob. „When Volcanic Ash Stopped a Jumbo at 37 000 ft", BBC, 15 kwietnia 2010 (*http://news.bbc.co.uk/2/hi/uk_news/magazine/8622099.stm*). Po ok. 15 min pilotom udało się wznowić pracę silników, po czym wylądowali w Dżakarcie. Czy to przypadek, że było to drugie nawiązanie do lotnictwa po wartości DEADF007 ze Stuxneta? A może napastnicy bawili się z badaczami i umieszczali w kodzie „jaja wielkanocne", aby zmusić analityków do myślenia? A może wartość w kodzie była po prostu przypadkową liczbą bez żadnego znaczenia?

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

jakieś znaczenie, czy jest tylko żartem. Serial przedstawiał Dextera Morgana, kryminologa i mściciela mordującego przestępców. Dexter jest mordercą przestrzegającym zasad i zabijającym tylko w imieniu dobra społecznego. Przynajmniej taki był punkt widzenia Dextera. Prawdopodobnie w ten właśnie sposób — jako środki prowadzące do większego dobra — Stany Zjednoczone i Izrael postrzegały cyberatak na Iran lub zamachy na irańskich naukowców jądrowych[27].

Nazwa czcionki i data praw autorskich były dla badaczy interesującą ciekawostką, jednak ważniejszym aspektem droppera była data kompilacji — 21 lutego 2008 r. Stanowiła ona wskazówkę sugerującą, od jak dawna Duqu mógł działać. Niedługo po znalezieniu droppera firma Kaspersky natrafiła na drugi plik, skompilowany jeszcze wcześniej i znaleziony w komputerze w Sudanie[28].

Sudan w obszarze wojskowości miał dobre stosunki z Iranem. Od 2004 do 2006 r. Sudańczycy otrzymali od Iranu broń wartą 12 mln dolarów i otwarcie wyrażali poparcie dla irańskiego programu nuklearnego. W 2006 r. Iran publicznie zobowiązał się podzielić wiedzą na temat technologii nuklearnych z Sudanem. Sudan także był objęty sankcjami ONZ-etu. Ofiarą Duqu w Sudanie była firma handlowa zainfekowana w kwietniu 2011 r., cztery miesiące przed atakiem na Węgrzech. Szkodliwy kod został zainstalowany za pomocą phishingu i tego samego eksploita typu zero-day Dexter, który zastosowano na Węgrzech. Szkodliwy e-mail, rzekomo wysłany przez menedżera ds. marketingu B. Jasona, nadszedł z komputera z Korei Południowej, przy czym maszyna ta została zapewne zhakowana w celu przesłania

[27] Costin Raiu z firmy Kaspersky kupił wszystkie odcinki serialu *Dexter*, aby sprawdzić, czy napastnicy celowo nawiązali do niego w Duqu. Tylko jeden odcinek można było uznać za choć trochę powiązany z atakiem. W tym odcinku siostrze Dextera, Debrze, oświadczył się detektyw Joey Quinn. W trakcie rozmowy o oświadczynach z bratem Debra stwierdziła, że gdyby wyszła za Quinna, jej inicjały brzmiałyby DQ. Raiu obejrzał też inny odcinek, który skojarzył mu się z atakiem. Dexter, aby zmylić śledczych, którzy byli na jego tropie, napisał 30-stronicowy manifest pełen nawiązań biblijnych. Gdy śledczy marnowali czas, szukając wskazówek w nieznaczącym dokumencie, Dexter kontynuował serię zabójstw. Analogie nie umknęły uwadze Raiu, który zaczął się zastanawiać, ile godzin zmarnotrawił, oglądając serial telewizyjny w poszukiwaniu wskazówek dotyczących Duqu.

[28] Plik droppera (sterownik) ukrywał się pod postacią sterownika graficznego firmy Intel i odpowiadał za wczytywanie tylnej furtki Duqu na komputer ofiary.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wiadomości[29]. „Szanowny panie — pisał nadawca — znalazłem w państwa witrynie informacje o firmie i chciałbym nawiązać z państwem współpracę biznesową. Proszę o zapoznanie się z listą zamówień z załącznika". W załączonym dokumencie znajdował się kwestionariusz z kilkoma pytaniami, a także rysunek zielonej Ziemi z wyrastającymi z jej górnej części roślinami. Gdy ofiara otworzyła załącznik, eksploit Dexter przystąpił do działania i umieścił swój szkodliwy ładunek na komputerze.

Ten instalujący Duqu dropper został skompilowany w sierpniu 2007 r., co dodatkowo potwierdzało, że Duqu działał już od lat przed wykryciem go na Węgrzech. Nie był to jedyny dowód wskazujący na dawną datę powstania kodu. Badacze stwierdzili też, że również plik do wykradania informacji istniał od wielu lat. Odkryli to tylko dzięki błędowi popełnionemu przez napastników.

Gdy po 36 dniach aktywowany był mechanizm samozniszczenia Duqu, jego zadaniem było usunięcie z zainfekowanych maszyn wszystkich śladów ataku, tak aby ofiara nigdy się o nim nie dowiedziała. Jednak zespół z firmy Kaspersky odkrył, że Duqu w trakcie usuwania danych pomijał niektóre tworzone na komputerach pliki tymczasowe przeznaczone do przechowywania skradzionych danych. Jeden z tych plików, zapisany na maszynie w Iranie, został utworzony 28 listopada 2008 r.

Firmy Kaspersky i Symantec od początku podejrzewały, że przed atakiem Stuxneta na wirówki w Iranie napastnicy posłużyli się narzędziem szpiegowskim do zebrania informacji na temat konfiguracji sterowników PLC Siemensa. Te dane mogły pochodzić od „kreta", jednak teraz bardziej prawdopodobne wydawało się, że napastnicy posłużyli się cyfrowym szpiegiem podobnym do Duqu.

Wydawało się możliwe, że twórcy Stuxneta zastosowali Duqu do wykradzenia cyfrowych kluczy i certyfikatów z firm RealTek i JMicron, ponieważ to właśnie narzędzie zostało użyte przeciwko jednostce certyfikacyjnej z Węgier.

Jeśli Duqu rzeczywiście niewykryty infekował systemy od 2007 r. (lub jeszcze dłużej), jego nagłe wykrycie na Węgrzech w 2011 r. wydawało się dziwne.

[29] Badacze wykryli dwie próby zainfekowania ofiary: pierwszą z 17 kwietnia 2011 r. (została ona zablokowana przez filtr antyspamowy programu Outlook) i drugą, udaną, z 21 kwietnia.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Dlaczego akurat wtedy?" — zastanawiał się Raiu. Doszedł do wniosku, że przyczynami musiały być pycha i zły wybór celu. Napastnicy pozostawali niewykryci przez tak długi czas, że zaczęli wierzyć, iż nigdy nie zostaną złapani. Prawdopodobnie uznali, że ujawnienie Stuxneta rok wcześniej było anomalią wynikającą tylko z tego, że ta cyfrowa broń zanadto się rozprzestrzeniła. Natomiast Duqu był starannie kontrolowany, a jego cele odpowiednio dobierane. Dlatego wykrycie go było mniej prawdopodobne. Jednak na Węgrzech napastnicy zaatakowali nieodpowiedni cel. Węgierska jednostka certyfikacyjna dużo bardziej dbała o zabezpieczenia niż firmy handlowe i produkcyjne, które Duqu atakował wcześniej. I to okazało się przyczyną niepowodzenia zespołu autorów Duqu[30].

Choć w Stuxnecie i Duqu używane były te same fragmenty kodu i techniki, Raiu i jego zespół ostatecznie stwierdzili, że oba ataki zostały opracowane przez inne grupy na tej samej podstawowej platformie. Tę platformę nazwano Tilde-d (czyli „tylda i d"), ponieważ zarówno w Stuxnecie, jak i w Duqu pliki zaczynały się od członu ~D[31].

Firma Kaspersky odkryła dowód na to, że na podstawie tej samej platformy zbudowano też inne narzędzie, a nie tylko Stuxneta i Duqu. Badacze znaleźli przynajmniej sześć sterowników o tych samych cechach i zbudowanych prawdopodobnie z użyciem platformy Tilde-d. Dwa z nich zostały

[30] W momencie włamania węgierska firma zachowywała wzmożoną czujność, ponieważ we wcześniejszych miesiącach nastąpiły dwa inne, pozornie niepowiązane ataki na jednostki certyfikacyjne. W marcu ktoś włamał się na konto firmy współpracującej z Comodo Group, jednostką certyfikacyjną z siedzibami pod New Jersey i w Wielkiej Brytanii. Haker posługujący się irańskim adresem IP uzyskał dostęp do serwerów tej firmy, aby wydać sobie osiem fałszywych certyfikatów dla domen mail.google.com, login.yahoo.com i sześciu innych. Pozwalało to podawać się za te witryny w trakcie ataków *man in the middle*. Cztery miesiące później nastąpiło włamanie do holenderskiej jednostki certyfikacyjnej DigiNotar. W tym przypadku intruzi wygenerowali ponad 200 fałszywych certyfikatów cyfrowych dla popularnych domen należących do firm Google, Yahoo! i Mozilla, a także dla witryn Mosadu, MI6 i CIA. Te ataki sprawiły, że inne jednostki certyfikacyjne zaczęły mieć się na baczności, a węgierska firma zapewne w efekcie rozpoczęła inspekcję swojej sieci.

[31] Keylogger i program do wykradania danych z Duqu tworzyły pliki o nazwach zaczynających się od ~DQ, jednak inne komponenty tego oprogramowania generowały pliki z nazwami o początkowych członach ~DO i ~DF. Stuxnet tworzył pliki tymczasowe o nazwach zaczynających się od ~D.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

użyte w znanych atakach Stuxneta, a trzecim był sterownik z Duqu[32]. Znalezione zostały też trzy samodzielne „sterowniki fantomowe" (niepowiązane z plikami Stuxneta lub Duqu), dlatego trudno było ustalić, czy były one używane w omawianych tu atakach, czy w zupełnie innych operacjach. We wszystkich tych sterownikach zastosowane zostały algorytmy i klucze podobne do tych ze sterowników ze Stuxneta i Duqu (lub nawet identyczne z nimi). Było więc jasne, że ich autorami są ludzie powiązani z zespołem twórców platformy Tilde-d.

Pierwszy z tych sterowników został wykryty w lipcu 2010 r. przez słowacką firmę antywirusową ESET i był podpisany certyfikatem firmy JMicron[33]. Ponieważ ten sterownik znaleziono krótko po ujawnieniu informacji o Stuxnecie, wszyscy zakładali, że był powiązany z tym atakiem. Nikt jednak nie odkrył go w żadnym systemie zainfekowanym przez Stuxneta. Ten sterownik łączył cechy sterowników ze Stuxneta i Duqu. Jego kod był prawie taki sam jak w sterowniku ze Stuxneta, ponadto używane były funkcje i techniki ze sterownika z Duqu. Jednak do szyfrowania posłużył szyfr siedmiokrotny, bardziej złożony od czterokrotnego szyfru sterownika ze Stuxneta. To sprawiło, że Raiu i Gostiew zaczęli podejrzewać, iż nowy sterownik został zaprojektowany na potrzeby innej wersji Stuxneta lub zupełnie innego złośliwego oprogramowania.

Drugi fantomowy sterownik został przesłany do firmy VirusTotal[34]. Data jego kompilacji to 20 stycznia 2008 r. Także w nim zastosowano szyfr siedmiokrotny, co wskazywało, że ten sterownik i sterownik z certyfikatem firmy JMicron mogły posłużyć do tego samego ataku (w nieznanej wersji Stuxneta lub w zupełnie innej akcji).

---

[32] Na zainfekowanych maszynach znajdowało się wiele wersji sterownika Duqu. Każda z nich miała inną nazwę, jednak wszystkie zawierały ten sam kod i zostały skompilowane tego samego dnia. Co ciekawe, jedna z wersji sterownika znaleziona na komputerach na Węgrzech była niepodpisana i miała udawać produkt firmy JMicron — tajwańskiego producenta, którego certyfikat posłużył do podpisania wiązanego ze Stuxnetem sterownika znalezionego przez ESET w lipcu 2010 r. W opisie właściwości sterownika napastnicy zapisali, że jest to JMicron Volume Snapshot Driver. Był to kolejny szczegół łączący Duqu ze Stuxnetem.

[33] Był to sterownik o nazwie *jmidebs.sys*.

[34] Był to sterownik o nazwie *rndismpc.sys*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Trzeci tajemniczy sterownik też został przesłany do firmy VirusTotal i nadszedł z chińskiego adresu IP 17 maja 2011 r., kilka miesięcy przed zainfekowaniem w sierpniu węgierskich maszyn przez Duqu[35]. W tym sterowniku używany był szyfr czterokrotny i taki sam klucz szyfrujący jak w sterownikach Stuxneta. Nowy sterownik został ponadto skompilowany w tym samym dniu co sterowniki Stuxneta i z użyciem zastosowanego także dla nich certyfikatu firmy RealTek. Został jednak podpisany 18 marca 2010 r., a nie 25 stycznia, kiedy to podpisano sterowniki Stuxneta. Dzień 18 marca tylko o kilka tygodni poprzedzał zastosowanie wersji Stuxneta z kwietnia 2010 r., ale z niewiadomych przyczyn w tej operacji napastnicy nie użyli nowego sterownika. Zamiast tego ponownie posłużyli się sterownikiem z ataku z czerwca 2009 r. To sugerowało, że każdy z trzech fantomowych sterowników został przygotowany na potrzeby innego ataku.

Pytanie, które nurtowało Gostiewa i Raiu, dotyczyło oczywiście tego, na potrzeby jakich ataków opracowane zostały fantomowe sterowniki i kim były ich ofiary. Czy te sterowniki były dowodem na to, że przed czerwcem 2009 r. lub po kwietniu 2010 r. wystąpiły inne, niewykryte ataki z użyciem Stuxneta?

Wyglądało na to, że historia Stuxneta nie jest jeszcze kompletna.

[35] Był to sterownik o nazwie *rtniczw.sys*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 15

FLAME

Do wiosny 2012 r. zespół z firmy Kaspersky zakończył analizy Duqu i serwerów. Badacze byli pewni, że to nie koniec całej historii, nie wyobrażali sobie jednak, jakie odkrycie ich czeka. Okazało się, że Stuxnet — program, który zadziwił wszystkich zuchwałością i niszczycielskim potencjałem — był tylko odgałęzieniem operacji cyberszpiegowskiej o kilka rzędów wielkości poważniejszej niż ta pojedyncza broń cyfrowa.

NOWE ODKRYCIA ZACZĘŁY pojawiać się w kwietniu, gdy wirus na komputerach irańskiego ministerstwa ds. ropy naftowej i irańskiej narodowej firmy naftowej skasował dyski twarde we wszystkich napotkanych systemach. Szkody były wyrządzane metodycznie i kompleksowo. Za każdym razem niszczone były gigabajty danych. Najpierw złośliwe oprogramowanie usuwało dokumenty i pliki z danymi, a później pliki systemowe. Uszkadzało też kluczowe fragmenty dysków twardych, co skutkowało ich zniszczeniem.

Nie było jasne, ile komputerów zostało dotkniętych. Według plotek problemy w niektórych komputerach zaczęły się już w grudniu. Początkowo nikt nie zauważył trendu. Zaczęto coś podejrzewać dopiero wtedy, gdy problem się rozprzestrzenił i nie dało się go dłużej ignorować. Nie było wiadomo, ile czasu wirus krył się w maszynach, zanim rozpoczął atak.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak zawsze zaczynał niszczyć dyski ok. 20. dnia miesiąca. Irańscy urzędnicy nazwali go Wiper (czyli „wycieraczka") i obwinili za atak Stany Zjednoczone oraz Izrael. Utrzymywali przy tym, że atak nie spowodował trwałych szkód, ponieważ wszystkie usunięte dane zostały zarchiwizowane.

Gdy Raiu i zespół z firmy Kaspersky otrzymali kopię lustrzaną jednego z wykasowanych dysków twardych z Iranu, okazało się, że dysk jest zapełniony przypadkowymi bitami. Zniknęły nie tylko wszystkie dokumenty i krytyczne pliki systemowe, ale też wszelkie ślady po Wiperze. Pozostała na szczęście ważna wskazówka: jedna referencja w kluczu w rejestrze prowadząca do pliku tymczasowego *~DF78.tmp*, utworzonego w systemie przed rozpoczęciem kasowania danych. Sam plik zniknął, przetrwała natomiast jego nazwa — duch zdradzający jego dawną obecność. Przedrostek ~D w nazwie był już dla badaczy ważnym znakiem. Była to ta sama konwencja nazewnicza, którą Duqu stosował dla generowanych w zainfekowanych maszynach plików tymczasowych. Tę samą konwencję dla niektórych plików stosował też Stuxnet.

Czy Duqu lub inny program napisany przez ten sam zespół znajdował się w komputerze przed wyczyszczeniem go przez Wipera[1]? Czy Wiper był efektem pracy tej samej grupy, która stworzyła też Duqu?

Raiu i jego zespół zaprogramowali narzędzia antywirusowe Kaspersky'ego, aby szukały pliku *~DF78.tmp*, a także by wskazywały inne pliki tymczasowe o nazwach zaczynających się od ~D. Znaleźli wiele maszyn w różnych krajach. Większość tych komputerów znajdowała się w Iranie. Gdy otrzymali kopię jednego z takich plików (*~DEB93D.tmp*), odkryli, że był to dziennik sniffera, który rejestrował hasła przesyłane w sieci lokalnej zainfekowanej maszyny. Po poszukiwaniach znaleźli moduł, który mógł odpowiadać za tworzenie dziennika sniffera[2]. Okazało się to jednym z najważniejszych odkryć zespołu.

---

[1] Także inna wskazówka odkryta w zniszczonych systemach wydawała się prowadzić do twórców Stuxneta i Duqu. Dotyczyła ona tego, że pierwszą rzeczą, jaką Wiper robił po znalezieniu się w systemie, było wyszukiwanie i usuwanie wszystkich plików o rozszerzeniu .PNF. Raiu przypomniał sobie, że było to rozszerzenie pliku z ładunkiem ze Stuxneta, a także niektórych innych plików tego robaka. Również w Duqu występowały pliki o tym rozszerzeniu, natomiast w innym złośliwym oprogramowaniu jest ono rzadkie.

[2] Dziennik zawierał też wewnętrzne nazwy zainfekowanych irańskich systemów.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nowy moduł nie przypominał plików ze Stuxneta lub Duqu. Nie wyglądał też jak Wiper, ponieważ nie zawierał kodu do kasowania dysku twardego zainfekowanych maszyn. Badacze przeszukali swoje archiwum, aby sprawdzić, czy w przeszłości automatyczny system raportowania nie wyszukał podobnych plików. Jeden po drugim znajdowali kolejne moduły, które zdawały się czekać w archiwum na odkrycie. Natrafili w sumie na 20 różnych plików o dziwnych nazwach, takich jak Euphoria, Munch, Limbo, Frog i Snack. Pliki te wyglądały na wtyczki lub komponenty powiązanych ataków.

Analityków najbardziej zaintrygowało jednak to, że jeden z plików trafił do systemu raportowania w październiku 2010 r. i został opisany jako plik Stuxneta. Początkowo badacze uznali, że nie ma to sensu, ponieważ plik nie przypominał komponentów Stuxneta. Po ponownej analizie odkryli, co te pliki miały ze sobą wspólnego — oba zawierały eksploit typu zero-day, który badacze z Symanteca przeoczyli, gdy dwa lata wcześniej analizowali Stuxneta.

Ten eksploit znajdował się w części Stuxneta nazwanej zasobem 207, występującej tylko w ataku z czerwca 2009 r. (nie było jej w wersjach z 2010 r.). To wyjaśniało, dlaczego badacze wcześniej ją przeoczyli. Na zainfekowanych komputerach znaleziono bardzo niewiele wersji z 2009 r.

Zasób 207 zawierał kod używany przez Stuxneta z 2009 r. do sprawiania, by mechanizm automatycznego uruchamiania z systemu Windows instalował robaka zapisanego na pendrive'ach. Zasób zawierał też przeoczony eksploit zastosowany w nowym ataku. Ten eksploit zapewniał napastnikom wyższe uprawnienia w zainfekowanych maszynach dzięki wykorzystaniu luki przepełnienia bufora w funkcji obsługi tapet w systemie Windows. W czasie tworzenia eksploita w lutym 2009 r. była to luka typu zero-day, jednak do momentu zastosowania Stuxneta cztery miesiące później (w czerwcu) Microsoft zdążył rozwiązać problem[3]. Gdy w marcu 2010 r. zastosowana została nowa wersja Stuxneta, napastnicy usunęli z niej ten eksploit wraz z kodem wykorzystującym mechanizm automatycznego uruchamiania. Te części zastąpiono eksploitem plików .LNK i dwoma innymi eksploitami (wówczas typu zero-day) zwiększającymi uprawnienia.

[3] Microsoft wyeliminował lukę 9 czerwca, mniej więcej dwa tygodnie przed wypuszczeniem czerwcowej wersji Stuxneta (22 czerwca 2009 r.).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Odkrycie eksploita funkcji obsługi tapet oznaczało, że Stuxnet na różnych etapach wykorzystywał nie cztery (co i tak było imponującą liczbą), a pięć eksploitów typu zero-day. Ważniejsze było jednak to, że powiązanie między Stuxnetem a nowym atakiem stanowiło dodatkowy dowód na to, że Stuxnet był częścią zestawu szkodliwych narzędzi opracowanych przez ten sam zespół.

ALEKSANDER GOSTIEW Z FIRMY Kaspersky i jego zespół podzielili 20 znalezionych modułów z nowego ataku i przystąpili do ich inżynierii odwrotnej, aby zobaczyć, w jaki sposób były powiązane. Badacze pracowali dniami i nocami, napędzani kofeiną i ekscytacją płynącą ze świadomości, że właśnie odkryli następne narzędzie w arsenale Stuxneta.

Po trzech tygodniach zespół miał w rękach zestaw cyfrowych narzędzi szpiegowskich większy niż cokolwiek, z czym wcześniej się zetknięto. Badacze nazwali go Flame (czyli „płomień") od nazwy jednego z głównych modułów ataku[4].

Już Stuxnet był duży, ponieważ po skompresowaniu zajmował 500 kB. Jednak wszystkie komponenty Flame'a po połączeniu liczyły przynajmniej 20 MB i ponad 650 tys. wierszy kodu. Ta wielkość szła w parze ze złożonością. Badacze oszacowali, że napisanie tego kodu zajęłoby sześciu programistom przynajmniej trzy lata. Aby odszyfrować cały kod, badacze z Kaspersky'ego musieliby pracować latami. Dlatego ograniczyli się do odszyfrowania wystarczającej ilości kodu, by móc go zrozumieć.

Zespół z Kaspersky'ego przez lata widział dużo różnych cyfrowych narzędzi szpiegowskich (uważano, że wiele z nich jest używanych przez Chiny). Jednak nowe narzędzie całkowicie zmieniało sytuację. Gdyby Wydział Q z filmów o Bondzie obejmował cyfrową zbrojownię, Flame by się w niej znajdował.

[4] W kwestii powiązania Flame'a z Wiperem pojawiły się pewne nieporozumienia, gdy badacze z Kaspersky'ego odkryli w kodzie Flame'a moduł o nazwie *Viper*. Moduł ten służył do przesyłania wykradzionych danych na serwer C&C, a nie do kasowania dysków twardych w zainfekowanych maszynach. Jednak istnienie tego modułu doprowadziło początkowo do pytań o to, czy Wiper znaleziony przez Irańczyków nie był komponentem Flame'a. W rozwianiu wątpliwości nie pomagało to, że w irańskich raportach Wiper był przedstawiany jako Viper, co wynikało z błędu w transliteracji perskiego tekstu na angielski. Ostatecznie badacze z Kaspersky'ego nie znaleźli bezpośrednich powiązań Wipera z Flame'em.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Narzędzie zawierało mnóstwo szpiegowskich gadżetów przeznaczonych do zbierania na różne sposoby danych dotyczących ofiar. Wśród tych gadżetów znajdował się moduł przesyłający dokumenty z zainfekowanych maszyn oraz mechanizm rejestrujący wciśnięcia klawiszy i wykonujący zrzuty ekranu w przedziałach od 15 do 60 s. Trzeci moduł ukradkowo uruchamiał wewnętrzny mikrofon zainfekowanego komputera, aby podsłuchiwać pobliskie rozmowy. Czwarty posługiwał się Bluetoothem do wykradania danych z wykrywalnych smartfonów i innych znajdujących się w pobliżu urządzeń.

Flame wyglądał na wielofunkcyjne narzędzie szpiegowskie opracowane w celu spełnienia wszelkich potrzeb w zależności od misji. Jednak nie do każdej ofiary używane były wszystkie moduły. Napastnicy instalowali tylko potrzebne komponenty. Na wielu zainfekowanych maszynach najpierw umieszczany był początkowy zestaw zajmujący 6 MB i obejmujący tylną furtkę, za pomocą której napastnicy mogli swobodnie instalować nowe moduły szpiegowskie z serwera C&C[5].

Także infrastruktura wspomagająca Flame'a była rozbudowana i nie przypominała niczego, co badacze wcześniej napotkali. Naliczono przynajmniej 80 domen działających jako serwery C&C w Niemczech, Holandii, Szwajcarii i innych krajach. Napastnicy kontrolowali przy ich użyciu zainfekowane maszyny i pobierali wykradzione dokumenty[6]. Tak duża liczba domen zapewne miała pomóc w niezależnym zarządzaniu różnymi operacjami i grupami ofiar.

Napastnicy do rejestrowania domen posługiwali się fałszywymi nazwiskami: Ivan Blix, Paolo Calzaretta, Traian Lucescu. Ponadto w niektórych transakcjach używali kart kredytowych typu prepaid, aby nie można ich było wyśledzić. Badacze z Kaspersky'ego przekierowali ruch z ok. 30 takich domen do kontrolowanego przez siebie ujścia. Wkrótce po jego

[5] W większości zainfekowanych maszyn zainstalowana była wersja zajmująca 6 MB. Badacze znaleźli też mniejsze zestawy, zajmujące ok. 900 kB i pozbawione dodatkowych modułów. Mniejszy pakiet mógł służyć do infekowania maszyn z użyciem wolniejszych połączeń, ponieważ zdalne instalowanie modułu o wielkości 6 MB w krajach z wolnymi i niestabilnymi łączami internetowymi trwałoby zbyt długo.

[6] Plik konfiguracyjny złośliwego oprogramowania zawierał listę pięciu domen statycznych (w tym *traffic-spot.biz*, *dailynewsupdater.com* i *bannezone.in*), a także inną listę, którą napastnicy mogli modyfikować po dodaniu nowych serwerów C&C.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

skonfigurowaniu zaczęły komunikować się z nim maszyny z Iranu i innych państw. Napłynęły wykradzione pliki przeznaczone dla napastników, choć były one zaszyfrowane, dlatego badacze nie potrafili stwierdzić, jakie dane są wykradane.

Po dodaniu sygnatur Flame'a do narzędzi antywirusowych Kaspersky'ego okazało się, że zainfekowanych jest kilkaset maszyn. Nie było zaskoczeniem, że najwięcej z nich miało lokalizację w Iranie. Było ich przynajmniej 189. Ponadto 98 ofiar znajdowało się na terytoriach palestyńskich, a po ok. 30 w Sudanie i Syrii.

W czasie gdy Kaspersky wciąż jeszcze badał moduły Flame'a, Bencsáth skontaktował się z Raiu w sprawie przesłanego Węgrowi podejrzanego pliku znalezionego w Iranie. Badacze dobrze poznali się w trakcie prac nad Duqu, dlatego nie było niczym niezwykłym, że Bencsáth napisał do Raiu. Plik z Iranu okazał się jednym z modułów analizowanych już przez Raiu i jego zespół. Bencsáth przesłał plik także do Chiena z Symanteca, która to firma równolegle z Kasperskym zaczęła badać zagrożenie. Gdy badacze z Symanteca dodali do swojego silnika antywirusowego odpowiednie sygnatury, wykryli kolejne ofiary w Austrii, Libanie, Rosji, Zjednoczonych Emiratach Arabskich, Hongkongu i na Węgrzech.

Ostatecznie znaleziono ponad 1000 ofiar — znacznie więcej niż 36 znanych włamań z użyciem Duqu i zdecydowanie mniej niż ponad 100 tys. maszyn zainfekowanych przez Stuxneta. Wynikało to z tego, że Flame (w odróżnieniu od Stuxneta) nie potrafił się automatycznie rozprzestrzeniać. Odbywało się to tylko na polecenie napastników. Dlatego choć większość infekcji Stuxnetem dotyczyła przypadkowych maszyn, to wszystkie ofiary Flame'a były prawdopodobnie wybranymi celami. Raiu podejrzewał, że ofiary były atakowane w grupach stosownie do misji, którą napastnicy w danym czasie przeprowadzali.

W doborze ofiar nie było widać wzorca. Flame atakował pojedyncze osoby, firmy prywatne, agencje rządowe i uczelnie. Łatwo jednak było dostrzec, na jakiego rodzaju plikach zależy napastnikom. Flame zawierał listę rozszerzeń szukanych plików. Zawierała ona dokumenty Worda, prezentacje w PowerPoincie i pliki Excela. Wysoko na liście znajdowały się również rysunki z AutoCAD-a, uwzględniane także przez Duqu. Flame, co ważne, służył też do zdobywania certyfikatów cyfrowych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Choć Flame obejmował długą listę szukanych plików, nie wykradał wszystkich znalezionych dokumentów. Zamiast tego pobierał z każdego pliku 1 kB tekstu i przesyłał ten fragment na jeden z serwerów C&C. Stamtąd dane trafiały prawdopodobnie w inne miejsce. Raiu podejrzewał, że napastnicy używali superkomputera do filtrowania wszystkich nadsyłanych fragmentów tekstu i ustalania, które pliki warto pobrać w całości. Rok później, gdy opublikowane zostały ujawnione przez Edwarda Snowdena dokumenty z NSA, znalazł się w nich opis systemu TURBINE o bardzo podobnym przeznaczeniu (zob. s. 228).

Ponieważ Flame związany był z tak rozbudowaną operacją, było zrozumiałe, że atak trwał od długiego czasu. Pierwsza odkryta infekcja nastąpiła w Europie w grudniu 2007 r.[7]. Maszyna w Dubaju została zaatakowana w kwietniu 2008 r. W tym czasie zarejestrowane zostały też niektóre z domen używanych przez napastników dla serwerów C&C. W latach 2009 i 2010 zarejestrowano kilka innych domen, jednak większość z nich pochodziła z 2011 r., z czasu po ujawnieniu Stuxneta. Wszystko to oznaczało, że Flame infekował systemy przynajmniej od pięciu lat i był aktywny w czasie tworzenia i stosowania Stuxneta oraz Duqu.

Wyłaniał się z tego jasny obraz cyfrowego arsenału wypełnionego narzędziami szpiegowskimi i bronią opracowaną do ataku nie tylko na irański program nuklearny, ale też na inne cele. Do tworzenia wykrytego do tego czasu szkodliwego kodu służyły dwie platformy. Jedną z nich była platforma Flame'a. Na jej podstawie powstało rozbudowane narzędzie szpiegowskie. Drugą była platforma Tilde-d, która posłużyła do zbudowania Duqu. Platforma Flame'a była dużo bardziej zaawansowana i złożona od Tilde-d, dlatego prawdopodobnie obie były budowane równolegle przez różne zespoły. Obie platformy posłużyły jednak na różnych etapach do prac nad Stuxnetem.

Raiu podejrzewał, że budowanie Flame'a rozpoczęto w 2005 lub 2006 r. Wynikało to z tego, że fragmenty kodu napisane przez napastników dla

[7] W przypadku Flame'a napastnicy zachowali większą ostrożność i zmienili w plikach znaczniki czasu, aby uniemożliwić badaczom określenie dat ich powstania. Choć niektóre daty wydawały się poprawne, inne wskazywały, że pliki zostały skompilowane w latach 1994 i 1995, co było niemożliwe, ponieważ w kodzie używane były biblioteki utworzone dopiero w 2010 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

serwerów C&C powstały w grudniu 2006 r.[8]. Narzędzie szpiegowskie stało się dojrzałe zapewne na początku 2007 r. Pierwsze znane daty z Duqu pochodziły z sierpnia 2007 r., kiedy to skompilowany został jeden z dropperów, i z listopada 2008 r., kiedy odnotowano pierwsze oznaki użycia programu do wykradania danych.

Raiu uważał, że w momencie rozpoczęcia prac nad Stuxnetem napastnicy użyli Flame'a do szybkiego zbudowania tej cyfrowej broni, a w późniejszych wersjach ataku przerzucili się na platformę Duqu. Badacz opierał swoje wnioski częściowo na tym, że znaleziony w wersji Stuxneta z 2009 r. (używającej mechanizmu automatycznego uruchamiania i eksploita mechanizmu obsługi tapet) zasób 207 przypominał wczesną wersję głównego modułu Flame'a. Flame w 2007 r. był już gotowy jako podstawowe narzędzie szpiegowskie i wyglądało na to, że gdy w 2009 r. napastnicy przystąpili do pisania pocisku Stuxneta, zespół rozwijający Flame'a udostępnił kod źródłowy zasobu 207 grupie pracującej nad Stuxnetem. Dzięki temu można było szybciej napisać kod pocisku. Do tego czasu ładunek był już gotowy, a napastnicy potrzebowali jedynie czegoś do jego dostarczenia. „Zapewne napastnicy musieli pilnie go [Stuxneta] uruchomić, dlatego wzięli już gotową wtyczkę z Flame'a i wykorzystali ją w Stuxnecie" — powiedział Raiu.

Jednak później prace nad oboma narzędziami przebiegały niezależnie. Programiści Flame'a rozbudowywali platformę do postaci potężnego narzędzia szpiegowskiego, a gdy w 2010 r. twórcy Stuxneta przygotowywali następną wersję kodu na potrzeby późniejszego ataku, zastosowali platformę Tilde-d (użytą do zbudowania Duqu) w celu zmodyfikowania pocisku. Zmiana platformy na Tilde-d wynikała zapewne z tego, że pocisk z wersji Stuxneta z 2010 r., z wieloma eksploitami typu zero-day i dodatkowymi mechanizmami rozprzestrzeniania, był znacznie bardziej skomplikowany i wymagał więcej kodu. Platforma Tilde-d była znacznie prostszym i bardziej zwięzłym narzędziem.

Kolejność zdarzeń ustalona przez Raiu i jego zespół była zgodna ze scenariuszem opisanym przez Davida Sangera, dziennikarza „New York Timesa". Sanger w książce *Confront and Conceal*, cytując obecnych i byłych

[8] W kodzie serwera znajdował się wiersz wstawiony przez programistów w celu określenia autorów i daty utworzenia pliku. Oto ten wiersz: „@author OCTOPUS in 12/3/2006; @author DeMO (modifications)". Te nazwy są zapewne pseudonimami osób lub zespołów konfigurujących serwery.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

urzędników rządowych, napisał, że pierwsze wersje Stuxneta zostały opracowane przez Stany Zjednoczone, natomiast późniejsze powstały we współpracy Stanów z Izraelem. Raiu sądził, że Flame i powiązana z nim platforma zostały zbudowane przez Stany Zjednoczone, a Izrael stworzył Duqu i platformę Tilde-d. Obie strony używały potem swoich platform do tworzenia fragmentów Stuxneta.

Niezależnie od tego, jaka była rola Flame'a w powstaniu Stuxneta, cała operacja szpiegowska załamała się 28 maja 2012 r., kiedy to firmy Kaspersky i Symantec upubliczniły swoje odkrycia w ogłoszonych niemal jednocześnie komunikatach[9]. Gdy wieści o narzędziu szpiegowskim się rozniosły, operatorzy Flame'a zareagowali błyskawicznie. W ciągu godziny od publikacji pierwszych informacji serwery C&C tego narzędzia stały się nieaktywne, ponieważ napastnicy je wyłączyli. W ciągu minut zakończyli w ten sposób niezwykle udaną pięcioletnią kampanię szpiegowską. Wyglądało to prawie tak, jakby czekali na pojawienie się wiadomości o tej operacji.

Nastąpił koniec sukcesów Flame'a, ale pozostały efekty jego działania. W jakiś czas po wyłączeniu serwerów Flame'a Microsoft poinformował, że odkrył jeszcze bardziej niepokojące aspekty ataku, przeoczone przez badaczy Kaspersky'ego i Symanteca.

GDY UJAWNIONO WIADOMOŚCI dotyczące Flame'a, Amerykanie obchodzili święto Memorial Day, dlatego w siedzibie głównej Microsoftu w Redmond w stanie Waszyngton pracowało niewiele osób. Jednak gdy inżynierowie z centrum reagowania na zagrożenia dowiedzieli się o odkryciu nowego ataku przypisywanego zespołowi stojącemu za Stuxnetem i Duqu,

[9] Kaspersky badał uzyskane pliki Flame'a, natomiast Symantec analizował pliki od Bencsátha oraz inne moduły z maszyn klientów otrzymane po dodaniu odpowiednich sygnatur do narzędzi antywirusowych. Zespoły nie komunikowały się ze sobą na temat prowadzonych prac, choć tajnymi kanałami dowiedziały się, że konkurencja pracuje nad kodem. Gdy badacze z Symanteca ustalili, że analitycy z Kaspersky'ego planują opublikować efekty prac w święto Memorial Day, zmobilizowali się do szybkiego zakończenia badań, aby móc opublikować je tego samego dnia. Obie firmy niezależnie (najpierw Kaspersky, później Symantec) skontaktowały się z autorką książki przed wydaniem komunikatów. Zob. Kim Zetter, „Meet Flame, the Massive Spy Malware Infiltrating Iranian Computers", *Wired.com*, 28 maja 2012 (*https://www.wired.com/2012/05/flame*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

natychmiast zabrali się za udostępnione przez badaczy pliki Flame'a. Chcieli zobaczyć, czy w nowym ataku wykorzystano luki typu zero-day z systemu Windows, tak jak w Stuxnecie i Duqu. Gdy przeanalizowali jeden z otrzymanych plików, zdali sobie sprawę, że zetknęli się z czymś znacznie gorszym niż eksploity typu zero-day. Flame przeprowadzał zaawansowany atak na część systemu aktualizacji Windows Update, aby rozprzestrzeniać się między maszynami w sieci lokalnej.

Windows Update to automatyczny system używany przez Microsoft do rozsyłania aktualizacji oprogramowania i łatek do milionów klientów. W celu pobierania aktualizacji na każdym komputerze działa narzędzie klienckie, które kontaktuje się z serwerami Microsoftu, aby wczytać łatki po ich udostępnieniu.

Przez lata społeczność zajmująca się zabezpieczeniami ostrzegała przed katastrofą, jaka może się wydarzyć, jeśli hakerzy przejmą system Windows Update i zaczną przesyłać przy jego użyciu szkodliwy kod, zagrażając w ten sposób bezpieczeństwu milionów użytkowników Windowsa. Flame nie osiągnął tego poziomu, ale był równie niebezpieczny. Zamiast opanowywać serwery Microsoftu dostarczające aktualizacje Windowsa do milionów maszyn, przejmował narzędzie Windows Update z komputerów użytkowników. Była to subtelna, ale ważna różnica. Gdyby napastnicy przejęli serwery Microsoftu, mogliby manipulować maszynami na skalę globalną. Jednak przeprowadzona operacja pozwalała im atakować maszyny tylko w konkretnych docelowych sieciach bez wpływu na inne komputery.

Narzędzie do aktualizacji, podobnie jak sam system Windows, jest okresowo aktualizowane przez Microsoft. Za każdym razem, gdy narzędzie to jest uruchamiane na komputerze użytkownika, przesyła na serwery Microsoftu sygnał, aby sprawdzić, czy istnieje nowsza wersja tego oprogramowania. Microsoft rozsyła aktualizacje w plikach .CAB podpisanych certyfikatem tej firmy w celu udowodnienia ich legalności.

By opanować ten proces, napastnicy najpierw infekowali jedną maszynę w sieci ofiary Flame'em. Następnie, gdy program aktualizujący z innego komputera z tej sieci wysyłał sygnał na serwery Microsoftu w celu sprawdzenia dostępności aktualizacji narzędzia Windows Update, zainfekowana maszyna przechwytywała sygnał i odsyłała szkodliwy plik Flame'a zamaskowany jako poprawny plik .CAB Microsoftu. W ten sposób nowa maszyna była infekowana narzędziem szpiegowskim. Ale nie to było najbardziej

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

zaawansowanym aspektem ataku. Aby przeprowadzić operację, napastnicy podpisywali szkodliwy plik .CAB poprawnym certyfikatem Microsoftu. Jednak certyfikat ten należał do firmy MS, a nie — jak powinien — do Microsoft Corporation. Gdy badacze w Microsofcie to zobaczyli, od razu podejrzewali, że coś jest nie tak. Wyglądało na to, że certyfikat został wydany i podpisany przez system Terminal Services Licensing Certificate Authority Microsoftu w lutym 2010 r. Certyfikat był jednak fałszywy, a system nie powinien go wygenerować i podpisać. Czy serwer Microsoftu został przejęty? A może ktoś wykradł klucz do podpisywania certyfikatów? By nikt nie mógł powtórzyć podobnej operacji, inżynierowie musieli szybko ustalić, w jaki sposób napastnicy zdobyli certyfikat. Ściągnęli wszystkie osoby, które mogły pracować w święto, i szybko stworzyli zespół.

Okazało się, że napastnicy zastosowali „kolizję" skrótów MD5. Skrót MD5 to kryptograficzna reprezentacja danych (tu chodziło o dane z certyfikatu) wygenerowana za pomocą algorytmu MD5. Skróty mają pełnić funkcję odcisku palca, dlatego dane przekazane do tego algorytmu powinny dawać unikatowy skrót. Po zmodyfikowaniu danych algorytm powinien wygenerować inny skrót. Tymczasem już przed laty okazało się, że algorytm MD5 ma słaby punkt umożliwiający utworzenie tego samego skrótu na podstawie różnych zbiorów danych[10]. Jest to tzw. kolizja skrótów. Z tego powodu wiele firm zrezygnowało ze stosowania algorytmu MD5. Jednak Microsoft na serwerze Terminal Service (TS) Licensing nie zmieniał algorytmu od 1999 r., czyli od czasu opracowania tego systemu.

TS Licensing to system używany przez korporacyjnych klientów Microsoftu w czasie konfigurowania serwera z oprogramowaniem tej firmy, z którego korzystać ma wiele osób lub komputerów. Klient kupuje od Microsoftu licencje, np. 100 licencji dla 100 pracowników lub maszyn, a następnie przesyła żądanie certyfikatu do systemu TS Licensing Certificate Authority Microsoftu. Ten system generuje certyfikat z nazwą klienta i znacznikiem czasu określającym moment wydania certyfikatu oraz numerem seryjnym tego cyfrowego dokumentu.

Gdy Microsoft wydaje certyfikat, przekazuje wszystkie dostępne w nim dane (w tym znacznik czasu i numer seryjny) do algorytmu MD5, aby utworzyć skrót. Następnie podpisuje skrót i przesyła certyfikat klientowi.

[10] O tym słabym punkcie wiedziano przynajmniej od 2004 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Klient może wtedy posłużyć się podpisanym certyfikatem, aby zagwarantować, że tylko uprawnione komputery lub osoby będą mogły korzystać z oprogramowania z licencją Microsoftu. Jednak napastnicy wykorzystali skrót od Microsoftu do podpisania fałszywego certyfikatu i szkodliwych plików .CAB.

Zanim napastnicy wysłali do Microsoftu prośbę o certyfikat, przygotowali fałszywy certyfikat z informacjami, jakie wedle ich przewidywań powinien zawierać prawdziwy certyfikat Microsoftu. Wprowadzili jednak kilka drobnych zmian, które miały gwarantować uzyskanie skrótu takiego samego jak w certyfikacie wydanym przez Microsoft. Nie było to łatwe. Konieczne było m.in. uruchomienie algorytmu MD5 dla tysięcy różnych wersji danych z fałszywego certyfikatu, aby uzyskać taki sam skrót jak w prawdziwym certyfikacie z Microsoftu zawierającym inne dane. Zadanie to wymagało dużych mocy obliczeniowych. Niezbędne było też przewidzenie numeru seryjnego przypisanego przez Microsoft certyfikatowi i dokładnego czasu podpisania prawdziwego certyfikatu przez serwer licencyjny (znacznik czasu i numer seryjny były używane do wygenerowania skrótu podpisywanego przez Microsoft)[11]. Gdyby napastnicy pomylili się choć o milisekundę, nie mogliby zastosować podpisanego skrótu w fałszywym certyfikacie, ponieważ skróty byłyby niezgodne[12]. Musieli więc dobrze zbadać

[11] Certyfikaty są zwykle generowane i podpisywane w ciągu sekund od zgłoszenia żądania do Microsoftu. Napastnicy mogli zmierzyć, ile czasu zajmuje Microsoftowi wydanie podpisanych certyfikatów, przesyłając serię takich żądań w celu wykrycia wzorca. Były pracownik Microsoftu zasugerował, że mogli też zająć pozycję w wewnętrznej sieci Microsoftu i obserwować nadchodzące żądania, aby stwierdzić, ile dokładnie czasu trwa przesyłanie i przetwarzanie żądań. Nie ma jednak dowodów, że tak właśnie było.

[12] Oprócz opisanych czynności napastnicy musieli też zmodyfikować certyfikat na potrzeby instalacji złośliwego oprogramowania w komputerach z systemem Windows Vista, ponieważ w pierwotnej postaci certyfikat nie był akceptowany przez żaden komputer z systemem Vista lub nowszym. Ta modyfikacja polegała na pozbyciu się rozszerzenia certyfikatu. Napastnicy nie usunęli rozszerzenia, ponieważ mogło to spowodować niepowodzenie procesu sprawdzania podpisu. Zamiast tego „wykomentowali" fragment certyfikatu — umieścili go w znacznikach, aby komputer zignorował rozszerzenie. Dzięki temu technika mogła działać w maszynach z systemem Vista. Jednak Vista była zainstalowana tylko w 5% zainfekowanych Flame'em komputerów, na jakie natrafił Kaspersky. W większości maszyn używane były systemy Windows 7 i Windows XP.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

system Microsoftu i przetestować wiele certyfikatów (zapewne setki), aby ustalić odpowiedni czas i numer seryjny[13].

Atakujący zastosowali później podpisany skrót z fałszywym certyfikatem do podpisania szkodliwych plików .CAB. Certyfikat wydawał się prawdziwy, ponieważ zawierał podpisany skrót wygenerowany przez Microsoft.

Przejęcie funkcji Windows Update było fantastyczną operacją, która przesuwała granice matematyki i mogła zostać przeprowadzona tylko przez światowej klasy kryptografów[14]. Gdy badacze z Kaspersky'ego się o niej dowiedzieli, nazwali ją eksploitem w trybie boga, ponieważ była bardzo pomysłowa pod względem technicznym i dawała znacznie większe możliwości w zakresie rozprzestrzeniania oprogramowania niż eksploity typu zero-day[15]. Aby przeprowadzić atak dający większe możliwości i bardziej niebezpieczny, napastnicy musieliby opanować same serwery systemu Windows Update.

---

[13] Według źródeł Microsoft próbował zbadać, kto zgłaszał żądania i ile żądań certyfikatu zostało przesłanych od danej jednostki. Niestety, między wydaniem certyfikatu (luty 2010 r.) a wykryciem Flame'a (2012 r.) minęło zbyt dużo czasu. Dzienniki Microsoftu są z czasem zastępowane i pliki z opisywanego okresu nie były już dostępne.

[14] Holenderski kryptograf i naukowiec Marc Stevens, który w 2007 r. wraz ze współpracownikiem Bennem de Wegerem przygotował w celach badawczych jeden z pierwszych praktycznych ataków z wykorzystaniem „kolizji" skrótów MD5, opisał atak z Flame'a jako „kryptoanalizę na poziomie światowym", odkrywającą nowe obszary i wykraczającą ponad to, co z kolizjami robił Stevens i inni. Stevens i de Weger byli częścią grupy badawczej (obejmującej też Aleksandra Sotirowa), która w 2008 r. zademonstrowała podobny, choć różniący się technicznie atak z wykorzystaniem „kolizji" w czasie Kongresu Klubu Komputerowego Chaos. Jest to coroczna konferencja hakerska odbywająca się w Niemczech. Badacze do obliczeń zastosowali klaster 200 urządzeń PlayStation 3, aby uzyskać identyczny skrót certyfikatu. Ich certyfikat miał pochodzić od innej firmy, nie od Microsoftu. W trakcie eksperymentu badacze kilkakrotnie dobierali zły znacznik czasu, dlatego musieli wygenerować skrót cztery razy przed uzyskaniem właściwej wartości. Gdy w 2012 r. wykryto Flame'a, Sotirow oszacował, że atak ten był 10 do 100 razy trudniejszy niż operacja przeprowadzona przez niego i współpracowników. Slajdy z prezentacji Sotirowa i innych znajdziesz na stronie: *https://events.ccc.de/congress/2008/Fahrplan/attachments/1251_md5-collisions-1.0.pdf*.

[15] Warto zauważyć, że nawet po wykonaniu tak ciężkiej pracy w celu uzyskania fałszywego certyfikatu napastnicy nie powinni mieć możliwości posłużenia się nim do podpisywania szkodliwego kodu. Udało im się to jednak zrobić, ponieważ Microsoft nie zaimplementował pewnych ograniczeń, dzięki którym certyfikaty wydawane dla TS Licensing byłyby przeznaczone tylko na potrzeby licencjonowania oprogramowania.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Inżynierowie z Microsoftu początkowo oszacowali, że innym napastnikom z odpowiednimi zasobami dowiedzenie się wszystkiego na temat certyfikatów Microsoftu i systemu aktualizacji, co jest potrzebne do przeprowadzenia podobnego ataku, zajmie tylko 12 dni. Jednak gdy przeprowadzili testy i wykonali wszystkie kroki potrzebne do skopiowania przejęcia funkcji Windows Update, zdali sobie sprawę, że mniej zaawansowaną wersję ataku (niewymagającą kolizji skrótów MD5) napastnicy będą mogli zastosować już za trzy dni[16].

Pracując pod presją czasu, Microsoft szybko przygotował poza kolejką łatkę eliminującą luki umożliwiające przeprowadzenie takich ataków. Firma w całym 2011 r. wypuściła tylko jedną łatkę poza kolejką. Takie łatki były przygotowywane wyłącznie dla najistotniejszych luk, co było dowodem na to, jak poważnie Microsoft traktował eksploit z Flame'a.

Twórcy Duqu i Stuxneta uderzyli już w podstawy systemu sprawdzania poprawności, dzięki któremu mógł funkcjonować internet. Najpierw ukradli pojedyncze certyfikaty z tajwańskich firm, aby podpisać sterowniki Stuxneta, a następnie wysłali Duqu, by wykradał dane z samych jednostek certyfikacyjnych. Jednak ten eksploit poszedł jeszcze o krok dalej, naruszając zaufanie między największym na świecie producentem oprogramowania a jego klientami. Przy założeniu, że napastnikami byli Amerykanie, prawdopodobnie usprawiedliwili oni tę operację i zyskali dla niej prawną akceptację, twierdząc, że nie atakują samych serwerów systemu Windows (co narażałoby na ryzyko wszystkich klientów Microsoftu), a jedynie przejmują program kliencki w systemach Windows na komputerach pojedynczych użytkowników. W ten sposób mogli przeprowadzić ataki tylko na ofiary i maszyny spoza Stanów[17].

---

[16] Ten prostszy certyfikat umożliwiał złośliwemu oprogramowaniu atak na komputery z systemem Windows XP, ale już nie na maszyny z systemem Windows Vista, który miał lepsze zabezpieczenia.

[17] Można jednak uznać, że ten atak był jeszcze gorszy niż przejęcie serwerów funkcji Windows Update w celu rozsyłania szkodliwego oprogramowania. Po przejęciu serwerów napastnicy wprawdzie mogli przesyłać z nich szkodliwe oprogramowanie do użytkowników, ale komputery klientów odrzucałyby kod niepodpisany przez Microsoft. Dzięki wykorzystaniu certyfikatów Microsoftu do podpisywania swojego szkodliwego kodu napastnicy nie potrzebowali serwerów funkcji Windows Update. Mogli przesyłać złośliwe oprogramowanie na komputery użytkowników z dowolnych serwerów i przekazywać swoje pliki jako poprawny kod Microsoftu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak ostatecznie to, że napastnicy nie przejęli serwerów Microsoftu, miało niewielkie znaczenie. Atak na program kliencki odpowiedzialny za aktualizacje wystarczał, aby wzbudzić w użytkownikach brak zaufania do bezpieczeństwa usługi aktualizacji. Mogło to skutkować wyłączeniem tej usługi i zakończeniem otrzymywania aktualizacji krytycznych dla bezpieczeństwa ich systemów.

Kto *odpowiadał* za naruszenie zaufania między Microsoftem a jego klientami? Mniej więcej trzy tygodnie po tym, jak Flame został ujawniony, do operacji przyznali się byli amerykańscy urzędnicy rządowi, którzy poinformowali „Washington Post", że Flame był wspólną akcją NSA, CIA i armii izraelskiej[18].

Według anonimowego informatora Flame został opracowany mniej więcej w 2007 r., co potwierdzało ogólne ramy czasowe wyznaczone przez Raiu i jego zespół. Miał służyć do zbierania danych o urzędnikach irańskich i tworzenia map systemów komputerowych będących częścią irańskiego programu nuklearnego. Urzędnicy stwierdzili też, że Flame był narzędziem wczesnych generacji i został wyparty przez inne rozwiązania.

„Chodzi o przygotowanie pola bitwy pod innego rodzaju utajnione akcje" — powiedział były pracownik amerykańskiego wywiadu gazecie, dodając, że proces zbierania danych o irańskim programie „był znacznie bardziej zaawansowany niż to, co odkryto". Możliwe, że miał na myśli rzeczy takie jak implanty używane przez NSA do przesyłania falami radiowymi danych wykradzionych z zainfekowanych maszyn (zob. s. 321).

Informatorzy gazety „Post" wyjaśnili też zagadkę przeprowadzonego wcześniej tego roku ataku Wipera na Iran. Powiedzieli gazecie, że ten atak, który wykasował dyski twarde na komputerach irańskiego ministerstwa ds. ropy naftowej i doprowadził do wykrycia Flame'a, także został przeprowadzony przez jednostki rządowe. Jednak pewien informator stwierdził, że Wiper był akcją przeprowadzoną przez samych Izraelczyków (w odróżnieniu od Flame'a i Stuxneta, które były wspólnymi operacjami Izraela i Stanów Zjednoczonych). Jeden z urzędników powiedział „Postowi", że Stany Zjednoczone były zaskoczone tym niszczycielskim atakiem.

[18] Ellen Nakashima, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, „Washington Post", 19 czerwca 2012.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

REWELACJE NA TEMAT ataków prowadzonych przez jednostki rządowe pojawiały się teraz bardzo szybko. Po latach ukrytej działalności ujawniano jedną operację po drugiej. A nie był to jeszcze koniec. Badacze z Kaspersky'ego wkrótce mieli znaleźć dowody na to, że wciąż działa *więcej* szkodliwych narzędzi opracowanych przez te same zespoły.

Przełom nastąpił, gdy badacze uzyskali dostęp do serwerów C&C używanych przez Flame'a. Okazało się, że dziesięć dni przed ujawnieniem informacji o tej operacji napastnicy rozpoczęli intensywną akcję kasowania danych, aby zatrzeć tropy i usunąć z serwerów wszelkie ślady aktywności. Sugerowało to, że już wcześniej wiedzieli, że operacja zostanie ujawniona[19]. Popełnili jednak poważny błąd, pozostawiając w Malezji serwer z dużą ilością nietkniętych informacji. Kilka tygodni przed operacją porządkową napastnicy nieostrożnie zmienili ustawienia serwera i przypadkowo zablokowali sobie dostęp do niego. W efekcie nie mogli na niego wrócić, by usunąć

[19] W Duqu napastnicy przeprowadzili operację usuwania danych *po* ujawnieniu informacji o tym oprogramowaniu. Jednak ponieważ twórcy Flame'a rozpoczęli akcję dziesięć dni przed pojawieniem się wiadomości w mediach, przypuszczalnie już wcześniej wiedzieli, że zostaną ujawnieni. Badacze z Kaspersky'ego prawdopodobnie przypadkowo ostrzegli napastników, gdy podłączyli do internetu maszynę testową zainfekowaną Flame'em. Gdy tylko maszyna rozpoczęła pracę, złośliwe oprogramowanie skontaktowało się z jednym z serwerów C&C Flame'a. Napastnicy musieli zdać sobie sprawę, że danej maszyny nie było na liście celów. Możliwe, że zidentyfikowali ją nawet jako komputer Kaspersky'ego i doszli do wniosku, że czas Flame'a się kończy. Dlatego w panice usunęli dane z serwerów C&C oraz wysłali na zainfekowane maszyny moduł porządkowy Browse32, aby wykasować wszelkie ślady złośliwego oprogramowania. Dzięki temu ofiary miały nigdy nie dowiedzieć się, że zostały zaatakowane. Operacja porządkowa w większości zakończyła się powodzeniem. Jednak Browse32 miał poważną wadę — pominął jeden charakterystyczny plik, *~DEB93D.tmp*, który wydał całą operację. Był to plik tymczasowy tworzony, gdy Flame wykonywał na zainfekowanej maszynie różne operacje. Po zakończeniu operacji Flame powinien automatycznie usuwać ten plik. Dlatego napastnicy nie umieścili go na liście plików przeznaczonych do usunięcia przez Browse32 — nie spodziewali się, że plik ten będzie znajdował się na komputerach. Jednak gdy moduł porządkowy Browse32 trafiał do komputera, w którym Flame wciąż jeszcze wykonywał jedną z operacji generujących wspomniany plik tymczasowy, moduł usuwał Flame'a, zanim ten zdążył skasować ów plik. Badacze z Kaspersky'ego znaleźli osierocony plik tymczasowy w setkach systemów zainfekowanych Flame'em. To ten plik pozostawiony na maszynie w Iranie doprowadził do tego, że w ogóle natrafili na Flame'a.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

z niego dane. Dzięki temu badacze z Kaspersky'ego uzyskali mnóstwo materiału do analiz[20].

Nietknięty pozostał panel sterowania używany przez napastników do przesyłania modułów Flame'a do zainfekowanych maszyn i przetwarzania wykradzionych danych. Ten panel przypominał biznesową platformę publikacyjną NewsforYou, dlatego gdyby ktoś z zewnątrz uzyskał dostęp do serwera, myślałby, że należy on do gazety lub firmy mediowej. Szkodliwe moduły, które napastnicy planowali zainstalować na maszynach ofiar, były przechowywane w katalogach o nazwach *News* i *Ads*, natomiast w katalogu *Entries* znajdowały się dane i pliki wykradzione z komputerów.

Badacze z Kaspersky'ego znaleźli też dzienniki z listą adresów IP wszystkich zainfekowanych maszyn, które kontaktowały się z danym serwerem. Ten serwer został uruchomiony niedawno, 25 marca, jednak w czasie dziesięciu dni jego działania komunikowało się z nim przynajmniej 5377 maszyn z kilkudziesięciu państw. Około 3700 komputerów pochodziło z Iranu, a następnych 1280 pracowało w Sudanie. W innych krajach odnotowano mniej niż 100 infekcji.

Raiu i jego zespół zdali sobie sprawę, że jeśli tylko jeden serwer C&C (z ponad 80 zarejestrowanych przez napastników) w krótkim okresie 10 dni skontaktował się z 5000 maszyn, a opisywane złośliwe oprogramowanie działało od 2007 lub 2008 r., to łączna liczba ofiar musiała być o kilkadziesiąt tysięcy wyższa od początkowych założeń. Ponadto badacze znaleźli na

[20] Nie był to jedyny błąd napastników. Nieudana była też operacja porządkowania serwerów, do których mieli dostęp. Napastnicy utworzyli skrypt *LogWiper.sh* do wykasowania dzienników aktywności na serwerach, aby uniemożliwić zbadanie wykonywanych na nich działań. Skrypt po zakończeniu pracy miał usuwać sam siebie (tak jak wąż Uroboros zjadający swój ogon). Jednak napastnicy w instrukcji usuwania podali niewłaściwą nazwę pliku. Zamiast nakazywać skryptowi skasowanie pliku *LogWiper.sh*, wskazali plik *logging.sh*. Dlatego skrypt LogWiper nie potrafił znaleźć sam siebie i pozostał na serwerach, gdzie mogli go znaleźć badacze z Kaspersky'ego. Napastnicy pozostawili też imiona lub pseudonimy programistów, którzy napisali skrypty i opracowali algorytmy szyfrowania oraz inną infrastrukturę Flame'a. Imiona pojawiały się w kodzie źródłowym niektórych narzędzi. Był to błąd, jaki mogli popełnić niedoświadczeni hakerzy. Dlatego badacze byli zaskoczeni, natykając się na nie w operacji prowadzonej przez państwo. Jeden z hakerów, Hikaru, był zapewne liderem zespołu i utworzył dużą część kodu serwera, w tym zaawansowane mechanizmy szyfrowania. Raiu nazwał go mistrzem szyfrowania. Nad częścią skryptów pracował też ktoś o imieniu Ryan.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

malezyjskim serwerze plik z 5,7 GB danych wykradzionych z maszyn ofiar w 10 dni. Skoro napastnicy potrafili w jedyne dziesięć dni pobrać takie ilości danych, Raiu podejrzewał, że ich łączna zdobycz z ponad pięciu lat pracy Flame'a musiała być liczona w terabajtach[21].

Wszystkie te rewelacje zbladły w obliczu innych dowodów, jakie pozostawili po sobie inżynierowie Flame'a. Wynikało z nich, że malezyjski serwer komunikował się nie z jednym rodzajem złośliwego oprogramowania, ale z *czterema*. Napastnicy nazwali je: SP, SPE, FL i IP. Zostały one utworzone w tej właśnie kolejności (SP było najstarsze). Każde miało komunikować się z serwerem C&C z użyciem innego niestandardowego protokołu opracowanego przez napastników[22].

FL dotyczyło Flame'a, natomiast trzy pozostałe nazwy były tajemnicą. Badacze z Kaspersky'ego wiedzieli z pewnością, że SPE istnieje, ponieważ widzieli już dowody jego działania. Gdy utworzyli ujście do przechwytywania danych kierowanych na serwery Flame'a, ok. 90 maszyn z Libanu, Iranu i Francji zainfekowanych kodem SPE tysiące razy próbowało

[21] Napastnicy najwyraźniej prowadzili projekt jak ściśle kontrolowaną operację wojskową z wieloma zespołami wykonującymi starannie rozdzielone zadania. Musiała istnieć grupa zarządzająca, która nadzorowała operację i wybierała cele. Byli też programiści, którzy tworzyli moduły Flame'a, oraz zespół od serwerów C&C, odpowiedzialny za ich przygotowanie i obsługę, przesyłanie modułów Flame'a na zainfekowane maszyny oraz pobieranie wykradzionych danych. Istniał też zespół wywiadu, analizujący zdobyte informacje i zgłaszający żądania dodatkowych plików z maszyn, które zawierały cenne dane. Był to dokładnie taki układ, jaki — według dokumentów ujawnionych przez Snowdena — funkcjonował w NSA. Zespół zarządzający serwerami C&C miał ograniczony wgląd w całą operację. Możliwe, że nie znał nawet prawdziwej natury misji, jakiej służyła ich praca. Proces przesyłania nowych modułów na zainfekowane maszyny był ściśle kontrolowany. Dlatego ani wspomniany zespół, ani żadni nie ludzie z zewnątrz, którzy zdołaliby uzyskać dostęp do serwerów, nie mogli modyfikować modułów ani tworzyć nowych i przesyłać ich na zainfekowane komputery. Moduły były m.in. przekazywane w gotowej postaci na serwer, gdzie system je przetwarzał i umieszczał w katalogu, aby zespół mógł dostarczyć plik do ofiary. Operator musiał tylko wcisnąć przycisk, by przesłać moduł. Dane wykradzione od ofiar były szyfrowane za pomocą zaawansowanego algorytmu i klucza publicznego. Klucz prywatny potrzebny do odszyfrowania danych nie był dostępny na serwerze, co sugerowało, że dane trafiały do odrębnego zespołu, który jako jedyny potrafił odszyfrować dane i zbadać je.

[22] Te protokoły zostały nazwane: Old Protocol, Old E Protocol, SignUp Protocol i Red Protocol.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

skomunikować się z ujściem przy użyciu specyficznego dla SPE protokołu. Jednak dwa pozostałe ataki jeszcze nie zostały wykryte. Badaczom nie udało się zdobyć kopii SPE, dlatego nie wiedzieli, jakie było jego przeznaczenie.

Wszystko to potwierdzało jednak, że choć doniesienia na temat Stuxneta, Duqu i Flame'a były szokujące, narzędzia te są tylko niewielką cząstką zestawu narzędzi i broni zbudowanych przez Stany Zjednoczone i Izrael.

Kilka tygodni po ujawnieniu Flame'a Kaspersky natrafił na następne rządowe narzędzie szpiegowskie, które latami pozostawało niewykryte.

Za każdym razem, gdy zespół Raiu wykrywał nowe pliki albo znajdował dodatkowe informacje dotyczące Stuxneta, Flame'a lub Duqu, dopracowywał sygnatury w produktach antywirusowych i wyrażenia używane do przeszukiwania archiwum, aby sprawdzić, czy nie znajdzie innych wersji tych samych plików. W archiwum badacze znaleźli podejrzany plik pobrany przez zautomatyzowany system raportowania z komputera klienta z Bliskiego Wschodu. Plik ten został oznaczony przez system jako moduł Flame'a i komunikował się z tymi samymi serwerami C&C co Flame. Nie był to jednak ani Flame, ani żaden z trzech tajemniczych programów (SP, SPE lub IP).

Badacze dodali do silnika antywirusowego sygnaturę wykrywającą ten plik i odkryli ok. 2500 zainfekowanych ofiar w 25 krajach. Ponad 1600 z nich pochodziło z Libanu, drugi na liście z 482 maszynami był Izrael. Kolejne 261 komputerów znaleziono na terytoriach palestyńskich, ok. 40 ofiar znajdowało się w Stanach Zjednoczonych, a tylko jedna w Iranie.

Gdy zespół przeprowadził inżynierię odwrotną pliku i zaczął go analizować, zobaczył, że używane są w nim te same biblioteki, algorytmy i kod co w kodzie Flame'a. To wyjaśniało, dlaczego system uznał plik za moduł Flame'a. Programiści w niektórych plikach pozostawili nawet ścieżkę i dane projektu, z których wynikało, że na komputerach napastników pliki znajdowały się w katalogu *Flamer*[23].

Badacze z Kaspersky'ego nazwali nowy atak Gauss (od nazwy nadanej przez napastników jednemu z głównych modułów). Ta nazwa najwyraźniej była hołdem oddanym uznanemu matematykowi Johannowi Carlowi

[23] Nazwy Flame i Flamer występowały w różnych częściach kodu. Kaspersky zdecydował się nazwać to złośliwe oprogramowanie Flame, jednak Symantec w swoim raporcie nazwał je Flamer.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Friedrichowi Gaussowi. Inne moduły nosiły nazwy Lagrange i Gödel — zapewne od matematyka Josepha-Louisa Lagrange'a i kryptografa Kurta Gödla. Ten szacunek dla matematyki i kryptografii stał się zrozumiały, gdy badacze odkryli, że w ataku wykorzystano ładunek z bardzo złożonym i zaawansowanym schematem szyfrowania, godnym mistrza kryptografii.

Nowe tajemnicze złośliwe oprogramowanie było, podobnie jak Flame, narzędziem szpiegowskim. Było jednak znacznie mniejsze niż Flame i najwyraźniej stanowiło część innej operacji szpiegowskiej. To złośliwe oprogramowanie zawierało zestaw modułów służących do wykradania haseł z systemów, rejestrowania danych konfiguracyjnych i wykradania danych uwierzytelniających do kont z sieci społecznościowych, poczty elektronicznej i komunikatorów. Używany był też moduł do infekowania pendrive'ów z eksploitem plików .LNK zastosowanym w Stuxnecie.

W tym ataku znajdowało się coś jeszcze — mechanizm, którego badacze nigdy wcześniej nie napotkali w narzędziach stosowanych przez rząd. Był nim trojan wykradający dane uwierzytelniające do kont bankowych. Nie był to jednak zwykły trojan. Koncentrował się on na klientach banków w Libanie: Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank i Credit Libanais. Nic nie wskazywało na to, że trojan był używany do okradania kont, jednak niektóre banki libańskie były podejrzane o pranie pieniędzy dla irańskiego programu nuklearnego i irańskiego Hezbollahu. Dlatego napastnicy mogli monitorować stany kont i transakcje, aby ustalić zależności między kontami i śledzić przepływ pieniędzy.

W kodzie były dwie zagadki, których badacze nie potrafili rozwiązać. Jedna dotyczyła pliku z niestandardową czcionką (nazwaną przez napastników Palida Narrow), który Gauss instalował w zainfekowanych maszynach. Palida Narrow, podobnie jak Dexter Regular z Duqu, była nazwą fikcyjną. Jednak plik tej czcionki, inaczej niż w Duqu, nie zawierał eksploita ani szkodliwego kodu. Wydawało się, że nie pełnił żadnych funkcji, dlatego badacze nie potrafili zrozumieć, po co napastnicy go instalowali[24].

Większą zagadką był jednak zaszyfrowany ładunek, który Gauss umieszczał w niektórych maszynach. Był on zamknięty w nieprzepuszczalnej skorupie.

[24] Możliwe, że w pewnym okresie Gauss używał na potrzeby instalacji tego samego eksploita czcionki dla systemu Windows co Duqu. Nie było jednak wskazujących na to oznak. Gdyby ten eksploit był używany, napastnicy mogli usunąć go po załataniu przez Microsoft odpowiedniej luki w 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Stuxnet umieszczał ładunek na każdej zainfekowanej maszynie, ale uruchamiał go tylko w komputerach z odpowiednią konfiguracją. Gauss jednak dostarczał ładunek tylko na maszyny o określonej konfiguracji. Wyglądało na to, że napastnicy wyciągnęli wnioski z błędów popełnionych w Stuxnecie. Ograniczenie liczby maszyn, na których znajdzie się ładunek Gaussa, znacznie zmniejszało ryzyko wykrycia ataku.

Gauss dostarczał ładunek w bardzo restrykcyjny sposób za pomocą pendrive'ów. Infekował tylko jednego pendrive'a umieszczonego w opanowanej maszynie. Gdy ten pendrive był umieszczany w innym komputerze, Gauss instalował na nim ładunek tylko pod warunkiem, że konfiguracja maszyny była zgodna z szukaną. Ponadto rejestrował dane konfiguracyjne każdej maszyny i zapisywał je na pendrivie w ukrytym pliku. Gdy pendrive został włożony do innego komputera zainfekowanego przez Gaussa i podłączonego do internetu, ukryty plik był przesyłany na serwer C&C napastników. W ten sposób napastnicy dowiadywali się o tym, że Gauss dotarł do celu.

Gauss stosował też inne środki ostrożności związane z ładunkiem. W odróżnieniu od Stuxneta klucze służące do odblokowania ładunku nie były zapisane w samym złośliwym oprogramowaniu. Zamiast tego ładunek można było odszyfrować wyłącznie przy użyciu klucza dynamicznie generowanego na podstawie danych konfiguracyjnych z docelowej maszyny.

Jednak aby wygenerować ten klucz, złośliwe oprogramowanie wykonywało serię wyrafinowanych operacji, by uniknąć umieszczenia ładunku na niewłaściwej maszynie i zapobiec odblokowaniu go przez atak siłowy. Najpierw zbierane były ściśle określone dane konfiguracyjne z atakowanej maszyny — informacje o katalogach, plikach programów i innych znajdujących się na niej danych. Następnie nazwy plików były dołączane jedna po drugiej do nazwy pierwszego katalogu z folderu *Program Files* z systemu Windows. Do tego łańcucha dodawana była specjalna wartość, po czym 10 tys. razy używany był algorytm MD5 (który za każdym razem tworzył skrót na podstawie skrótu uzyskanego w poprzednim przebiegu)[25]. Jeśli ostatecznie wygenerowany został szukany skrót, złośliwe oprogramowanie przechodziło do następnego etapu.

[25] Napastnicy sprawdzali, czy w komputerze zainstalowany jest specyficzny program — zapewne unikatowy dla regionu, w którym go stosowano. Nie wiadomo, co to za program, jednak badacze z Kaspersky'ego stwierdzili, że jego nazwa zaczynała się od dziwnego znaku. Dlatego uznali, że program mógł nosić arabską lub hebrajską nazwę.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nawet gdy Gauss uzyskał szukany skrót, nie odblokowywał natychmiast ładunku. Zamiast tego ponownie obliczał dziesięciotysięczny skrót z użyciem innej dodanej wartości. Skrót z *tej* operacji był kluczem odblokowującym ładunek. Po odblokowaniu ładunku Gauss używał ścieżek i danych, które posłużyły do uzyskania pierwszego skrótu, dodawał do nich nową wartość, po czym odszyfrowywał drugą sekcję kodu ataku. Następnie kroki te były powtarzane jeszcze raz w celu odszyfrowania trzeciej sekcji kodu.

Tak właśnie powinno wyglądać szyfrowanie w bardzo starannie prowadzonej i ściśle kontrolowanej operacji. W porównaniu z tym ładunek Stuxneta prawie w ogóle nie był zabezpieczony. Badacze mogli łatwo go odblokować i ustalić jego działanie. Jednak skomplikowany schemat szyfrowania zastosowany dla ładunku Gaussa gwarantował, że ładunek pozostanie zamknięty w niedostępnym skarbcu, do którego nikt się nie włamie.

Rzeczywiście tak było. Choć badacze z Kaspersky'ego wypróbowali miliony par danych, aby wykryć konfigurację odblokowującą ładunek Gaussa, nie udało im się uzyskać właściwego klucza. Zastanawiali się, co było tak wyjątkowego w ładunku Gaussa, że napastnicy zadali sobie tyle trudu, by go zabezpieczyć. Nie mogli wykluczyć, że chodziło o niszczycielski kod, taki jak w Stuxnecie lub Wiperze. Ładunek mógł też zawierać poufne dane związane z trojanem wykradającym hasła bankowe i z sieciami finansowymi.

Zablokowany ładunek Gaussa uniemożliwił odszyfrowanie całego ataku, jednak w trakcie analizowania zagrożenia badacze natrafili na coś, co wcześniej przeoczyli. Był to fragment tajemniczego złośliwego oprogramowania SPE.

SPE był jednym z czterech programów komunikujących się z serwerami C&C Flame'a. Kilka miesięcy wcześniej SPE skontaktował się z ujściem Flame'a przygotowanym przez badaczy. Odkryli oni, że był to niezależny moduł, a nie odrębny atak. SPE mógł działać sam albo razem z Flame'em lub Gaussem, zwiększając możliwości szpiegowskie obu tych narzędzi[26]. Ten moduł, nazwany przez Kaspersky'ego miniFlame'em, był pierwszym bezpośrednim powiązaniem między Gaussem i Flame'em. Wcześniej badacze uważali, że oba ataki są zupełnie odrębnymi operacjami prowadzonymi

[26] Po natrafieniu na SPE nadal niewykryte pozostały dwa z czterech fragmentów złośliwego oprogramowania używanego razem z serwerami Flame'a. Raiu podejrzewał, że SP było wcześniejszą, nieszyfrowaną wersją SPE.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

przez tych samych napastników. Jednak miniFlame dowodził czegoś innego. Kaspersky znalazł nawet w Libanie komputer zainfekowany wszystkimi trzema programami: Flame'em, Gaussem i miniFlame'em[27].

Prostsza wersja Flame'a otwierała w zainfekowanych komputerach tylną furtkę, a ponadto wykradała informacje. Umożliwiała napastnikom zdalne sprawdzanie konfiguracji maszyn i tworzenie map innych powiązanych z nimi systemów. Napastnicy zapewne najpierw infekowali system za pomocą Flame'a lub Gaussa, aby zebrać podstawowe informacje na jego temat i ustalić, czy cel jest wartościowy. Następnie tylko na kluczowych komputerach należących do ważnych ofiar instalowali miniFlame'a, gdy potrzebowali uzyskać bezpośrednią kontrolę nad maszyną, pobrać z niej konkretne dane lub lepiej poznać sieć lokalną ofiary. Po zainstalowaniu miniFlame'a prawdopodobnie przesyłali z serwerów C&C moduł usuwający większy zestaw szpiegowski Flame'a, zmniejszając w ten sposób zakres pozostawianych śladów.

Kaspersky znalazł tylko ok. 50 ofiar zainfekowanych miniFlame'em — głównie w Iranie i innych krajach Bliskiego Wschodu, ale też na Litwie i w Stanach Zjednoczonych. U ofiar wykryto sześć różnych wersji modułu. Wszystkie powstały między październikiem 2010 r. a wrześniem 2011 r. Jednak pierwszy moduł miniFlame'a zbudowano zapewne w 2007 r., gdy tworzone były Stuxnet, Duqu i większa wersja Flame'a. W tym właśnie czasie opracowany został protokół używany w miniFlamie do komunikacji z serwerami C&C. Dziwne było to, że choć miniFlame w okresie czterech miesięcy latem 2012 r. komunikował się z ujściem Kaspersky'ego ok. 14 tys. razy, całkowicie wstrzymał kontakty w dniach 4 – 7 lipca tego roku. Kaspersky nigdy nie zdołał wyjaśnić tej przerwy.

PO ODKRYCIU OSTATNIEGO modułu praca Kaspersky'ego nad kodem twórców Stuxneta zaczęła spowalniać. Po części wynikało to z tego, że szczegółowa analiza przeprowadzona przez Raiu i jego zespół w celu ujawnienia utajnionych narzędzi rządowych zaczęła ściągać na badaczy niepożądaną uwagę.

[27] Pliki Gaussa nosiły nazwy utworzone od nazwisk słynnych matematyków i kryptografów. W SPE zastosowano bardziej „populistyczne" podejście, nazywając pliki: Fiona, Sonia, Tiffany, Elvis, Sam itd.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy zespół ujawniał jedno odkrycie po drugim, w społeczności zajmującej się zabezpieczeniami niektóre osoby zaczęły kwestionować motywy badaczy. Podobnie jak Symantec był krytykowany za brak lojalności wobec Stanów Zjednoczonych, ponieważ ujawnił Stuxneta i zaszkodził bezpieczeństwu narodowemu swojego kraju, tak część obserwatorów oskarżała moskiewską firmę Kaspersky Lab o działania na rzecz rosyjskiego wywiadu, ponieważ badacze ujawniali i sabotowali zachodnie operacje szpiegowskie.

Raiu stwierdził jednak, że żadne agencje rządowe ani wywiadowcze nie wywierały na niego nacisków. On i jego zespół nie interesowali się polityką. Ich jedynym celem, podobnie jak badaczy z Symanteca, było wykorzystanie umiejętności z zakresu inżynierii odwrotnej do zabezpieczania klientów i zwiększania bezpieczeństwa społeczności użytkowników komputerów. Ujawnienie Stuxneta i Flame'a stało *w sprzeczności* z interesami firmy. Kaspersky Lab intensywnie walczyła o rynek amerykański, a założyciel tej firmy, Eugene Kaspersky, starał się w tym celu zjednać sobie przyjaciół w Waszyngtonie i Izraelu. Ujawnianie utajnionych operacji przez jego badaczy z pewnością nie pomagało mu w nawiązywaniu stosunków z rządami tych państw.

Nie tylko interesy firmy były zagrożone. Badacze z Symanteca w trakcie analiz Stuxneta martwili się, że ich praca może być potajemnie obserwowana przez Izrael i Stany Zjednoczone, a nawet przez Iran. Nigdy jednak nie natknęli się na świadczące o tym konkretne oznaki. Raiu był natomiast przekonany, że w 2012 r. śledzono go w czasie konferencji w Monachium. Było to wkrótce po wykryciu Flame'a, ale jeszcze przed upublicznieniem tych informacji. Zauważył, że ktoś przyglądał się recepcji w hotelu w Monachium, gdzie badacz się zameldował. Raiu podejrzewał, że ten ktoś chciał ustalić numer jego pokoju. Później zaobserwował, że ktoś szedł za nim do toalety lub do pokoju hotelowego. Gdy wspomniał o tym współpracownikom, dowiedział się, że mieli podobne spostrzeżenia. Podejrzewał, że śledzili go pracownicy obcego wywiadu, ale nie był tego pewien. Później został zagadnięty przez trzech Izraelczyków chcących pomówić na temat jego pracy nad Duqu, a także przez kobietę, która chciała się dowiedzieć, czy Kaspersky potrafi odzyskać skasowane pliki z dysku twardego. To ostatnie pytanie było niepokojące, ponieważ Kaspersky starał się właśnie odtworzyć usunięte przez Wipera pliki z systemów w Iranie.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Był to następny nieprzyjemny dowód na to, że wraz z ujawnieniem Stuxneta świat łowców wirusów radykalnie się zmienił. Wcześniej ujawnienie cyfrowych zagrożeń oznaczało dla badaczy najwyżej ryzyko zemsty ze strony cyberprzestępców, którym mogło się nie podobać, że ktoś utrudnia im zarabianie na życie. Ale rozmontowanie rządowych operacji rodziło wiele nowych obaw. Raiu zdecydował, że ze względu na swoją rodzinę powinien być bardziej dyskretny. Po incydentach na konferencji w Monachium zrezygnował z publicznego omawiania prac Kaspersky'ego nad operacjami rządowymi i pozostawił rozmowy z mediami współpracownikom.

Nie było więc przypadkiem, że niedługo potem badacze z Kaspersky'ego przenieśli uwagę z rodziny Stuxnet-Duqu-Flame na inne projekty, a zwłaszcza na atak, który uważano za dzieło Rosjan. Ta operacja, nazwana Red October (czyli „czerwony październik"), była wymierzona w dyplomatów, rządy i instytucje badawcze, przede wszystkim z Europy Wschodniej i Azji. Głównym celem było zdobywanie poufnych dokumentów i informacji o znaczeniu geopolitycznym. Raiu i jego współpracownicy podejrzewali, że nie była to akcja rządowa, tylko operacja cyberprzestępców lub niezależnych szpiegów szukających danych w celu ich sprzedaży.

Zajmując się operacją Red October, zespół z Kaspersky'ego zdawał się na dobre pozostawiać za sobą twórców Stuxneta. Nie oznaczało to jednak, że świat nie miał już usłyszeć o Stuxnecie. Okazało się, że z tą cyfrową bronią związana jest jeszcze jedna niespodzianka.

BYŁ LISTOPAD 2012 r., ponad dwa lata od czasu wykrycia Stuxneta. Nawet Duqu i Flame były już tylko wspomnieniem, gdy badacze z Symanteca trafili na brakujące ogniwo, na którego znalezienie już dawno stracili nadzieję. Była to wczesna wersja Stuxneta, poprzedzająca wszystkie inne znane odmiany tego ataku.

Badacze odkryli ją w trakcie wyszukiwania w archiwum szkodliwych plików z „odciskami palców" pasującymi do Stuxneta. Robili to regularnie z użyciem sygnatur, aby się upewnić, że nie pominęli niczego ważnego. W trakcie tych poszukiwań natknęli się na komponent, którego wcześniej nie widzieli. Znajdował się on w archiwum od 15 listopada 2007 r., kiedy to ktoś przesłał go do witryny VirusTotal. Oznaczało to, że pierwszy atak Stuxneta został przeprowadzony znacznie wcześniej, niż badacze

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

pierwotnie sądzili[28]. Od zawsze uważali, że istnieją inne wersje Stuxneta, co wynikało z luk w numerach wersji z 2009 i 2010 r. — 1.001, 1.100 i 1.101. Podejrzewali nawet, że może istnieć wczesna wersja Stuxneta poprzedzająca wszystkie znane. Teraz ją znaleźli — był to Stuxnet 0.5.

Gdy odszukali inne pliki powiązane z tym komponentem, odkryli, że nie jest to byle jaka wersja Stuxneta. Zawierała ona kompletny kod ataku na model 417 sterowników PLC — nienaruszony i aktywny.

Wcześniejsze próby wyjaśnienia tajemnicy ataku na sterowniki PLC S7-417 Siemensa zakończyły się niepowodzeniem, ponieważ w nowszych wersjach Stuxneta kod był niekompletny i nieaktywny. Nicolas Falliere z Symanteca myślał, że napastnicy mogli wyłączyć kod, ponieważ oczekiwali na kluczowe dane o konfiguracji, aby dokończyć atak. Teraz było jasne, że napastnicy zdezaktywowali kod, ponieważ zdecydowali się zmienić taktykę. Choć nowsze wersje obejmowały zarówno kod ataku na model 315, jak i (nieaktywny) kod dla modelu 417, w znalezionej wczesnej wersji nie było śladu kodu związanego z modelem 315. Było więc oczywiste, że napastnicy początkowo koncentrowali się na ataku na model 415 z Natanzu, a później z jakichś przyczyn (możliwe, że atak nie pozwolił osiągnąć celu lub trwał zbyt długo) zmienili zdanie i skupili się na modelu 315.

Teraz, gdy zespół z Symanteca (już bez Falliere'a, który odszedł do Google'a) zdobył ten wczesny wariant kodu, mógł wreszcie ustalić, co kontrolowały sterowniki 417 i co robił z nimi Stuxnet. Okazało się, że ta wersja kodu atakowała zawory sterujące przepływem sześciofluorku uranu do wirówek

[28] Gdy szkodliwe pliki są przesyłane do witryny VirusTotal, przekazuje ona kopię każdej firmie antywirusowej, której skaner nie wykrył danego pliku. Czasem przesyła też wykryte pliki. Z informacji o tym wczesnym pliku Stuxneta wynika, że został przesłany do witryny VirusTotal przynajmniej dwukrotnie: 15 i 24 listopada. W obu sytuacjach tylko jeden z 36 skanerów oznaczył plik jako podejrzany, co było dobrą informacją dla napastników. Co dziwne, w rekordzie dotyczącym przesłania tego pliku brakuje pewnych informacji dostępnych dla innych plików. Na przykład pole z liczbą określającą, ile razy plik został sprawdzony, było puste, podobnie jak pole z krajem, z którego go przesłano. To ostatnie pole mogło zapewnić cenne informacje o lokalizacji napastników (jeśli to oni przesłali plik) lub o pierwszej ofierze (jeżeli plik pochodził z zainfekowanego komputera). Nie jest jasne, czy dane te zostały celowo usunięte z rekordu. Witryna VirusTotal została założona przez zespół hiszpańskich inżynierów, jednak firma Google przejęła ją we wrześniu 2012 r., kilka miesięcy przed tym, jak Symantec natrafił na wczesną wersję Stuxneta. Google nie odpowiedziała na pytania dotyczące tego, dlaczego w rekordzie brakuje wymienionych danych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

i kaskad w Natanzie oraz poza nie[29]. Stuxnet otwierał i zamykał zawory, aby zwiększać napięcie w wirówkach do pięciokrotności normalnego poziomu. Przy tym ciśnieniu gaz prawdopodobnie zacząłby przechodzić w stan stały. Zniweczyłoby to proces wzbogacania i spowodowało, że obracające się z dużą prędkością wirówki straciłyby równowagę i zaczęły uderzać w urządzenia stojące obok nich. Prawdopodobnie taki był plan. Możliwe, że nie zadziałał tak dobrze lub szybko, jak napastnicy sobie tego życzyli. Dlatego w 2009 r. taktyka została zmieniona i napastnicy skoncentrowali się na konwerterach częstotliwości. Była to bardziej bezpośrednia metoda uszkadzania wirówek.

Choć dla Stuxneta 0.5 nie określono daty zakończenia pracy i dlatego atak wciąż powinien być aktywny po zastosowaniu nowszych wersji Stuxneta, badacze po odkryciu robaka w 2010 r. nie znaleźli tego wariantu na żadnych komputerach[30]. Możliwe, że Stuxnet 0.5 został usunięty. Jedną z pierwszych rzeczy, jakie robiły nowsze wersje Stuxneta po instalacji na komputerze, było wyszukiwanie wcześniejszych wariantów tego robaka i zastępowanie ich. Dlatego możliwe, że Stuxnet 0.5 został automatycznie zastąpiony na zainfekowanych maszynach, gdy pojawiła się wersja z czerwca 2009 r.[31].

Było też możliwe, że próbek Stuxneta 0.5 nigdy nie znaleziono, ponieważ ta wersja była znacznie ściślej kontrolowana niż późniejsze i zainfekowała niewielką liczbę maszyn. Zamiast stosować do rozprzestrzeniania eksploity typu zero-day, ta wersja powielała się w tylko jeden sposób —

[29] Na podstawie danych konfiguracyjnych z tej wersji Stuxneta jeszcze łatwiej było stwierdzić, że robak szukał technologii z Natanzu. Z kodu wynikało, że robak poszukiwał obiektu z systemami o nazwach od A21 do A28. W Natanzie znajdowały się dwie hale z kaskadami: hala A i hala B. Gdy Stuxnet zaatakował, wirówki znajdowały się tylko w hali A. Była ona podzielona na pomieszczenia (moduły) z kaskadami. Moduły nosiły nazwy: jednostka A21, A22, …, A28.

[30] W Stuxnecie 0.5 znajdowała się data zaprzestania infekowania — 4 lipca 2009 r. Od tego dnia robak nie infekował już nowych maszyn, choć pozostawał aktywny na komputerach, na których już się znajdował (dopóki nie został zastąpiony przez inną wersję). Następna wersja Stuxneta pojawiła się 22 czerwca 2009 r., tylko dwa tygodnie przed datą zaprzestania infekowania ze Stuxneta 0.5.

[31] Ta wersja (podobnie jak nowsze) potrafiła aktualizować się na zainfekowanych maszynach bez połączenia z internetem. Robiła to za pomocą komunikacji P2P. Napastnicy musieli tylko przesłać aktualizację z jednego z serwerów C&C do komputera podłączonego do internetu lub dostarczyć ją za pomocą pendrive'a. Aktualizacja była następnie rozsyłana do innych maszyn w sieci lokalnej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

infekując pliki projektu z narzędzia Step 7 Siemensa. Były to pliki współużytkowane przez programistów i stosowane do programowania sterowników PLC Siemensa z serii S7. Dlatego doskonale nadawały się do dostarczenia Stuxneta do docelowych sterowników PLC. Fakt, że ta wersja rozprzestrzeniała się tylko za pomocą plików z narzędzia Step 7, wskazywał na to, że napastnicy mieli wewnętrzne dojścia pozwalające umieścić ją w podstawowych systemach Natanzu. Dlatego ryzyko wykrycia Stuxneta 0.5 było niewielkie, ponieważ pierwsza zainfekowana maszyna, czyli „pacjent zero", mogła być jedną z docelowych. Po powstaniu późniejszych wersji złośliwego oprogramowania napastnicy mogli stracić to dojście, co zmusiło ich do rozbudowania możliwości rozprzestrzeniania się Stuxneta, aby zwiększyć prawdopodobieństwo dotarcia ataku do celu[32]. Właśnie te możliwości i lokalizacja „pacjenta zero" w biurze poza Natanzem sprawiły, że Stuxnet został wykryty[33].

Stuxnet 0.5 po uruchomieniu był zupełnie autonomiczny, dlatego napastnicy nie musieli go kontrolować. Jeśli jednak znalazł się na komputerze podłączonym do internetu, kontaktował się z jednym z czterech serwerów C&C, z których napastnicy mogli przesyłać nowy kod w celu aktualizowania tej cyfrowej broni, gdy było to konieczne[34]. Stuxnet był tak zaprogramowany,

[32] Inną ciekawostką z tej wersji jest to, że obejmowała ona plik sterownika powodujący ponowne uruchomienie zainfekowanych komputerów z Windowsem 20 dni po infekcji. Stuxnet został wykryty w 2010 r., po tym jak maszyny w Iranie zaczęły się wyłączać i ponownie uruchamiać. Mimo że na tych komputerach znaleziono wersję inną niż 0.5, możliwe, że wciąż znajdował się na nich Stuxnet 0.5 lub jego sterownik, powodując wielokrotny ponowny rozruch systemu. Choć firma VirusBlokAda nigdy nie znalazła w tych maszynach wersji 0.5, mogli po prostu ją przeoczyć.

[33] Po wykryciu w swoim archiwum Stuxneta 0.5 badacze z Symanteca zaczęli go szukać. Znaleźli kilka zagubionych i uśpionych infekcji w Iranie, ale także w Stanach Zjednoczonych, Europie i Brazylii.

[34] Te serwery znajdowały się w Stanach Zjednoczonych, Kanadzie, we Francji i w Tajlandii. Serwery C&C były zamaskowane jako własność firmy z branży reklamy internetowej, Media Suffix, aby ukryć ich prawdziwe przeznaczenie przed osobami, które mogły uzyskać do nich dostęp. Domeny serwerów (*smartclick.org*, *best-advertising.net*, *internetadvertising4u.com* i *ad-marketing.net*) zawierały tę samą stronę główną fikcyjnej firmy reklamowej z hasłem „Zapewniaj to, co można sobie wymarzyć". Na stronie głównej można było przeczytać: „Internet staje się najważniejszym medium reklamowym i marketingowym na świecie. Media Suffix koncentruje się ściśle na reklamie internetowej i jest gotowa pokazać waszej firmie, jak wykorzystać ten niezwykle szybko rosnący rynek. Nie zostawaj z tyłu. […] Oferujemy naszym klientom niezrównany zakres pomysłowych rozwiązań dostosowanych do ich zróżnicowanych potrzeb".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

aby kończył komunikować się z serwerami 11 stycznia 2009 r. Jednak w tym czasie napastnicy przygotowywali już nową wersję ataku. Pierwszego stycznia 2009 r. skompilowali sterownik przeznaczony dla nowej wersji Stuxneta, uruchomionej pięć miesięcy później.

Przesłanie Stuxneta 0.5 do witryny VirusTotal w 2007 r. w połączeniu z datami związanymi z kodem zmusiło badaczy do zrewidowania szacowanego czasu rozpoczęcia prac nad Stuxnetem[35]. Wyglądało na to, że prace nad atakiem zapoczątkowano już w listopadzie 2005 r. To wtedy zostały zarejestrowane niektóre domeny dla serwerów C&C używanych przez Stuxneta 0.5. Kod innych serwerów C&C, używanych w atakach Stuxneta z lat 2009 i 2010 (w domenach todaysfutbol.com i mypremierfutbol.com), został skompilowany w maju 2006 r. Choć sam Stuxnet w 2006 r. nie został jeszcze uruchomiony — doradcy Busha w tym roku dopiero to zaproponowali — prace nad infrastrukturą do sterowania atakiem już trwały. Możliwe, że serwery C&C początkowo komunikowały się z Flame'em, Duqu lub innym narzędziem szpiegowskim używanym przez napastników do zbierania danych na potrzeby operacji, a potem zostały wykorzystane w Stuxnecie. Daty początków operacji są zbieżne z szacowanym przez badaczy z Kaspersky'ego początkiem prac nad Flame'em.

Te daty pasują też do okresu, w którym zbliżał się przełom w sytuacji politycznej związanej z irańskim programem nuklearnym. W sierpniu 2005 r., dwa miesiące po tym, jak Ahmadineżad zwyciężył w wyborach prezydenckich, międzynarodowe rozmowy na temat tego programu zostały przerwane, a Iran ogłosił, że wycofuje się z porozumienia o wstrzymaniu prac. Trzy miesiące później napastnicy zarejestrowali serwery C&C dla Stuxneta 0.5.

Iran w tym czasie zainstalował już w Natanzie wirówki, ale tylko w zakładzie pilotażowym. W lutym 2006 r., trzy miesiące po zarejestrowaniu serwerów C&C, Iran próbował wzbogacić pierwszą partię uranu w małej kaskadzie pilotażowej. Proces zakończył się niepowodzeniem, ponieważ 50 wirówek eksplodowało. Możliwe, że przyczyną była wczesna wersja Stuxneta. Irańskie władze wiązały sabotaż z zasilaczami UPS z Turcji, które ich zdaniem zostały zmodyfikowane, by powodować nagłe skoki napięcia.

[35] Stuxnet 0.5 mógł zostać uruchomiony wcześniej niż w listopadzie 2007 r., jednak to wtedy po raz pierwszy go zauważono. Zgodnie z datą kompilacji znalezioną w komponencie Stuxneta przesłanym do witryny VirusTotal kod został skompilowany w 2001 r., choć Chien i O'Murchu uważają, że ta data jest błędna.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Iran szybko otrząsnął się po tym niepowodzeniu i w maju ogłosił, że technikom udało się wzbogacić uran do 3,5% w kompletnej kaskadzie w zakładzie pilotażowym. Rozpoczęto więc realizację planu instalacji pierwszych 3000 wirówek w jednej z podziemnych hal. Jednak pierwsze urządzenia pojawiły się w hali dopiero na początku 2007 r. Do listopada zainstalowanych było ok. 3000 wirówek. W tym samym miesiącu po raz pierwszy został zauważony Stuxnet, gdy ktoś przesłał wersję 0.5 do witryny VirusTotal.

PO ODKRYCIU WCZESNEJ wersji Stuxneta badacze mieli możliwie kompletny obraz przebiegu tego wymierzonego w Iran przełomowego ataku.

Była to długa i nieprawdopodobna podróż, możliwa tylko dzięki serii niefortunnych zdarzeń i błędów, które nigdy nie powinny się wydarzyć: od eksploitów typu zero-day, które rozpoczęły szaloną drogę Stuxneta, przez tysiące maszyn z całego świata, po awarie maszyn w Iranie, co doprowadziło do pierwszego ujawnienia robaka; od początkujących badaczy z Białorusi, którym brakowało umiejętności i doświadczenia, by poradzić sobie z zagrożeniem pokroju Stuxneta, po badaczy z Symanteca męczących się z kodem sterowników PLC; od narzędzia Wiper w Iranie, co doprowadziło zespół z Kaspersky'ego do wykrycia Flame'a, po serwer w Malezji, który zablokował dostęp napastnikom i zachował wiele przydatnych badaczom dowodów. Tak wiele rzeczy w Stuxnecie i jego wielu narzędziach musiało zadziałać nieprawidłowo, aby atak został wykryty i odszyfrowany, że jego ujawnienie można uznać za cud.

Gdy cała sprawa się zakończyła, badacze z Kaspersky'ego i Symanteca przyjrzeli się dwóm latom pracy, jaką włożyli w inżynierię odwrotną i analizę szkodliwych narzędzi twórców Stuxneta, i mogli tylko podziwiać poziom umiejętności i kunsztu potrzebnych do opracowania ataku. Jednocześnie dziwili się temu, jak szybko operacja pozostająca przez tyle lat w ukryciu została przez nich rozwikłana — tak jakby pociągając za nić zwisającą ze swetra, doprowadzili do sprucia go w całości.

Napastnicy bez wątpienia zakładali (a nawet liczyli na to), że Irańczykom zabraknie umiejętności, aby samodzielnie wykryć lub odszyfrować ataki. Najwyraźniej nie przewidzieli jednak, że zbiorowa mądrość „ula" pozwoli je wykryć i przeanalizować bez udziału Irańczyków — dzięki globalnej społeczności zainteresowanej cyberbezpieczeństwem.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wraz ze Stuxnetem narodził się nowy porządek, w którym badacze zabezpieczeń i specjaliści od inżynierii odwrotnej stali się nieświadomymi członkami policji nowego rodzaju, zwerbowanymi w celu likwidacji cyfrowych broni stosowanych przez jedne kraje przeciwko innym oraz ochrony przed cyfrowymi atakami. Ta sytuacja stawia badaczy przed wieloma nowymi dylematami etycznymi i związanymi z bezpieczeństwem narodowym. Naukowcy muszą uwzględnić zarówno potrzeby użytkowników komputerów, jak i interesy agencji wywiadowczych oraz rządów. Jeśli Stuxnet oznaczał początek militaryzacji cyberprzestrzeni, zasygnalizował też upolitycznienie badań nad wirusami.

„Powstaje nowe pytanie o to, kto jest dobry, a kto zły, co może nas stawiać w bardzo trudnej sytuacji" — powiedział Eric Chien w 2012 r. po zakończeniu analiz nad Stuxnetem. Praca jego zespołu nad robakiem była wolna od wpływów politycznych. Chien miał nadzieję, że nigdy nie znajdzie się w położeniu, gdy będzie musiał wybierać między dobrem klientów a bezpieczeństwem narodowym. Nie był jednak na tyle naiwny, aby sądzić, że z pewnością uda mu się tego uniknąć.

„Może to zabrzmieć jak frazes, ale staramy się tylko pomagać ludziom i robić to, co słuszne — powiedział. — Jeśli dojdziemy do miejsca, w którym będziemy musieli zadać sobie to pytanie, będzie to bardzo trudna kwestia [do rozwiązania]. Uważam, że jeżeli tak się stanie, nie będzie to dobre miejsce"[36].

[36] Z wywiadu przeprowadzonego przez autorkę z Chienem w kwietniu 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 16

OPERACJA OLYMPIC GAMES

W 2012 r. Chien mógł zastanawiać się nad mroczną i skomplikowaną przyszłością, do której wiódł Stuxnet. Jednak cztery lata wcześniej architekci tego kodu rozważali inną mroczną przyszłość, związaną ze zbudowaniem przez Iran bomby atomowej.

W kwietniu 2008 r. prezydent Ahmadineżad odbył mocno nagłośnioną wizytę w zakładach wzbogacania uranu w Natanzie, aby uhonorować drugą rocznicę działalności kompleksu. Przy okazji dał specjalistom od kontroli zbrojeń pierwszy wgląd we wnętrze tego tajemniczego obiektu. Ubrany w biały fartuch i niebieskie plastikowe buty używane przez techników Ahmadineżad został sfotografowany, jak przygląda się monitorom komputerów w sterowni, pokazuje przed kamerami znany znak pokoju oraz przewodzi grupie sztywnych naukowców i biurokratów, idąc wzdłuż dwóch rzędów błyszczących wirówek mierzących po 1,8 m i stojących na baczność jak gotowi do przeglądu żołnierze w pełnym umundurowaniu.

Biuro prezydenta udostępniło prawie 50 zdjęć z tej wizyty. Analitycy nuklearni byli przerażeni widokiem zaawansowanych wirówek IR-2, o których tak dużo słyszeli. „To informacje, za które warto byłoby oddać życie" — powiedział jeden z londyńskich analityków o tych zdjęciach[1].

[1] Ten komentarz pojawił się w artykule na temat wizyty Ahmadineżada opublikowanym w witrynie Arms Control Wonk. William J. Broad, *A Tantalizing Look at Iran's Nuclear Program*, „New York Times", 29 kwietnia 2008.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W świcie towarzyszącej Ahmadineżadowi w wizycie w Natanzie znajdował się irański minister obrony. Był to dziwny członek grupy, jeśli wziąć pod uwagę utrzymywanie przez Iran, że ich program wzbogacania uranu ma charakter pokojowy.

Irańscy technicy cały 2007 r. spędzili na instalowaniu 3000 wirówek w jednej z podziemnych hal w Natanzie. W trakcie wizyty Ahmadineżad ogłosił plany dodania 6000 kolejnych urządzeń, dzięki czemu Iran miał znaleźć się w grupie niewielu państw zdolnych do wzbogacania uranu na skalę przemysłową. Była to słodka chwila triumfu po pokonaniu przez Iran wielu przeszkód, z jakimi musiał się zmierzyć w ciągu poprzednich dziesięciu lat. Znajdowały się wśród nich trudności techniczne, problemy z zakupem materiałów, sankcje oraz machinacje polityczne i tajne akcje sabotażowe mające powstrzymać prace. Teraz sukces programu wzbogacania uranu wydawał się pewny.

Jednak nie wszystko w Natanzie było już gotowe. Produkcja wzbogaconego uranu na skalę przemysłową wymagała tysięcy wirówek obracających się miesiącami z ponaddźwiękową szybkością bez przeszkód lub najwyżej z niewielkimi zakłóceniami[2]. I choć Ahmadineżad odbywał rundę honorową wzdłuż urządzeń, w bitach i bajtach kontrolujących je maszyn kryło się coś, co zapowiadało kolejne problemy.

POD KONIEC 2007 r. prezydent Bush podobno zażądał (z powodzeniem) od Kongresu 400 mln dolarów, aby sfinansować intensyfikację utajnionych operacji wymierzonych w nuklearne ambicje Iranu. Pieniądze zostały przeznaczone na zbieranie informacji, operacje polityczne służące destabilizacji i prowokujące do obalenia reżimu, a także tajne akcje dotyczące sabotażu urządzeń i zakładów związanych z programem nuklearnym[3]. Te ostatnie obejmowały eksperymentalne próby manipulacji komputerowymi systemami kontroli w Natanzie.

[2] Według Davida Albrighta przetworzenie partii gazu w kaskadzie i zakończenie wzbogacania wymagało tylko dnia lub dwóch, jednak wirówki obracały się latami, przyjmując nowe porcje gazu.

[3] Joby Warrick, *U.S. Is Said to Expand Covert Operations in Iran*, „Washington Post", 30 czerwca 2008.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Choć doradcy Busha cyfrowy sabotaż zaproponowali prawdopodobnie w 2006 r., przygotowania do niego rozpoczęto znacznie wcześniej, może nawet kilka lat wstecz, jeśli znaczniki czasu w użytych do ataku plikach są prawdziwe. Bloki szkodliwego kodu wstrzykiwane przez Stuxneta do modeli 315 i 417 sterowników PLC zawierały znaczniki czasu wskazujące na kompilację w latach 2000 i 2001. Szkodliwy plik .DLL dla systemu Step 7, używany przez Stuxneta do przejęcia prawdziwego pliku, według znacznika czasu pochodził z 2003 r.[4].

Możliwe, że zegary w komputerze używanym do kompilowania plików były źle ustawione lub że programiści zmienili znaczniki czasu, by zmylić śledczych. Jeśli jednak znaczniki były poprawne, oznaczało to, że napastnicy trzymali szkodliwy kod w pogotowiu przez trzy do sześciu lat. W tym czasie Stany Zjednoczone czekały na wyniki dyplomatycznych rozgrywek z Iranem. Kod zastosowały dopiero w 2006 r., kiedy stało się jasne, że negocjacje i sankcje nie przyniosły powodzenia.

Część kodu ataku została dostosowana do wielu systemów Siemensa, nie tylko tych z Natanzu. Dlatego *było* możliwe, że fragmenty kodu powstały w wyniku ogólnego projektu badawczego, którego celem było wykrycie luk we wszystkich sterownikach PLC Siemensa. Systemy kontroli tej firmy były popularne w Iranie. Wykorzystywano je w wielu branżach (ropy, gazu, petrochemicznej, mineralnej), a nie tylko w programie nuklearnym. Te systemy były też popularne w innych państwach Bliskiego Wschodu. Ponieważ pod koniec lat 90. cyberwojna stawała się już możliwa, dla Stanów Zjednoczonych i Izraela sensowna była inwestycja w badania nad lukami w systemie Step 7 i powiązanych sterownikach PLC Siemensa (pojawiły się one na rynku w połowie lat 90.) w przewidywaniu tego, że zyskana wiedza może się w przyszłości przydać.

[4] Datą kompilacji kodu infekującego bloki OB1 i OB35 sterowników PLC (są to bloki porządkowe kontrolujące odczyt poleceń w sterowniku PLC i system alarmowy) był 7 lutego 2001 r. Kod dokonujący sabotażu konwerterów częstotliwości i manipulujący zaworami zawierał podobne znaczniki czasu. Na przykład w ataku na model 315 związanym z sabotażem konwerterów firm Vacon i Fararo Paya znajdowało się 30 bloków kodu. Datą kompilacji dwóch z nich był maj 2000 r., natomiast pozostałych — 23 września 2001 r. Bloki kodu służące do manipulowania zaworami w ataku na model 417 też nosiły datę 23 września 2001 r., ale późniejszą o trzy godziny, tak jakby osoba odpowiedzialna za kompilację zrobiła sobie przerwę obiadową, a później wróciła dokończyć pracę.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jednak nie cały kod można było stosować do wszystkich systemów Siemensa. Bloki atakujące konwertery częstotliwości i zawory były specyficzne dla Natanzu i wymagały znajomości komponentów, jakie Irańczycy planowali zainstalować w tym zakładzie, oraz wiedzy na temat dokładnej konfiguracji urządzeń i działania zakładu. Aby znaczniki czasu z tych bloków kodu były wiarygodne, programiści musieliby w 2001 r. znać sprzęt, jaki miał zostać zainstalowany w zakładzie, który nie został jeszcze zbudowany.

Nie jest to jednak tak niewiarygodne, jak się może wydawać. Iran przetestował już proces wzbogacania uranu za pomocą niewielkich kaskad wirówek w fabryce Kalaye Electric mniej więcej w 1999 r. Ponadto w latach 2000 i 2002 CIA zrekrutowała ważnych dostawców z sieci A.Q. Khana, którzy przekazali agencji informacje na temat niektórych komponentów dostarczanych Iranowi i innym klientom Khana. Dlatego już przed rozpoczęciem w 2000 r. prac w Natanzie CIA mogła wiedzieć, jaki sprzęt (włącznie z systemami kontroli Siemensa) Iran planuje zainstalować w zakładzie.

David Albright z ISIS zgadza się, że wiele informacji na temat Natanzu mogło być znanych już w 2001 r.

„Szczegóły dotyczące kaskady, w tym liczba 164 wirówek na kaskadę, liczba etapów [w kaskadzie], większość zaworów, przetworniki napięcia i system rur mogły być znane [tak wcześnie]" — powiedział[5]. Jednak informacje o konwerterach Vacon i Fararo Paya zapewne były jeszcze niedostępne. „Konwertery częstotliwości to inna sprawa, ponieważ Iran w tym czasie kupował je od różnych zagranicznych firm. Trudno więc wierzyć, że projektanci Stuxneta mogli w 2001 r. liczyć na to, iż używane będą urządzenia z Finlandii lub produkowane w kraju [przez Fararo Paya]. Ponadto pierwszy moduł [kaskad zainstalowanych w Natanzie w 2007 r.] został zbudowany za pomocą różnych importowanych konwerterów częstotliwości"[6].

[5] Wcześniej opisano już, że kaskady są konfigurowane na podstawie liczby etapów wzbogacania. Na każdym etapie używana jest inna liczba wirówek.

[6] Z wywiadu przeprowadzonego przez autorkę z Albrightem w listopadzie 2013 r. Uważa się, że pierwszy moduł kaskad, A24, został zaatakowany przez Stuxneta 0.5, który manipulował tylko przy zaworach, a nie przy konwerterach częstotliwości. Późniejsze wersje, atakujące konwertery, miały być wymierzone w inny moduł, A26, który Iran zaczął instalować pod koniec 2007 lub na początku 2008 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2003 r., kiedy to zgodnie ze znacznikiem czasu skompilowana została kopia pliku z systemu Step 7, dostępnych było już więcej informacji na temat Natanzu.

Gdy inspektorzy z MAEA w lutym 2003 r. pierwszy raz odwiedzili Natanz, Iran posiadał już niewielką kaskadę w zakładzie pilotażowym i przygotowywał się do zainstalowania do końca roku nawet 1000 wirówek. W ramach kontroli irańskiego programu nuklearnego Iran miał udostępnić MAEA listy sprzętu zamówionego na potrzeby Natanzu i innych obiektów nuklearnych. Listy te obejmowały obrabiarki, zawory i pompy próżniowe[7]. Agencje wywiadowcze monitorowały też tajne transakcje przeprowadzane przez Iran i wiedziały, że Neda Industrial Group (czołowa teherańska firma z branży automatyki przemysłowej) uczestniczyła w zakupach towarów na potrzeby programu nuklearnego. Firma ta współpracowała z Kalaye Electric, byłym producentem zegarków przekształconym w fabrykę wirówek, przy instalowaniu sprzętu w Natanzie[8]. Neda była też lokalnym partnerem Siemensa w Iranie. Według witryny Nedy w latach 2000 i 2001 firma instalowała sterowniki PLC S7 Siemensa w innych obiektach w kraju. Był to model atakowany przez Stuxneta. Nietrudno było się domyślić, że skoro Neda instalowała te systemy w innych zakładach, zastosuje je także w Natanzie.

Siemens rzeczywiście sprzedawał dużo sprzętu do automatyki różnym jednostkom niezwiązanym z przemysłem atomowym, jednak urządzenia tej firmy trafiały też do zakładów nuklearnych. Z przechwyconego później przez zachodnie źródła listu napisanego w 2003 r. przez jedną firmę irańską do innej wynikało, że sterowniki S7-300 i S7-400 Siemensa, wraz z oprogramowaniem SIMATIC potrzebnym do komunikacji między nimi, zostały zakupione przez firmę Kimia Maadan zaangażowaną w przetwarzanie

[7] Iran oskarżył MAEA o udostępnianie informacji o programie nuklearnym tego kraju Stanom Zjednoczonym i Izraelowi. Nawet jeśli MAEA nie ujawniała otwarcie takich informacji, agencje wywiadowcze państw zachodnich i Izraela mogły włamać się na komputery MAEA w celu zdobycia danych na temat Natanzu. Ostatnio zostało ujawnione, że amerykańskie agencje wywiadowcze szpiegowały Radę Bezpieczeństwa ONZ-etu, patrona MAEA, i włamały się do systemu wideokonferencji ONZ-etu w celu pozyskania wiadomości o działalności tej organizacji.

[8] Więcej informacji o firmie Neda znajdziesz na s. 346.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

uranu w Iranie[9]. Sterowniki miały być przeznaczone dla irańskiej kopalni w Gachinie, gdzie Iran planował wydobywać naturalny uran do wzbogacania w wirówkach[10]. Wszystkie te informacje były znane Stanom Zjednoczonym i Izraelowi.

Choć początkowe plany mogły zostać opracowane w amerykańskim dowództwie strategicznym kierowanym przez gen. Jamesa Cartwrighta, to mieli je realizować cyberżołnierze z NSA i amerykańskiego cyberdowództwa we współpracy z programistami z izraelskiej elitarnej Jednostki 8200.

Przeprowadzenie ataku wymagało znacznie więcej informacji niż tylko dane o sprzęcie z Natanzu. Napastnicy musieli np. znać dokładną częstotliwość pracy konwerterów i konfigurację sprzętu. Nie mogli polegać tylko na dawnych projektach i planach, które mogły być nieaktualne. Potrzebowali ponadto wiedzy na temat działania systemu Step 7 i tego, jak komputery z Natanzu są podłączone do sieci. Te ostatnie informacje miały pomóc przekonać prawników Białego Domu, że kod nie wywoła kaskadowych efektów w innych systemach. Gdyby napastnicy błędnie założyli, że komputery z Natanzu nie mają połączenia z maszynami z zewnątrz, kod mógłby

[9] Treść dokumentu *Related to a PLC device Siemens TTE sold to Kimian Madaan for G'chin mine* z 4 maja 2003 r. została ujawniona autorce przez osobę mającą dostęp do tych danych. List został wysłany przez Tehran Tamman Engineering do Kimia Maadan i zawierał informacje, że Iran w 2002 r. pozyskał sprzęt i oprogramowanie potrzebne do monitorowania i kontrolowania sterowników SIMATIC S7-300 PLC. Według dokumentu w następnym roku Iran zakupił następny sterownik S7-300, dwa sterowniki S7-400, a także oprogramowanie Siemens SIMATIC WinCC do monitorowania tych urządzeń. W liście ten sprzęt został opisany jako „skomputeryzowany system do monitorowania i kontroli procesów przemysłowych na podstawie informacji otrzymywanych z przekaźników pomiarów fizycznych, np. ciśnienia i temperatury, oraz sterowników zaworów i systemu ogrzewania/chłodzenia z wykorzystaniem specjalistycznego oprogramowania". Opis ten ściśle pasował do działania systemu kontroli dla kaskady.

[10] Gdy w 2010 r. Stuxnet został wykryty i badacze ujawnili, że ta cyfrowa broń atakowała sterowniki Siemensa, wielu obserwatorów zastanawiało się, czy Iran w ogóle zainstalował w Natanzie takie sterowniki. Jednak rok wcześniej brytyjska Marynarka Wojenna w porcie w Dubaju przechwyciła tajną dostawę 111 opakowań sterowników Siemensa, prawdopodobnie przeznaczonych dla irańskiego programu wzbogacania uranu. Siemens wysłał je do odbiorcy z Chin, gdzie zostały przez Dubaj skierowane do Iranu. Odkrycie przesyłki spowodowało incydent międzynarodowy, ponieważ na podstawie sankcji ONZ-etu sprzedaż technologii do irańskiego programu nuklearnego była zabroniona. Ostatecznie Siemens na początku 2010 r. ogłosił, że od zakończenia lata 2010 nie będzie zawierał nowych kontraktów w Iranie.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

rozprzestrzenić się na inne urządzenia. Mogło to skutkować uszkodzeniem tych urządzeń i ujawnieniem operacji. To wtedy przydatne stały się narzędzia takie jak Flame i Duqu, pozwalające pobierać dane z komputerów administratorów systemów, którzy pomagali w instalowaniu sieci i zarządzaniu nią, oraz z maszyn pracowników kontraktowych i innych osób programujących sterowniki PLC. Jeśli używany był Duqu, mógł zostać przesłany za pomocą phishingu — tak jak pliki, które posłużyły do zainfekowania firmy na Węgrzech. To rozwiązanie sprawdzało się w przypadku maszyn podłączonych do internetu, np. laptopów programistów. Jednak w niepołączonych z internetem sterownikach PLC ukryte były dane konfiguracyjne dotyczące m.in. liczby podłączonych kart Profibus oraz modelu i liczby konwerterów częstotliwości.

Jeśli nie można było uzyskać takich danych w inny sposób, napastnicy potrzebowali pendrive'a, aby przedostać się do odizolowanej sieci i umieścić narzędzie szpiegowskie w maszynie podłączonej do sterowników PLC. Ponieważ programiści sterowników zwykle pracują na laptopach niepodłączonych do sieci systemu kontroli, łączą laptopy fizycznie z maszyną z sieci ze sterownikami PLC lub kopiują pliki z kodem na pendrive i przenoszą je do komputera z takiej sieci, co pozwala na łatwe zainstalowanie narzędzia szpiegowskiego. Napastnicy mogli następnie pobierać dane na temat sterowników PLC i sieci systemu kontroli w odwrotnej kolejności. Złośliwe oprogramowanie zapisywało dane na pendrivie, który programista umieszczał w laptopie podłączonym do internetu, co pozwalało pobrać informacje. Pojawiły się też doniesienia, że agencje wywiadowcze posługiwały się specjalnymi implantami w niepodłączonych do sieci maszynach w Iranie. Implanty te przesyłały dane o zainfekowanych systemach drogą radiową[11].

Zdobycie danych potrzebnych napastnikom mogło zająć wiele miesięcy. Jednak część prac zwiadowczych mogła zostać wykonana już w 2005 r., kiedy to zarejestrowano domeny dla serwerów C&C używanych przez Stuxneta 0.5. Choć Stuxnet został uruchomiony później, domeny początkowo mogły służyć do komunikowania się z narzędziami szpiegowskimi. Rekonesans mógł też być przeprowadzony w okolicach maja 2006 r., ponieważ badacze odkryli, że wtedy utworzony został kod serwerów C&C używanych dla późniejszych wersji Stuxneta.

[11] David E. Sanger, Thom Shanker, *N.S.A. Devises Radio Pathway into Computers*, „New York Times", 14 stycznia 2014.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Po zebraniu informacji o systemach napastnicy przystąpili do końcowych prac nad kodem ataków. Symantec podejrzewał, że kod ataków na modele 315 i 417 napisały dwa odrębne zespoły. Te podejrzenia wynikały z różnic w kodzie obu ataków. Nie było wiadomo, czy Stany Zjednoczone i Izrael wspólnie pracowały nad wszystkimi komponentami, czy też Izraelczycy przygotowali tylko pocisk, a Amerykanie ładunek. Trzeci zespół mógł pracować nad kodem przejmującym system Step 7 (podmieniającym poprawny plik .DLL na plik Stuxneta) i wstrzykującym szkodliwe polecenia do sterowników PLC. Symantec oszacował, że napisanie kodu związanego z systemem Step 7 zajęło ok. sześciu miesięcy, a przygotowanie szkodliwych bloków dla sterowników PLC trwało trochę krócej. Potrzebny był jednak jeszcze czas na testy.

Ktokolwiek odpowiadał za kod ataku, ta część operacji musiała być przygotowana bardzo precyzyjnie. Atak mógł się nie powieść z wielu powodów, a napastnicy nie mogli sobie pozwolić na błędy. Trudno było też ocenić efekty działania kodu w praktyce lub zmodyfikować go po jego uruchomieniu. To oznaczało, że napastnicy musieli przeprowadzić szeroko zakrojone testy — nie tylko w środowisku testowym dla sprzętu Siemensa, co pozwalało się upewnić, że kod nie zatrzyma systemu Step 7 lub sterowników PLC, ale też (w atakach z lat 2009 i 2010) z użyciem wszystkich wersji Windowsa, aby mieć pewność, że złośliwe oprogramowanie będzie się niewykryte sprawnie rozprzestrzeniać oraz instalować[12].

[12] W 2011 r. Ralph Langner zasugerował, że testy, jakie Laboratorium Narodowe Idaho przeprowadziło latem 2008 r. na systemie PCS7 Siemensa (obejmował on oprogramowanie Step 7 i WinCC oraz sterowniki S7-400), służyły do wykrycia luk, które mógł zaatakować Stuxnet. Te testy zostały przeprowadzone w ramach programu oceny producenta, a badacze oceniali różne systemy kontroli procesów przemysłowych pod kątem luk w zabezpieczeniach. Langner po raz pierwszy zasugerował, że laboratorium odgrywało rolę w tworzeniu Stuxneta, gdy natrafił na przygotowaną przez laboratorium prezentację w PowerPoincie na temat wspomnianych testów. Jednak testy te odbyły się od lipca do września 2008 r., a obecnie wiadomo już, że najstarsza znaleziona wersja Stuxneta, 0.5, została opracowana przed tymi testami i działała w listopadzie 2007 r., kiedy to ktoś przesłał ją do witryny VirusTotal. Ponadto jeśli wierzyć znacznikowi czasu ze szkodliwego pliku .DLL dla systemu Step 7, plik ten został skompilowany w 2006 r. Kierownictwo laboratorium w 2011 r. w trakcie oprowadzania reporterów (wśród których znajdowała się też autorka tej książki) przekonywało ich, że nie udostępniało informacji o lukach w systemie Siemensa nikomu, kto mógłby być twórcą Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

A przede wszystkim napastnicy potrzebowali precyzyjnej wiedzy o tym, jak każda zmiana w kodzie wpłynie na wirówki, zwłaszcza w kontekście tego, że planowali wyrafinowany atak, a nie akcję siłową. Najmniejszy błąd mógł zbyt szybko zniszczyć wirówki lub uszkodzić zbyt dużą ich liczbę i ujawnić sabotaż, demaskując całą operację.

Aby przeprowadzić akcję, napastnicy potrzebowali zespołu materiałoznawców i ekspertów od wirówek, znających gęstość i wytrzymałość aluminiowych wirników i obudów oraz wiedzących, jak łożyska w dolnej części wirówek, zapewniające równowagę obracających się urządzeń, zareagują na wzrost wibracji. Należało też obliczyć normalne wewnętrzne ciśnienie na ścianki wirówek i ustalić, w jakim stopniu wzrośnie wraz ze zwiększeniem ciśnienia gazu[13].

Potrzebne do tego były wirówki, na których można przetestować ataki. Na szczęście, jak wcześniej wspomniano, prowadzone przez Departament Energii Laboratorium Narodowe Oak Ridge w stanie Tennessee posiadało kilka wirówek P-1, na podstawie których powstał model IR-1 z Natanzu.

Historia pozyskania tych wirówek przez laboratorium miała początek w sierpniu 2003 r., trzy lata po tym, jak CIA zinfiltrowała nielegalną sieć dostaw sprzętu nuklearnego A.Q. Khana, i sześć miesięcy po pierwszej wizycie MAEA w Natanzie. Agencja szpiegowska przechwyciła dostawę czarnorynkowych komponentów do wzbogacania uranu, w tym 25 tys. obudów wirówek oraz pomp, rurek i innych części. Ten sprzęt zmierzał z Malezji do tajnego zakładu wzbogacania uranu w Libii. Przejęte skrzynie posłużyły Zachodowi w konfrontacji z libańskim dyktatorem Mu'ammarem al-Kaddafim jako dowód na prowadzenie tajnego programu nuklearnego. Zachód wywierał presję na zamknięcie tego programu. Dziewiętnastego grudnia libijski minister spraw zagranicznych ogłosił w telewizji narodowej rezygnację z prac nad programami budowy broni nuklearnej i chemicznej, choć wcześniej Libia nie przyznawała się do ich prowadzenia.

MAEA dowiedziała się, że w Libii znajdowało się już więcej sprzętu do wzbogacania uranu. Stany Zjednoczone zamierzały zdemontować ten sprzęt i przesłać go do laboratorium w Oak Ridge. Dlatego w czasie świąt

[13] Pojawiły się sugestie, że Niemcy i Wielka Brytania, dwa państwa z konsorcjum Urenco, które to konsorcjum produkowało wirówki będące wzorem dla irańskiego modelu IR-1, mogły udzielić pomocy w zrozumieniu tych urządzeń.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Bożego Narodzenia Olli Heinonen, jego szef Muhammad el-Baradei i inni pracownicy MAEA pojechali do Trypolisu, aby sporządzić wykaz urządzeń. Odkryli ponad 100 t sprzętu wartego ok. 80 mln dolarów. Sprzęt obejmował zasilacze UPS z Turcji (podobne do tych, które zostały poddane sabotażowi w Iranie w 2006 r.), 200 wirówek P-1 z Pakistanu, z których Libijczycy zbudowali już niewielką kaskadę, a także komponenty potrzebne do zbudowania ok. 4000 następnych wirówek[14]. Do marca 2004 r. przejęty sprzęt został spakowany i przesłany do kompleksu National Security Y-12 w Oak Ridge, gdzie był zabezpieczany przez ochroniarzy wyposażonych w karabiny szturmowe i udostępniany dziennikarzom.

„Wedle wszelkich obiektywnych wskaźników — powiedział wówczas zebranym reporterom Spencer Abraham, amerykański sekretarz energii — Stany Zjednoczone i inne państwa cywilizowanego świata stały się bezpieczniejsze dzięki przejęciu i likwidacji materiałów nuklearnych w Libii"[15]. Możliwe, że tak było, ale zdobyte „łupy" pozwalały też Amerykanom zbudować tajny obiekt do zbadania wirówek i przetestowania ataków na nie[16].

LABORATORIUM NARODOWE OAK RIDGE, powstałe w 1943 r. i zlokalizowane pod Knoxville, jest zarządzane przez UT-Battelle, organizację non profit założoną w 2000 r. przez Battelle Memorial Institute i University of Tennessee. Laboratorium określa się jako jednostka naukowa skupiona na zaawansowanych badaniach z zakresu materiałoznawstwa, energii atomowej, czystej energii i superkomputerów. Jednak tak naprawdę istnieje ono dzięki lukratywnym tajnym kontraktom związanym z bezpieczeństwem narodowym, podpisywanym z Departamentem Obrony, Departamentem Energii i agencjami wywiadowczymi. Wykonywane prace są związane z nierozprzestrzenianiem broni nuklearnej, eksploracją danych, łamaniem szyfrów itd.

---

[14] Podawane są różne liczby. Stany Zjednoczone poinformowały dziennikarzy, że Libia zakupiła 4000 wirówek. Zdaniem ISIS było ich ok. 200. Resztę sprzętu stanowiły komponenty do wirówek: obudowy (puste aluminiowe cylindry), a także inne części. Brakowało jednak umożliwiających pracę urządzeń wirników.

[15] Jody Warrick, *U.S. Displays Nuclear Parts Given by Libya*, „Washington Post", 15 marca 2004.

[16] William J. Broad, John Markoff, David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, „New York Times", 15 stycznia 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Tajny zakład z wirówkami — część trwającego obecnie już dziesięć lat poufnego programu badań nad uszkadzaniem tych urządzeń — został zbudowany po 2005 r. na położonym z dala od siedzib ludzkich obszarze ponad 14-hektarowego rezerwatu Oak Ridge. Ośrodek ten był niewidoczny i niedostępny nawet dla większości pracowników laboratorium. Do tego tajnego zakładu (nazywanego według jednej z osób, które o nim wiedziały, „Wzgórzem" lub „farmą kurczaków") można było dotrzeć nieoznakowaną drogą, która meandrowała przez kilkanaście kilometrów wzdłuż gęstego lasu i wiodła najpierw do jednej strzeżonej bramy, a następnie do drugiej[17].

Wzgórze obejmowało dwa budynki — jeden nadziemny i drugi podziemny. Podziemna hala, zbudowana znacznie wcześniej w innym celu, została wykorzystana do pierwszego etapu prac nad wirówkami. Najpierw badacze koncentrowali się tylko na ustaleniu, jak działają wirówki znalezione w Libii. Laboratorium otrzymało z tego kraju modele P-1 i P-2, jednak nadeszły one w postaci niezłożonych komponentów bez instrukcji obsługi. Badacze mieli więc wiele szuflad zapełnionych częściami, ale nie mieli doświadczenia w pracy ze schematami, dlatego początkowo dużo czasu zajęło im ustalenie, jak połączyć komponenty i zmusić je do działania.

Naukowcy w Oak Ridge natrafili na podobne problemy co Irańczycy doświadczeni w korzystaniu z tych nieprzewidywalnych i delikatnych urządzeń. Kłopotliwe okazały się zwłaszcza czerpaki i łożyska kulkowe, które na pewien czas spowolniły postępy badaczy.

Pierwotnie program nie miał na celu zbudowania wirusa do ataku na wirówki. Badacze chcieli się jedynie dowiedzieć, jak działają wirówki i kaskady, aby zrozumieć możliwości tych urządzeń i oszacować, jak daleko Irańczycy zaszli w programie wzbogacania uranu, a także ustalić, jak dużo Iranowi brakuje, aby uzyskać ilość wzbogaconego uranu wystarczającą do zbudowania bomby atomowej. Gdy naukowcy w Oak Ridge ukończyli wstępne badania i testy, oszacowali, że Iran w 12 – 18 miesięcy wyprodukuje wystarczającą ilość materiałów rozszczepialnych do otrzymania bomby.

Badania nad wirówkami nie były dla laboratorium niczym nowym. Kompleks miał długą historię takich badań i produkcji wirówek. W latach 60. wyprodukował jedne z pierwszych wirówek z wirnikami. Jednak w 1985 r.

[17] Oak Ridge znajduje się na dawnych terenach rolniczych. Określenie „farma kurczaków" może dotyczyć prawdziwej farmy, która istniała w tym miejscu w latach 40., zanim rolnicy zostali wysiedleni po wykupieniu ich ziemi przez rząd na potrzeby działań wojennych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

program ten został wstrzymany, ponieważ lasery zastąpiły wirówki jako podstawowa metoda wzbogacania uranu w Stanach Zjednoczonych. Zakończenie projektu spowodowało zwolnienie tysięcy wykwalifikowanych robotników i badaczy, których specjalistyczna wiedza przestała być potrzebna.

W 2002 r., mniej więcej w czasie, gdy świat dowiedział się o tajnym zakładzie wzbogacania uranu w Natanzie, nastąpił powrót zainteresowania wirówkami. W Oak Ridge wznowiono program w celu zaprojektowania wirówek nowej generacji na potrzeby firmy United States Enrichment Corporation, producenta wzbogaconego uranu dla komercyjnych elektrowni atomowych w Stanach Zjednoczonych. Aby zapewnić obsadę tego projektu, laboratorium ściągnęło z emerytury wielu byłych ekspertów od wirówek (niektórzy mieli już po 70 – 80 lat), aby współpracowali razem z młodszymi naukowcami.

Po przejęciu od Libii partii cennych wirówek wielu badaczy zostało oddelegowanych do analizy tych urządzeń. Według osoby zaznajomionej z programem prace były prowadzone pod zwierzchnictwem NNSA (ang. *National Nuclear Security Administration*), jednostki Departamentu Energii odpowiedzialnej za bezpieczeństwo broni atomowej państwa, ale też prowadzącej badania związane z nierozprzestrzenianiem takiej broni i program badawczy o nazwie NA-22[18]. W ramach tego programu zbierane są informacje na temat nielegalnych działań nuklearnych — od ludzi, a także za pomocą zdalnych czujników i testów środowiskowych. Celem jest uzyskanie dowodów tajnych prac nad wzbogacaniem uranu i detonacjami ładunków atomowych przez wrogie reżimy i podmioty[19].

---

[18] NNSA prowadzi działalność w Oak Ridge w budynku MRF (ang. *Multi-Program Research Facility*). Jest to duży obiekt z obszaru SIGINT mieszczący w piwnicy superkomputer służący np. do eksploracji danych na potrzeby NSA. Inni pracownicy w MRF (często byli agenci CIA i NSA) posiadają wiedzę techniczną i pracują nad różnymi innymi programami. Między innymi łamią szyfry i zajmują się scalaniem danych (ang. *data fusion*; pracownicy nazywają to czasem biegunką danych), co polega na łączeniu informacji z różnych jednostek wywiadowczych z całego świata.

[19] Używane są różne techniki, np. analizowanie emitowanych przez fabryki gazów pod kątem cząsteczek śladowych lub pomiar temperatury wody w pobliżu podejrzanych kompleksów. Wiele obiektów nuklearnych jest budowanych blisko rzek i innych źródeł wody. Temperatura wody może wskazywać na prowadzenie działalności nuklearnej. Inna metoda polega na pomiarze z dużych odległości migotania świateł w oknach fabryki. Ponieważ wirówki działają z określoną częstotliwością, wzorzec migotania świateł czasem wskazuje na obecność i rodzaj wirówek używanych w danym budynku.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

NNSA już od pewnego czasu próbowała zdobyć irańskie wirówki, dlatego dostawa modeli P-1 i P-2 z Libii z 2004 r., na których wzorowane były irańskie urządzenia, okazała się cennym łupem.

Badacze otrzymali też części bezpośrednio z irańskiego programu (dzięki źródłom związanym z wywiadem). Te części były niezwykle cenne, ponieważ uważano, że Korea Północna używa wirówek o takim samym ogólnym projekcie. Pracownicy otrzymali polecenie, aby używać tych komponentów bardzo ostrożnie i w rozsądny sposób, ponieważ niektórzy dostawcy tych części oddali za nie życie. Nie można było łatwo zastąpić tych komponentów, dlatego każdy test musiał do czegoś prowadzić.

W 2006 r., gdy Iran ogłosił rozpoczęcie wzbogacania uranu w Natanzie, badania nad urządzeniami już trwały. Jednak według osoby znającej program badacze robili niewielkie postępy. Ale w 2007 r. zintensyfikowano prace, ponieważ Iran rozpoczął instalowanie pierwszych wirówek w podziemnej hali w Natanzie.

Jednocześnie zbudowana została nadziemna hala na potrzeby testowania (i niszczenia) wirówek. Uważa się, że niektóre z tych badań początkowo były skoncentrowane na ustaleniu możliwych niszczycielskich efektów ataku kinetycznego, np. bombardowania podziemnej hali z wirówkami. Możliwość przeprowadzenia cyberataku pojawiła się dopiero później. Gdy już *zaproponowano* operację cyfrową, pierwotnym celem nie było uszkodzenie wirówek w Natanzie z użyciem wirusa, ale umieszczenie kodu szpiegowskiego w wyposażeniu zakładu. Miało to pozwolić uzyskać dane, które pomogłyby naukowcom ustalić postępy Iranu w programie wzbogacania uranu. Na pewnym etapie program niszczenia wirówek i operacja szpiegowska zostały połączone w plan cyfrowego ataku kinetycznego. Większość naukowców testujących wirówki prawdopodobnie nie wiedziała o planach ataku, a była tylko skupiona na ocenie, jak na te urządzenia wpłyną różne warunki, np. wyższa lub niższa prędkość albo wyższe ciśnienie na ścianki wirówki. Przyczyna zaistnienia tych warunków zapewne nie była przez badaczy uwzględniana.

W dużej hali testów w przedniej części stały uporządkowane jak w bibliotece wysokie półki z systemami kontroli Siemensa i innych firm. Po drugiej stronie pomieszczenia znajdowało się kilkanaście wirówek wielkości człowieka. Prowizorycznie podłączone kable biegły z niektórych wirówek do czujników, co pozwalało rejestrować dane diagnostyczne i pomiary takie jak

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

temperatura obudowy lub drżenie i wibracje sworzni oraz łożysk kulkowych odpowiedzialnych za utrzymanie urządzeń w równowadze.

Niektóre wirówki obracały się miesiącami, w czasie gdy zbierane były dane na ich temat. Były to egzemplarze badawcze. Inne czekał mniej przyjemny los. Zaraz obok wejścia do hali znajdowała się duża skrzynka z akrylu i metalu (wyglądała ona tak, jakby zespół z programu *Pogromcy mitów* zaprojektował szpitalną salę do oglądania noworodków), gdzie trafiały wirówki skazane na zniszczenie. Pracownicy zawsze wiedzieli, kiedy w ochronnej skrzynce wirówki ulegają destrukcji, ponieważ urządzenia wydawały wtedy przeraźliwe, przypominające wybuch odgłosy, połączone z uderzeniami w podłogę.

W 2008 r. operacja trwała w pełni, a wirówki były niszczone prawie codziennie. „Było widać, że budżet znacznie wzrósł" — powiedział informator. Prezydent Bush, prawdopodobnie nieprzypadkowo, otrzymał właśnie od Kongresu 400 mln dolarów na utajnione operacje wymierzone w irański program nuklearny.

Gdy przeprowadzane były testy w Oak Ridge, w izraelskim obiekcie nuklearnym w Dimonie miały podobno miejsce inne próby związane z wirówkami. Nie jest jasne, jak długo trwały badania i kiedy urzędnicy zdecydowali, że mają wystarczającą ilość danych, by przeprowadzić skuteczny atak.

W czasie testów w 2006 r. prace nad kodem ataku już trwały. Dokładny harmonogram nie jest znany, jednak badacze z Symanteca stwierdzili, że ich zdaniem w maju 2006 r. została zmodyfikowana ważna funkcja użyta w kodzie ataku. Była to funkcja używana w Stuxnecie do inicjowania komunikacji z konwerterami częstotliwości w ataku na model 315. W maju 2006 r. został też skompilowany kod dwóch serwerów C&C używanych z tą wersją Stuxneta — mypremierfutbol.com i todaysfutbol.com. Inne istotne funkcje zostały zmienione we wrześniu 2007 r. Zaledwie dwa miesiące później, w listopadzie 2007 r., wersja 0.5 robaka została przesłana do witryny VirusTotal — przez testerów lub zainfekowaną ofiarę.

W pewnym momencie niektóre wirówki w Oak Ridge lub innym laboratorium zostały poddane testom nowego rodzaju, aby bezpośrednio zmierzyć skuteczność cyfrowej broni przeciw wirówkom. Gdy testy słuszności koncepcji zostały ukończone, oficjele podobno zaprezentowali Bushowi wyniki swojej pracy — szczątki zniszczonej wirówki, potwierdzające, że

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

niezwykły plan może się powieść[20]. Test wirówek (podobnie jak test Aurora Generator przeprowadzony w Idaho przez siostrzaną jednostkę laboratorium z Oak Ridge na początku 2007 r.) pokazał, że ciężkie maszyny nie mają szans z dobrze zaprojektowanym kodem.

WCIĄŻ POZOSTAJE TAJEMNICĄ, jak i kiedy Stuxnet 0.5 trafił do komputerów w Natanzie[21]. Ponieważ systemy kontroli procesów przemysłowych w Natanzie nie były bezpośrednio podłączone do internetu, a ta wersja Stuxneta obejmowała niewiele mechanizmów rozprzestrzeniania, napastnicy musieli dotrzeć do odizolowanych systemów, wnosząc kod do zakładu lub wysyłając go e-mailem. Ta wersja Stuxneta potrafiła się rozprzestrzeniać w tylko jeden sposób: za pomocą zainfekowanych plików projektu z narzędzia Step 7. To oznaczało, że kod musiał zostać umieszczony bezpośrednio na komputerze programisty lub operatora maszyny z użyciem pendrive'a — np. przez pracownika kontraktowego nieświadomego, że przenosi robaka, lub przez opłaconego „kreta". Inną możliwością było przesłanie zainfekowanego pliku projektu e-mailem do kogoś w Natanzie[22]. Z maszyny programisty lub operatora robak miał tylko krok lub dwa do docelowych sterowników PLC. W odróżnieniu od późniejszych wersji, które przechowywały dziennik z każdym zainfekowanym systemem oraz znacznikiem czasu określającym datę infekcji, w Stuxnecie 0.5 badacze nie znaleźli cyfrowego tropu pozwalającego odkryć drogę tego robaka.

[20] David E. Sanger, *Confront and Conceal*, Crown, Nowy Jork 2012, s. 197.

[21] Ponieważ pierwsza wersja Stuxneta pojawiła się w listopadzie 2007 r., sabotaż mógł się rozpocząć w tym samym roku. David Sanger pisze, że jeszcze w czasie prezydentury Busha wypuszczonych zostało kilka wersji robaka. Badacze znaleźli tylko jedną z nich. Pozostałe pochodzą z okresu urzędowania Obamy.

[22] W 2008 r. w Iranie powieszono irańskiego sprzedawcę elektroniki Alego Ashtariego, który według irańskich serwisów informacyjnych zeznał, że próbował wprowadzić przygotowane przez Mosad wirusy i nadajniki GPS do sprzętu używanego przez członków gwardii rewolucyjnej. Po wykryciu Stuxneta pojawiły się raporty donoszące, że Ashtari pomógł umieścić Stuxneta w Natanzie. Jednak informacje z Iranu są często niewiarygodne, ponieważ zwykle pochodzą z nieobiektywnych mediów powiązanych z rządem. Iran przez lata oskarżył wiele osób o szpiegowanie na rzecz Mosadu, często nie mając na to wystarczających dowodów.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ta wersja nie atakowała modelu 315 i konwerterów częstotliwości. Jej celem były model 417 i zawory. Te ostatnie miały być otwierane i zamykane w celu manipulowania przepływem uranu w postaci gazowej.

Kaskady w Natanzie były podzielone na 15 etapów. Na każdym z nich działała inna liczba wirówek. Gdy gaz przechodził z jednego etapu do następnego i ilość wzbogacanego gazu się zmniejszała, liczba używanych wirówek też była coraz mniejsza.

Na przykład etap 10., był „etapem podawania", na którym do kaskady wpompowywane były nowe porcje gazu. Obejmował on 24 wirówki. Gdy wirniki kręciły się z dużą prędkością i oddzielały od siebie izotopy, gaz zawierający koncentrat ^{235}U był pobierany czerpakami i przekazywany do etapu 9. (z 20 wirówkami), gdzie polegał dalszemu wzbogaceniu, a następnie trafiał do etapu 8. (z 16 wirówkami). W tym czasie gaz zawierający koncentrat ^{238}U był kierowany do etapu 11., gdzie podlegał dalszemu rozdzielaniu. Koncentrat ^{235}U z etapu 11. był przekazywany do etapu 8., gdzie był złączany z resztą wzbogaconego gazu. Proces ten był powtarzany do czasu dojścia wzbogaconego gazu do ostatniego etapu kaskady (zubożony gaz był usuwany). Ostatni etap kaskady, do którego trafiał wzbogacony uran, obejmował zwykle tylko jedną wirówkę i — na wypadek jej awarii — urządzenie rezerwowe.

W każdej kaskadzie znajdowały się pomocnicze zawory kontrolujące przepływ gazu między poszczególnymi etapami wzbogacania. Ponadto każda wirówka IR-1 miała w górnej części trzy wąskie rurki z zaworami kontrolującymi przepływ gazu do urządzenia i z niego. Otwarcie zaworu podawania powodowało dopływ gazu, wzbogacony uran był przekazywany dalej za pomocą zaworu zbierania produktu, a zubożony gaz był pobierany dzięki zaworowi wylotowemu i połączonej z nim rurce.

Stuxnet atakował tylko wybrane zawory w Natanzie. Podziemna hala, w której zainstalowano wirówki, była podzielona na moduły (sale kaskad). Każdy moduł mógł pomieścić 18 kaskad zawierających po 164 wirówki, co w sumie dawało ok. 3000 wirówek na salę. W momencie gdy Stuxnet został wypuszczony, w podziemnej hali gotowa była tylko jedna sala zapełniona 18 kaskadami. Jednak Stuxnet atakował tylko 6 kaskad. Nie wpływał też na wszystkie wirówki w każdej z nich. Jego celem były zawory w tylko 110 z 164 wirówek w tych kaskadach. Pozostałe 54 pozostawały nietknięte.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy ta wersja trafiła do systemu w Natanzie, pozostawała w uśpieniu przez jakieś 30 dni przed rozpoczęciem ataku. W tym czasie sprawdzała system, aby się upewnić, że różne zawory, mierniki ciśnienia gazu i inne komponenty są dostępne, oraz prześledzić ich pracę[23].

W trakcie analizowania systemu Stuxnet rejestrował też różne dane związane z normalnym działaniem kaskady, które potem odtwarzał operatorom po rozpoczęciu sabotażu (podobnie działał kod ataku na model 315). Na przykład na krótko otwierał zawory w ostatnim etapie kaskady, aby odczytać ciśnienie, a następnie odtwarzał normalny odczyt operatorom w trakcie ataku, co pozwalało ukryć wzrost ciśnienia.

Po zebraniu wszystkich potrzebnych danych Stuxnet czekał do momentu spełnienia określonych warunków w kaskadzie, a potem kontynuował pracę. Przykładowo: pojedyncza kaskada musiała działać ponad 35 dni przed rozpoczęciem ataku lub wszystkich 6 atakowanych kaskad (jeśli wszystkie były aktywne) musiało pracować w sumie przynajmniej 298 dni.

Po rozpoczęciu ataku Stuxnet zamykał różne zawory oprócz tych z etapu podawania, na którym gaz był wprowadzany do kaskady. Na przykład na etapie 9. zamykał zawory wylotowe w 14 z 20 wirówek, a na etapie 8. — w 13 z 16. Zawory zamykane na poszczególnych etapach były wybierane na podstawie skomplikowanego procesu.

Po zamknięciu zaworów Stuxnet czekał na wzrost ciśnienia w wirówkach, gdy gaz napływał do urządzeń, ale nie mógł z nich się wydostać. Czekał albo dwie godziny, albo do momentu pięciokrotnego wzrostu ciśnienia (w zależności od tego, który z tych warunków został spełniony wcześniej). Następnie wykonywał kolejny krok: otwierał wszystkie zawory pomocnicze oprócz trzech, które uznał, że znajdują się blisko etapu podawania. Potem czekał trzy minuty i przekazywał operatorom kolejne fałszywe dane, zapobiegając wprowadzeniu zmian w systemie przez dalszych siedem minut. Pod koniec ataku otwierał grupę ok. 25 zaworów. Albright i jego współpracownicy z ISIS podejrzewali, że były to zawory powiązane z kolektorem odpadów. Na każdym etapie kaskady znajdowała się rurka prowadząca do kolektora odpadów. Gdy wystąpiły problemy z wirówkami lub w procesie wzbogacania, gaz można było przesłać z kaskady do schłodzonego zbiornika.

[23] Stuxnet 0.5 oczekiwał np., że jego cel będzie miał od 2 do 25 pomocniczych zaworów i od 3 do 30 mierników ciśnienia gazu na każdym etapie kaskady.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Po otwarciu przez Stuxneta zaworów do kolektora odpadów gaz z kaskady trafiał do zbiornika i nie nadawał się już do użytku.

Po wykonaniu wszystkich kroków atak kończył się i cały proces rozpoczynał się od nowa.

To, że atakowane były zawory wyłącznie niektórych wirówek, a sama akcja trwała tylko dwie godziny, kiedy to operatorom przekazywane były błędne odczyty, bardzo dezorientowało techników w Natanzie, którzy dostrzegali narastające w wirówkach problemy, a także spadek ilości wzbogacanego uranu, a jednocześnie nie potrafili wykryć wzorca ani ustalić przyczyny kłopotów.

Badacze do tej pory nie wiedzą, które dokładnie zawory były otwierane i zamykane przez Stuxneta. Dlatego nie da się jednoznacznie określić efektów jego działania. Na podstawie pewnych założeń Albright i jego współpracownicy przedstawili dwa scenariusze. W jednym z nich zawór zbierania produktu i zawór wylotowy na końcu kaskady były zamykane, dlatego gaz wciąż był pompowany do kaskady, ale nie mógł się z niej wydostać. W tym scenariuszu ciśnienie gwałtownie rosło, a gdy osiągnęło pięciokrotność normalnego poziomu, następowała kondensacja i przejście w stan stały. Kiedy zestalony uran uderzał w obracający się wirnik, uszkadzał go lub powodował utratę równowagi przez urządzenie i uderzał o ścianki. Drżenie destabilizowało łożyska pod wirówką, co skutkowało zaburzeniem ruchu urządzenia. Kręcąca się z dużą szybkością wirówka odrywająca się od podstawy ma dużą siłę niszczycielską i może uszkodzić inne urządzenia.

W tym scenariuszu na późniejszych etapach kaskady ciśnienie rosło szybciej niż na wcześniejszych. Dlatego wirówki z dalszych etapów psuły się jako pierwsze. Albright i jego zespół oszacowali, że taki atak mógł niszczyć ok. 30 wirówek na kaskadę. Dzięki skoncentrowaniu ataku na wirówkach z dalszych etapów kaskady, z największym poziomem koncentracji wzbogaconego uranu, sabotaż przynosił lepsze efekty. Uszkadzanie wirówek w pobliżu etapu podawania, gdzie koncentracja izotopu ^{235}U jest najmniejsza, oznaczałoby utratę mniejszej ilości czasu i pracy niż w sytuacji, gdy uran przeszedł przez całą kaskadę i był już prawie gotowy — w momencie zniszczenia końcowych wirówek i utraty gazu.

Możliwe było też to, że Stuxnet nie zamykał zaworów zbierania produktu i wylotowego na końcu kaskady. W tym scenariuszu główny cel Stuxneta był skromniejszy — robak jedynie ograniczał ilość wzbogacanego gazu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gaz był wprowadzany do kaskady, jednak ponieważ zawory 110 ze 164 wirówek zostały zamknięte, mógł trafić tylko do 54 wirówek, na które Stuxnet nie wpływał. Skutkowało to mniejszą ilością wzbogaconego gazu i niższym stężeniem potrzebnego izotopu.

Gdy Stuxnet przeprowadzał sabotaż i przekazywał operatorom fałszywe dane, jednocześnie wyłączał w kaskadzie system bezpieczeństwa zaprojektowany w celu izolowania wirówek, zanim spowodują szkody. Ten system był zaawansowanym rozwiązaniem i obejmował akcelerometr podłączony do każdej wirówki (aby mierzyć poziom wibracji), a także kilkadziesiąt mierników ciśnienia w każdej kaskadzie. Gdy wirówce groziła awaria, błyskawicznie (w ciągu milisekund od wykrycia problemu) aktywowany był system reagowania, który zamykał zawory w wirówce i izolował umieszczony w niej gaz[24]. Energia kinetyczna pochodząca z uszkodzonej wirówki mogła wywołać impuls gorącego gazu, który — gdyby nie został powstrzymany — mógł rozejść się po kaskadzie i zniszczyć inne urządzenia. System reagowania miał szybko podejmować działania i zatrzymywać wypływ gazu z wirówki, jednak Stuxnet wyłączał ten system, dlatego nic nie chroniło kaskady przed szkodami.

Stuxnet 0.5 działał więc wielokierunkowo. Zwiększał ciśnienie, by uszkodzić wirówki i zniszczyć gaz, wyrzucał część gazu z kaskady, przez co nie można go było wzbogacić, a także zmniejszał liczbę pracujących wirówek, co przekładało się na mniejszą ilość wzbogaconego uranu uzyskiwaną na końcu kaskady. Nie wiadomo, jak skuteczna była ta wersja Stuxneta. Jednak z raportów MAEA wynika, że miała ona pewien wpływ na irański program.

Instalacja kASKAD W NATANZIE odbywała się w trzech etapach. Każdy z nich inspektorzy z MAEA obserwowali w trakcie swoich wizyt[25]. Najpierw umieszczana była infrastruktura kaskady — rurki, pompy i zawory. Następnie technicy instalowali wirówki i uruchamiali ich silniki, aby wprawić

[24] Różne systemy stale monitorowały dopływ prądu do wirówek, ich szybkość i poziom wibracji, ciśnienie i temperaturę gazu, a także temperaturę wody używanej do ogrzewania lub schładzania urządzeń.

[25] Inspektorzy MAEA odwiedzali Natanz mniej więcej 24 razy rocznie. Co 3 miesiące publikowali raport z liczbą odnotowanych w czasie ostatniej wizyty wirówek, które obracały się w próżni, ale nie zawierały jeszcze gazu, oraz wirówek wzbogacających już uran. Raporty obejmowały też ilość gazu wprowadzonego przez techników do kaskad i ilość wyprodukowanego wzbogaconego uranu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

urządzenia w ruch. Na tym etapie pompy próżniowe usuwały powietrze, które mogło spowodować nadmierne tarcie i generowanie ciepła. Gdy wirówki osiągały optymalną prędkość, wprowadzany był do nich gaz w celu rozpoczęcia wzbogacania go.

Iran rozpoczął instalowanie wirówek w hali A (jednej z dwóch obszernych podziemnych hal w Natanzie) na początku 2007 r. Hala według projektu miała mieścić osiem dużych sal lub jednostek — od A21 do A28. W każdej sali można było umieścić 18 kaskad. Każda kaskada miała obejmować 164 wirówki, co łącznie dawało 2952 wirówki w każdej jednostce[26].

Technicy rozpoczęli instalowanie pierwszych wirówek w jednostce A24 w lutym tego roku i planowali umieszczenie do maja wszystkich kaskad w jednostce. Tak się jednak nie stało[27]. W połowie sierpnia gaz wzbogacało tylko 12 kaskad. Instalowanie pozostałych urządzeń trwało do listopada. Ale wtedy widoczne stały się już oznaki problemów. Technicy wprowadzali do wirówek mniej gazu, niż mogły one pomieścić, i utrzymywali część gazu w buforze między punktem podawania materiału a kaskadami. Od lutego do listopada do zasobnika podawczego wprowadzono 1670 kg gazu, jednak 400 kg pozostawało w buforze, dlatego do kaskad trafiło tylko 1240 kg materiału. Co więcej, kaskady produkowały znacznie mniej wzbogaconego uranu, niż oczekiwano. Powinny dać 124 kg nisko wzbogaconego uranu — 10% ilości wprowadzonej do kaskad. Zamiast tego Irańczycy otrzymali tylko 75 kg wzbogaconego materiału[28]. Ten trend utrzymywał się przez większość 2007 r. Przez ten czas ilość produkowanego materiału była nieproporcjonalnie niska do ilości wprowadzonego gazu. Ponadto poziom wzbogacenia też był niski. Technicy twierdzili, że wzbogacają gaz do 4,8%, natomiast z testów MAEA wynikało, że uzyskane wyniki wynosiły od 3,7% do 4,0%.

---

[26] W przypisie 29. na s. 303 znajdziesz opis dokładnie znanej Stuxnetowi konfiguracji hali A. Iran później, w listopadzie 2010 r., zwiększył liczbę wirówek na kaskadę. Jednak do tego czasu liczba ta pozostawała stała i wynosiła 164.

[27] Raport MAEA dla Rady Gubernatorów, „Implementation of the NPT Standards Agreement and Relevant Provisions of Security Council Resolution 1737 (2006) in the Islamic Republic of Iran", 22 lutego 2007 (*https://www.iaea.org/sites/default/files/gov2007-08.pdf*).

[28] Raport MAEA dla Rady Gubernatorów, „Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions 1737 (2006) and 1747 (2007) in the Islamic Republic of Iran", 15 listopada 2007 (*https://www.iaea.org/sites/default/files/gov2007-58.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Czy był to efekt działania Stuxneta 0.5, który manipulował przy zaworach i wpływał na poziom wzbogacenia uranu? Trudno to z całą pewnością stwierdzić, jednak problemy zostały zauważone przez osoby z zewnątrz. W raporcie NIE z 2007 r. opublikowanym przez Stany Zjednoczone w grudniu napisano, że Iran miał „poważne problemy techniczne z obsługą" wirówek. Wirówki psuły się z częstotliwością o 20% wyższą od spodziewanej. Wysoki urzędnik MAEA powiedział Davidowi Albrightowi, że uszkodzenia wynikały m.in. z przesyłania częściowo wzbogaconego gazu do zasobników na odpady, co zapewne było powodem niewielkiej ilości wyprodukowanego materiału[29].

W tym czasie Albright i jego współpracownicy przypisywali dużą liczbę uszkodzeń niskiej jakości projektom wirówek i temu, że Iran „wciąż się uczy, z jakimi trudnościami wiąże się obsługa dużej liczby wirówek". Jednak problemy były zgodne z tym, co by się stało w wyniku manipulowania zaworami przez Stuxneta 0.5.

Niezależnie od przyczyn Iran nie mógł sobie pozwolić na marnowanie uranu w postaci gazowej. Kraj posiadał ograniczone zasoby zaimportowanego uranu, a kopalnia w Gachinie nie zapewniała materiału w ilości wystarczającej do podtrzymania programu nuklearnego[30].

Od listopada 2007 r. do lutego 2008 r. technicy nie instalowali nowych kaskad. Zamiast tego skupili się na próbie ustalenia przyczyn problemów. Od lutego sytuacja zaczęła się zmieniać. Gdy Ahmadineżad wiosną odbył triumfalną wizytę w zakładzie, kaskady działały bardziej stabilnie, a liczba uszkodzeń spadła. Poziom wzbogacenia był stabilny i wynosił 4%, a choć wcześniej technicy napełniali wirówki tylko do połowy, teraz umieszczali w nich 85% dopuszczalnej ilości gazu. Nawet wydajność pojedynczych urządzeń wzrosła.

---

[29] Urzędnik z MAEA prywatnie poinformował ISIS o psujących się wirówkach i utracie gazu.

[30] David Albright, Jacqueline Shire, Paul Brannan, „Is Iran Running Out of Yellowcake?", *Institute for Science and International Security*, 11 lutego 2009 (*http://isis-online.org/publications/iran/Iran_Yellowcake.pdf*); Barak Ravid, „Israel Slams Clinton Statement on Nuclear Iran", *Ha'aretz*, 22 lipca 2009; Mark Fitzpatrick, „Statement Before the Senate Committee on Foreign Relations", 3 marca 2009 (*http://www.iranwatch.org/sites/default/files/us-sfrc-fitzpatrick-iranrealities-030309.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Wszystko wskazywało na to, że Iran poradził sobie z problemami kaskad. Technicy zaczęli pospiesznie instalować kaskady. Robili to znacznie szybciej, niż sugerowały rozsądek lub ostrożność. Gdy tylko zamontowali jedną kaskadę, wprowadzali do niej gaz, po czym przystępowali do instalacji następnej. W maju 2008 r. Iran posiadał 3280 wirówek wzbogacających gaz. Do sierpnia ta liczba wzrosła do 3772, co oznaczało 500 wirówek dodanych w trzy miesiące[31].

W Iranie panowała duża presja polityczna na szybkie realizowanie programu nuklearnego. Sankcje ONZ-etu i brak postępów w negocjacjach z Zachodem irytowały irańskich przywódców. Mieli oni dosyć opóźnień. Jednak nagłe przyspieszenie prac było nierozważne, a irańscy naukowcy i inżynierowie zapewne tego nie pochwalali. Nawet w normalnych warunkach instalacja wirówek i zapewnienie ich prawidłowego działania to skomplikowane zadanie. Jeśli dodać do tego podatność modelu IR-1 na awarie, tak duży pośpiech w pracach nie miał sensu.

„Z perspektywy inżynieryjnej było to nieostrożne, ponieważ skoro technicy ledwo co radzili sobie z obsługą kaskady ze 164 wirówkami, po co się spieszyć i próbować zarządzać 18 lub 30 kaskadami jednocześnie? — powiedział Albright. — Inżynier zaleciłby, aby robić to bardzo powoli i przed zmianą skali działalności dobrze zrozumieć, jak sprawić, by wszystkie elementy współpracowały jako jedna całość"[32].

W tym okresie wystąpiły tylko nieliczne problemy. Do końca lata technicy w Natanzie musieli poczuć pewność, że wcześniejsze trudności pozostawili już za sobą. I wtedy sytuacja znów się pogorszyła.

Raporty MAEA przedstawiają tę historię w suchych liczbach.

W trakcie wizyty z kwietnia 2008 r. Ahmadineżad optymistycznie ogłosił, że technicy niedługo dodadzą 6000 wirówek do 3000 urządzeń już zainstalowanych w podziemnej hali. Jednak po dojściu w sierpniu do poziomu 3772 wirówek technicy wstrzymali prace i przez kolejne trzy miesiące

[31] Gaz był wtłaczany do 18 kaskad z jednostki A24 i do 5 kaskad z jednostki A26. Następna kaskada z tej ostatniej pracowała już w próżni, a technicy pracowali nad kolejnymi 12 kaskadami. Zob. raport Rady Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions 1737 (2006), 1747 (2007) and 1803 (2008) in the Islamic Republic of Iran", 15 września 2008 (*https://www.iaea.org/sites/default/files/gov2008-38.pdf*).

[32] Z wywiadu przeprowadzonego z Albrightem przez autorkę w styczniu 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

nie instalowali nowych urządzeń. Poziom produkcji uranu też znacznie spadł. Od początku 2007 r. (czyli od momentu rozpoczęcia wzbogacania) technicy wtłoczyli do kaskad 7600 kg gazu. Do sierpnia 2008 r. wirówki wyprodukowały tylko 480 kg wzbogaconego uranu zamiast oczekiwanych 760 kg. Niska produkcja utrzymywała się przez resztę 2008 r. Od sierpnia do listopada technicy przesłali do kaskad 2150 kg gazu, a uzyskali tylko 150 kg wzbogaconego uranu. Podobnie jak w 2007 r. zaczęli tracić nieoczekiwanie dużą ilość gazu.

Mimo tych wszystkich problemów rok 2008 był dla Iranu lepszy niż 2007[33]. W całym 2007 r. w Natanzie wyprodukowano tylko 75 kg wzbogaconego uranu. Do końca 2008 r. ta wartość wzrosła do 630 kg. Albright i jego współpracownicy z ISIS oszacowali, że w optymalnych warunkach Iran może przekształcić 700 – 800 kg nisko wzbogaconego uranu w 20 – 25 kg uranu odpowiedniego dla celów militarnych, co wystarczało do zbudowania prostej broni atomowej. Jednak nie dało się ukryć faktu, że irański program nuklearny nie znajdował się na oczekiwanym poziomie.

Wystąpienie problemów pod koniec 2008 r. było zbieżne z tym, jak miał działać Stuxnet 0.5. Gdy robak zainfekował model 417, potrzebny był czas na przeprowadzenie sabotażu. Rekonesans trwał przynajmniej miesiąc. W tym okresie Stuxnet rejestrował dane odtwarzane operatorom, a przed rozpoczęciem sabotażu kaskady musiały być aktywne przez określony czas (przynajmniej 35 dni w przypadku pojedynczej kaskady lub ponad 297 dni w sumie dla sześciu kaskad). Po zakończeniu ataku mijało 35 dni do jego ponowienia. Problemy z końca 2008 r. dotyczyły głównie jednostki A26, w której technicy rozpoczęli instalowanie wirówek wiosną. Jeśli Stuxnet został umieszczony w sterownikach tej jednostki pod koniec 2007 r. lub na początku 2008 r., mogły minąć miesiące do momentu pojawienia się negatywnych skutków ataku, wynikających ze wzrostu ciśnienia w wirówkach.

Mniej więcej w tym samym czasie człowiek o kanadyjsko-irańskich korzeniach próbował kupić od dwóch zachodnich producentów partię mierników ciśnienia, aby wysłać je do Iranu. Te czujniki służyły m.in. do pomiaru ciśnienia gazu w wirówkach. Od grudnia 2008 r. do marca 2009 r.

[33] David Albright, Jacqueline Shire, Paul Brannan, „IAEA Report on Iran: Centrifuge Operation Significantly Improving; Gridlock on Alleged Weaponization Issues", 15 września 2008 (*http://isis-online.org/publications/iran/ISIS_Report_Iran_15September2008.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Mahmoud Yadegari kupił dziesięć mierników za 11 tys. dolarów i przesłał dwa z nich przez Dubaj do Iranu. Złożył też zamówienie na 20 kolejnych urządzeń w drugiej firmie, ta jednak odrzuciła transakcję, gdy nie zdołała potwierdzić tożsamości docelowego odbiorcy. Yadegari został aresztowany w kwietniu, gdy władze otrzymały informację o podejrzanym zamówieniu[34]. Czy Iran próbował wtedy kupić mierniki, aby zastąpić urządzenia, które najwyraźniej nie sprawdzały się w Natanzie? A może nie było powiązania między działaniami Yadegariego a problemami w Natanzie?

Na początku 2009 r. irańscy technicy zaczęli szybko dodawać nowe wirówki i kaskady do jednostki A26. Do lutego w próżni działało już dziewięć kaskad. Jednak do wirówek z tych kaskad nie pompowano na razie gazu. W przeszłości technicy zaczynali wtłaczać gaz do nowych kaskad wkrótce po ich zainstalowaniu. Tym razem z jakichś powodów tego nie robili. Jednocześnie poziom SWU (określający, ile pracy każda zamontowana wirówka wykonuje w procesie wzbogacania) gwałtownie spadł z 0,8 do 0,55 dla wirówek z jednostek A24 i A26. Poziom wzbogacenia też spadł z 4%, która to wartość utrzymywała się przez większość 2008 r., do 3,49%. Jeśli były to skutki działania Stuxneta, wydawało się, że ta cyfrowa broń robiła dokładnie to, do czego została zaprojektowana.

Wtedy jednak napastnicy zdecydowali się zastosować nowe rozwiązanie.

NA POCZĄTKU 2009 r. prezydent elekt Barack Obama został zaproszony do Białego Domu na spotkanie z prezydentem Bushem w celu odbycia standardowej rozmowy między nowym prezydentem a jego poprzednikiem, przygotowującej do przekazania sterów państwa. W trakcie rozmowy Bush opisał szczegóły cyfrowego ataku i wyrafinowane sztuczki, jakie robak wykonywał w ciągu ostatniego roku, aby zaszkodzić wirówkom w Natanzie[35]. Udało się osiągnąć postępy w spowalnianiu irańskiego programu, jednak aby zapewnić operacji sukces, potrzebne było jeszcze trochę czasu. Kontynuacja operacji wymagała autoryzacji ze strony urzędującego prezydenta, co oznaczało, że Obama musiał ponownie wydać na nią zgodę. Ponieważ

[34] Yadegari został skazany, a wyjaśnienia trybunału sprawiedliwości w Ontario wraz ze szczegółowym opisem powodów wydania tego wyroku można znaleźć w witrynie organizacji ISIS: *http://isis-online.org/uploads/isis-reports/documents/Yadegari_Reasons.pdf*.

[35] Broad, Markoff, Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

inne rozwiązania do tej pory zawodziły, a jedyną sensowną alternatywą było bombardowanie, Obamy nie trzeba było długo przekonywać[36].

Latem 2008 r., jeszcze w trakcie kampanii prezydenckiej, Obama odbył krótką wizytę w Izraelu, gdzie powiedział Izraelczykom, że rozumie ich problemy. Stwierdził, że wyposażony w broń atomową Iran byłby „poważnym zagrożeniem" dla pokoju nie tylko na Bliskim Wschodzie, ale też na świecie[37]. Obiecał, że pod jego przywództwem wszystkie opcje pozwalające zapobiec zdobyciu broni nuklearnej przez Iran pozostaną otwarte. Choć oznaczało to także możliwość interwencji militarnej, Obama, podobnie jak Bush, chciał tego za wszelką cenę uniknąć. Dlatego utajniona operacja z wykorzystaniem bajtów zamiast bomb była bardziej atrakcyjnym rozwiązaniem.

Obejmując urząd, Obama już zmagał się z presją z wielu stron. Kanałami dyplomatycznymi nie udało się uzyskać postępów. Nieskuteczne okazały się również sankcje. Istniały też obawy przed tym, że Izraelczycy mogą wziąć sprawy w swoje ręce, jeśli Stany Zjednoczone szybko nie pokażą jakichś efektów własnych działań. Z tych i innych powodów Obama zdecydował się nie tylko ponownie autoryzować program cyfrowego sabotażu, ale też zintensyfikować go. To w takim kontekście dał zielone światło nowej, bardziej agresywnej wersji Stuxneta, która atakowała konwertery częstotliwości w Natanzie.

Po co jednak przeprowadzać nowy atak, skoro pierwszy przynosił sukcesy? Atak na zawory był skuteczny, ale powolny. Twórcom Stuxneta kończył się czas. Potrzebowali szybszego ataku, który bardziej bezpośrednio dotykałby wirówek i definitywnie powstrzymywał irański program. Chcieli też zmylić techników nowym zestawem problemów.

Paradoksalne jest to, że gdy Obama autoryzował nowy atak wymierzony w irańskie systemy komputerowe, ogłaszał też nowe federalne inicjatywy na rzecz zabezpieczania cyberprzestrzeni i infrastruktury krytycznej w Stanach Zjednoczonych, aby chronić je przed dokładnie takimi uszkodzeniami, jakie

[36] Mike Shuster, „Inside the United States' Secret Sabotage of Iran", *NPR.org*, 9 maja 2011 (*http://www.npr.org/2011/05/09/135854490/inside-the-united-states-secret-sabotage-of-iran*). Spotkanie prezydenta Busha z Barackiem Obamą zostało opisane w: Sanger, *Confront and Conceal*, s. 200 – 203.

[37] Rebecca Harrison, „Obama Says Nuclear Iran Poses Grave Threat", Reuters, 23 lipca 2008 (*http://www.reuters.com/article/us-iran-usa-obama-idUSL23104041320080723*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

powodował Stuxnet[38]. W przemówieniu kilka tygodni po inauguracji powiedział, że infrastruktura cyfrowa jest strategicznym zasobem kraju, a jej ochrona stanowi priorytet w obszarze bezpieczeństwa narodowego. „Zadbamy o to, aby te sieci były bezpieczne, godne zaufania i odporne — oświadczył. — Będziemy zniechęcać do ataków, zapobiegać im, wykrywać je i chronić się przed nimi, a także szybko dokonywać napraw w obliczu zakłóceń lub uszkodzeń"[39].

Gdy Obama ponownie autoryzował utajnioną operację, pojawiła się groźba jej ujawnienia. Nie było tajemnicą, że Stany Zjednoczone i sojusznicy tego kraju angażowali się w sabotaż irańskiego programu nuklearnego. W lutym 2009 r. londyński dziennik „Telegraph" doniósł, że Izrael rozpoczął szeroko zakrojoną utajnioną wojnę przeciw irańskiemu programowi, w której udział brali zabójcy, firmy przykrywki, podwójni agenci i sabotażyści[40]. W artykule były oficer CIA zdawał się sugerować istnienie Stuxneta, ujawniając, że sabotaż miał spowalniać postępy programu w taki sposób, że Irańczycy nigdy się nie dowiedzą, co spowodowało problemy. Powiedział też, że celem było „opóźniać, opóźniać, opóźniać do czasu wymyślenia innego rozwiązania lub podejścia. […] To dobra polityka, jeśli nie można zniszczyć wroga drogą wojskową, co prawdopodobnie niosłoby za sobą nieakceptowane ryzyko".

Mniej więcej w tym samym czasie „New York Times" także poinformował o nowej utajnionej kampanii przeciw Iranowi, nie podał jednak szczegółów[41].

Nie wiadomo, czy Irańczycy przeczytali te informacje, a jeśli to zrobili, to czy powiązali je z problemami z Natanzie. Z pewnością jednak byli świadomi zagrożenia sabotażem, którego doświadczyli już w 2006 r. w związku z zasilaczami z Turcji. Jednak podejrzewanie sabotażu to jedna sprawa, a wskazanie konkretnych części lub komponentów, które zostały nim dotknięte, to coś zupełnie innego.

---

[38] W maju tego roku ogłosił utworzenie stanowiska głównego doradcy ds. cyberbezpieczeństwa. Jego zadaniem miała być pomoc w zabezpieczaniu amerykańskiej infrastruktury krytycznej przed cyberatakami.

[39] Kim Zetter, „Obama Says New Cyberczar Won't Spy on the Net", *Wired*, 29 maja 2009 (*https://www.wired.com/2009/05/netprivacy*).

[40] Philip Sherwell, *Israel Launches Covert War Against Iran*, „Telegraph", 16 lutego 2009.

[41] David Sanger, *U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site*, „New York Times", 10 stycznia 2009.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy napastnicy przygotowywali się do uruchomienia nowej wersji Stuxneta, Obama spełniał związane z Iranem obietnice z kampanii wyborczej. W trakcie kampanii deklarował, że podejmie bardziej zdecydowane działania dyplomatyczne wobec Iranu. W ramach wypełnienia tych obietnic dokonał bezprecedensowego kroku i podczas transmitowanego w telewizji przemówienia inauguracyjnego zwrócił się bezpośrednio do świata islamskiego. „Szukamy nowej drogi naprzód, opartej na wzajemnym uwzględnianiu interesów i szacunku — powiedział. — [Te słowa kieruję do] tych przywódców z całego świata, którzy dążą do konfliktów lub zrzucają winę za bolączki swojego społeczeństwa na Zachód: wiedzcie, że wasz lud rozliczy was z tego, co potrafiliście zbudować, a nie z tego, co zniszczyliście”[42].

Obama ponownie zwrócił się do Irańczyków 20 marca, kiedy zaapelował do przywódców tego kraju i jego mieszkańców w przemówieniu transmitowanym przez *Głos Ameryki* w Nouruz, irański Nowy Rok.

„W okresie nowych początków chciałbym jasno przemówić do irańskich przywódców” — powiedział. Stany Zjednoczone były zainteresowane budowaniem konstruktywnych stosunków z Iranem, „uczciwych i opartych na wzajemnym szacunku”, i dążyły do przyszłości, w której Irańczycy, ich sąsiedzi i społeczność międzynarodowa mogliby żyć „w większym bezpieczeństwie i pokoju”. Przemówienie zakończył cytatem z perskiego poety Sadiego: „Dzieci Adama są dla siebie rękami i nogami, z tej samej bowiem zostali stworzeni istoty”. Stwierdził też, że Stany Zjednoczone są przygotowane do wyciągnięcia ręki w geście przyjaźni i pokoju, jeśli Irańczycy „są gotowi najpierw otworzyć pięść”[43].

Jednak gdy Obama wyciągał jedną metaforyczną rękę w geście pokoju wobec Iranu, inne ręce przygotowywały nową serię cyfrowych ataków na Natanz.

[42] Zob.: *https://obamawhitehouse.archives.gov/blog/2009/01/21/president-barack-obamas-inaugural-address.*

[43] Zob.: *https://obamawhitehouse.archives.gov/the-press-office/2015/03/19/remarks-president-obama-nowruz.*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 17

TAJEMNICA WIRÓWEK

Dwa tygodnie przed uruchomieniem nowego ataku były dla Irańczyków burzliwe. Dwunastego czerwca 2009 r. odbyły się wybory prezydenckie, w których wzięli udział sprawujący urząd Mahmud Ahmadineżad i aspirujący do stanowiska Mir-Hosejn Musawi. Wyniki nie były zgodne z oczekiwaniami. Miał to być wyrównany pojedynek, jednak gdy dwie godziny po zamknięciu lokali wyborczych zostały ogłoszone wyniki, okazało się, że Ahmadineżad wygrał stosunkiem 63% do 34%. Wyborcy uznali to za oszustwo, a następnego dnia tłumy gniewnych demonstrantów wyszły na ulice Teheranu, aby zamanifestować swoje oburzenie i brak zaufania do wyników. Według doniesień mediów był to największy cywilny protest w kraju od czasu obalenia szacha w trakcie rewolucji z 1979 r. Manifestacje szybko przerodziły się w zamieszki. Demonstranci zaczęli niszczyć sklepy i podpalać kosze na śmieci, a policja i siły Basij (lojalna wobec rządu milicja w cywilnych ubraniach) próbowali rozproszyć manifestantów za pomocą pałek, paralizatorów i kul.

Tej niedzieli Ahmadineżad wygłosił prowokacyjne przemówienie z okazji zwycięstwa. Zadeklarował nadejście nowej ery dla Iranu i zbagatelizował protestantów, nazywając ich nikim więcej jak kibicami piłkarskimi rozżalonymi z powodu porażki ich zespołu. Demonstracje trwały jednak przez cały tydzień, a 19 czerwca w próbie uspokojenia tłumów ajatollah Ali Chamenei zaakceptował wyniki wyborów, stwierdzając, że różnica między kandydatami

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

— 11 mln głosów — była zbyt duża, aby można ją było osiągnąć za pomocą fałszerstw. Tłumów jednak to nie uspokoiło.

Następnego dnia Neda Agha-Soltan, 26-letnia kobieta, została unieruchomiona w spowodowanym przez manifestantów korku i zastrzelona przez snajpera po tym, jak wraz ze swoim nauczycielem muzyki wyszła z samochodu, by przyjrzeć się demonstracji.

Dwa dni później, w poniedziałek 22 czerwca, organ nadzorujący wybory w Iranie, Rada Strażników Rewolucji, oficjalnie uznał Ahmadineżada zwycięzcą. Po prawie dwóch tygodniach protestów w Teheranie zapanował niezwykły spokój. Policja zastosowała gaz łzawiący i ostrą amunicję do rozpędzenia demonstrantów, a większość z nich opuściła już ulice. Tego popołudnia, ok. 16:30 czasu lokalnego, gdy Irańczycy otrząsali się z szoku i smutku spowodowanego wydarzeniami poprzednich dni, została skompilowana i uruchomiona nowa wersja Stuxneta[1].

GDY NA ULICACH Teheranu panował chaos, w Natanzie było stosunkowo spokojnie. Około 1 stycznia technicy zaczęli ponownie instalować nowe wirówki. Do końca lutego było ich 5400 — wartość bliska 6000 urządzeń, jakie Ahmadineżad obiecał poprzedniego roku. Nie wszystkie z tych wirówek wzbogacały już uran, jednak przynajmniej technicy robili postępy. Do czerwca liczba urządzeń wzrosła do 7052, z czego 4092 wzbogacały materiał[2]. Oprócz 18 kaskad wzbogacających gaz w jednostce A24 obecnie robiło to też 12 kaskad z jednostki A26. Dodatkowych siedem kaskad zostało zainstalowanych i umieszczonych w próżni w jednostce A28. Były one gotowe do pobierania gazu.

---

[1] Znacznik czasu w wersji Stuxneta z czerwca 2009 r. wskazywał na to, że napastnicy skompilowali złośliwe oprogramowanie 22 czerwca o 16:31 czasu lokalnego (z komputera, na którym skompilowano kod). Pierwsza ofiara została zaatakowana następnego dnia o 4:40 (czasu lokalnego z komputera ofiary). Dawało to różnicę 12 godz., choć zależała ona od strefy czasowej komputera, na którym przeprowadzono kompilację. Czas infekcji pochodzi z pliku dziennika ukrytego w każdej znalezionej kopii Stuxneta. Za każdym razem gdy Stuxnet infekował komputer, rejestrował w tym dzienniku czas (oparty na wewnętrznym zegarze komputera). Nie wiadomo, czy napastnicy rozpoczęli atak zaraz po skompilowaniu pliku i złośliwe oprogramowanie po 12 godz. dotarło do ofiary, czy czekali z rozpoczęciem akcji do następnego dnia.

[2] David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*, Free Press, Nowy Jork 2010, s. 202 – 203.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Poprawiała się też wydajność wirówek. Latem 2009 r. dzienna produkcja nisko wzbogaconego uranu wzrosła o 20% i pozostawała stała[3]. Mimo wcześniejszych problemów Iran przekroczył techniczny punkt graniczny i zdołał wyprodukować 839 kg nisko wzbogaconego uranu. Ta ilość pozwalała myśleć o budowie broni atomowej[4]. Gdyby Iran kontynuował produkcję w takim tempie, w ciągu roku uzyskałby wystarczająco dużo wzbogaconego uranu do dwóch bomb atomowych[5]. Te szacunki były oparte na możliwościach obecnie zainstalowanych w Natanzie wirówek IR-1. Jednak Iran w niewielkiej kaskadzie w zakładzie pilotażowym zainstalował już wirówki IR-2. Po zakończeniu testów technicy zaczęli instalować te urządzenia w podziemnej hali, co wymagało zmiany szacunków. Aby w ciągu roku wyprodukować ilość uranu wystarczającą do budowy broni atomowej, potrzeba było 3000 wirówek IR-1, ale tylko 1200 wirówek IR-2.

Gdyby nie uderzył Stuxnet 1.001, który pojawił się pod koniec czerwca.

Chcąc umieścić broń w zakładzie, napastnicy przeprowadzili atak na komputery czterech firm. Każda z nich zajmowała się kontrolą procesów przemysłowych lub zarządzaniem nimi. Firmy te albo produkowały sprzęt i montowały komponenty, albo instalowały systemy kontroli procesów przemysłowych. Wybór tych organizacji zapewne wynikał z ich związków z Natanzem. Firmy realizowały kontrakty w zakładzie i stanowiły bramę, przez którą można było wprowadzić Stuxneta do Natanzu za pośrednictwem zainfekowanych pracowników.

By zagwarantować dotarcie kodu do celu, nową wersję Stuxneta wyposażono w dwa dodatkowe sposoby rozprzestrzeniania się (w porównaniu do poprzedniej). Stuxnet 0.5 potrafił się powielać tylko za pomocą infekcji plików projektu z narzędzia Step 7. Były to pliki służące do programowania sterowników PLC Siemensa. Nowa wersja potrafiła rozprzestrzeniać się za pomocą pendrive'ów z wykorzystaniem mechanizmu automatycznego uruchamiania z Windowsa lub w sieci lokalnej ofiary, posługując się eksploitem typu zero-day atakującym program do obsługi drukowania,

---

[3] David Albright, Jacqueline Shire, „IAEA Report on Iran: Centrifuge and LEU Increases; Access to Arak Reactor Denied; No Progress on Outstanding Issues", 5 czerwca 2009 (*http://isis-online.org/publications/iran/Iran_IAEA_Report_Analysis_5June2009.pdf*).

[4] Albright, *Peddling Peril*, s. 202 – 203.

[5] Albright, Shire, „IAEA Report…", 5 czerwca 2009.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

który to eksploit został później znaleziony w kodzie przez badaczy z Kaspersky'ego i Symanteca.

Z plików dziennika ze Stuxneta wynika, że pierwszą ofiarą była firma Foolad Technique. Została zainfekowana o 4:40 we wtorek 23 czerwca[6]. Do momentu zaatakowania następnej firmy minął prawie tydzień.

W następny poniedziałek ok. 5000 manifestantów przeszło w milczeniu ulicami Teheranu do meczetu Ghoba, upamiętniając ofiary zabite w trakcie niedawnych protestów związanych z wyborami. Późnym wieczorem, ok. 23:20, Stuxnet zaatakował maszyny należące do drugiej ofiary, firmy Behpajooh.

Łatwo można zrozumieć, dlaczego to ona stała się celem. Była to firma inżynieryjna z Isfahanu, lokalizacji nowego irańskiego zakładu przetwarzaniu uranu, który miał przekształcać oczyszczoną rudę uranu w gaz przeznaczony do wzbogacania w Natanzie. W Isfahanie zlokalizowane było też irańskie Centrum Technologii Nuklearnych, uważane za siedzibę główną irańskiego programu budowy broni atomowej. Behpajooh wymieniona była też w dokumentach amerykańskiego sądu federalnego w związku z zakupem przez Iran niedozwolonych materiałów[7].

Behpajooh działała w branży instalowania i programowania systemów kontroli i automatyzowania procesów przemysłowych, w tym systemów Siemensa. W witrynie firmy nie występują wzmianki o Natanzie, napisano tam jednak, że Behpajooh instalowała sterowniki PLC S7-400 Siemensa, a także oprogramowanie Step 7 i WinCC oraz moduły komunikacyjne Profibus w stalowni w Isfahanie. Był to ten sam sprzęt, który stanowił cel Stuxneta w Natanzie.

Siódmego lipca o 5:00, dziewięć dni po ataku na Behpajooh, Stuxnet trafił na komputery firmy Neda Industrial Group, a także organizacji opisanej w dziennikach jako CGJ, którą prawdopodobnie była Control Gostar Jahed. Obie firmy projektowały lub instalowały systemy kontroli procesów przemysłowych.

---

[6] Foolad Technique korzysta z domeny ISIE. Możliwe, że ISIE została przejęta przez firmę Foolad lub jest jednym z działów tej ostatniej.

[7] W 2006 r. Amerykanin pochodzenia irańskiego został oskarżony o próbę przemytu zakazanych technologii wojskowych do Iranu. Zakupił on czujniki ciśnienia od firmy z Minneapolis i przesłał je do pośrednika z Dubaju, który miał przekazać je firmie Behpajooh. Zob. *Dubai Firm Implicated in Iran 'Bomb Component's Investigation in US*, „Khaleej Times", 12 maja 2006.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Neda projektowała i instalowała systemy kontroli, urządzenia precyzyjne i systemy elektryczne w branży ropy naftowej i gazu, a także w elektrowniach, kopalniach i zakładach przetwórczych w Iranie. W latach 2000 i 2001 zainstalowała sterowniki PLC S7 Siemensa u kilku irańskich operatorów gazociągów. Montowała też systemy S7 Siemensa w stalowni w Isfahanie[8]. Neda, podobnie jak Behpajooh, znalazła się na liście firm obserwowanych w związku z układami o nierozprzestrzenieniu broni z powodu domniemanego udziału w nielegalnych transakcjach. Pojawiła się też w amerykańskim akcie oskarżenia w związku z otrzymaniem przemyconych mikrokontrolerów i innych komponentów[9].

Dwudziestego drugiego lipca, mniej więcej dwa tygodnie po ataku na firmę Neda, zatrudniony w niej inżynier systemów kontroli zgłosił na forum użytkowników produktów Siemensa występujący u pracowników problem z maszynami. Inżynier zamieścił wpis jako użytkownik Behrooz i stwierdził, że we wszystkich komputerach w firmie występuje identyczny problem z generującym komunikat o błędzie plikiem .DLL w oprogramowaniu Step 7. Behrooz podejrzewał, że przyczyną problemu jest wirus rozprzestrzeniany za pomocą pendrive'ów[10].

---

[8] Jednym z klientów firmy Neda była stacja sprężania gazu na wyspie Chark w Iranie. To miejsce jednej z eksplozji, które zwróciły uwagę Erika Chiena w 2010 r. po wykryciu Stuxneta. Według witryny firmy od 2008 do 2010 r. Neda przeprowadzała renowację systemów kontroli w turbosprężarkach stacji. Nie ma dowodów na to, że eksplozja w zakładzie została spowodowana przez cyfrowy sabotaż, jednak to, że Stuxnet zainfekował komputery firmy Neda, pokazuje, jak łatwo byłoby przeprowadzić ataki cyfrowe na inne obiekty w Iranie.

[9] W 2004 r. firma handlowa z Dubaju zamówiła 7500 mikrokontrolerów od producenta z Arizony i skierowała dostawę do Nedy, gdzie sprzęt ewidentnie miał być wykorzystany przez irańskie wojsko. Była to sprawa *US District Court, Mayrow General Trading et al., Indictment*, 11 września 2008 (*http://www.dodig.mil/iginformation/Mayrow%20Superseding%20Indictment.pdf*).

[10] Choć inżynier zamieszczał wpisy jako użytkownik Behrooz, podpisywał je M.R. Tajalli. Wyszukiwanie nazwy użytkownika i nazwiska pozwoliło dotrzeć w serwisie LinkedIn i innych źródłach do profilów Mohammada Rezy Tajallego, inżyniera systemów kontroli pracującego dla Nedy od 2006 r. Według profilu z serwisu LinkedIn Tajalli specjalizował się w systemach kontroli dla branży ropy naftowej. Tajalli nie odpowiedział na próby kontaktu ze strony autorki.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy inżynier używał do przenoszenia plików z zainfekowanego do czystego systemu płyt DVD lub CD, wszystko działało poprawnie. Jednak gdy posłużył się pendrive'em, w nowym komputerze występowały te same problemy co w innych maszynach. Pendrive był podstawową metodą rozprzestrzeniania się Stuxneta. Choć Behrooz i jego współpracownicy przeskanowali systemy pod kątem wirusów, nie znaleźli w maszynach złośliwego oprogramowania. Z dyskusji na forum nie wynikało, czy firmie udało się wówczas rozwiązać problem.

Nie wiadomo, jak długo zajęło Stuxnetowi dotarcie do celu po zainfekowaniu maszyn w Nedzie i innych firmach. Jednak między czerwcem a sierpniem liczba wirówek wzbogacających uran w Natanzie zaczęła spadać. Nie da się ustalić, czy był to wyłącznie efekt działania nowej wersji Stuxneta, czy długofalowe skutki pracy starszej wersji. W sierpniu tego roku wzbogacanie uranu odbywało się tylko w 4592 wirówkach, co oznaczało spadek o 328 urządzeń względem czerwca. Problemem ponownie była jednostka A26, w której już wcześniej występowały problemy. W czerwcu w tej jednostce gaz był wzbogacany przez 12 kaskad. Jednak do listopada z połowy z nich usunięto gaz i pracowało tylko sześć pozostałych kaskad. Łączna liczba wirówek wzbogacających uran zmalała do 3936. Był to spadek o 984 urządzenia w ciągu pięciu miesięcy. Ponadto, choć wciąż instalowane były nowe maszyny, gaz nie był pompowany do żadnej z nich. W jednostce A28 zainstalowanych było 17 kaskad, ale żadna z prawie 3000 wchodzących w jej skład wirówek nie wzbogacała gazu.

Najwyraźniej pojawiły się problemy z kaskadami, a technicy nie mieli pojęcia, z czego one wynikają. Zmiany jednak dokładnie odpowiadały temu, do czego napastnicy zaprojektowali Stuxneta.

Nowa wersja Stuxneta zwiększała na 15 min częstotliwość pracy wirników wirówek do 1410 Hz, co oznaczało prędkość ok. 1600 km/h. Po trzech tygodniach częstotliwość na 50 min spadała do 2 Hz[11]. Te zmiany po kilku powtórzeniach prowadziły do uszkodzenia wirówek i wpływały na poziom wzbogacenia gazu.

Jednak Albright i jego współpracownicy ustalili, że osiągnięcie przez wirniki poziomu 1410 Hz, który był dla wirówek najbardziej szkodliwy,

[11] Zob. rozdział 13., s. 244 i 253.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wymagało więcej niż 15 min. W tym czasie urządzenia dochodziły prawdopodobnie tylko do poziomu 1324 – 1381 Hz. Mimo to zmieniająca się szybkość oraz przyspieszanie i spowalnianie pracy przyczyniały się do przyrostowego wzrostu obciążenia oraz uszkadzania wirników. Wzrost szybkości skutkował też zmianą kształtu i utratą równowagi aluminiowych wirówek.

Model IR-1 był z natury podatny na awarie. Źródłem problemu mogły być najdrobniejsze zakłócenia. Na przykład kurz w komorze mógł doprowadzić do zniszczenia urządzenia. Gholam Reza Aghazadeh, szef irańskiej Agencji Energii Atomowej, w wywiadzie z 2006 r. ujawnił, że w początkowej fazie programu wzbogacania wirówki IR-1 często psuły się z powodu znajdujących się w maszynie *zarazków*. Początkowo Irańczycy nie potrafili ustalić, dlaczego wirówki eksplodowały, ostatecznie za przyczynę problemu uznali to, że technicy składali urządzenia bez rękawiczek. Zarazki pozostawione w maszynach dosłownie obracały urządzenia w pył. „Gdy mówię, że maszyna została zniszczona — powiedział Aghazadeh dziennikarzowi — mam na myśli to, że została zmieniona w proch”[12].

U góry i u dołu wirówek znajdowały się łożyska, które pomagały utrzymać urządzenia w równowadze (podobnie balans zachowuje kręcący się bączek)[13]. Wirówki trzeba rozpędzać powoli. Po nabraniu prędkości wyglądają estetycznie i dostojnie. Jednak wystarczy chwila, by wszystko się zmieniło. Gdy wirówka się zachwieje, szybko zaczyna kręcić się w niekontrolowany sposób. Obudowa była solidna i wytrzymała, ale mogła pęknąć wzdłuż (tak jak parówka włożona do kuchenki mikrofalowej) lub wygiąć się, powodując zerwanie zatyczek po obu stronach. Wewnątrz obudowy mogły rozpaść się wirnik i inne komponenty.

Zwiększona prędkość spowodowana przez Stuxneta mogła wywołać wibracje, które po kilku cyklach prowadziły do zużycia się łożysk, utraty przez wirówkę równowagi i przewrócenia się urządzenia. Jednak z powodu

[12] William Broad, *A Tantalizing Look at Iran's Nuclear Program*, „New York Times”, 29 kwietnia 2008.

[13] Wirówki mają zatyczki po obu stronach i utrzymują równowagę dzięki łożyskom kulkowym z osiami. Górna część osi jest przyczepiona do zatyczki umieszczonej u dołu wirówki, natomiast dolna część osi, z łożyskiem, jest przymocowana do sprężyny. Cała ta konstrukcja umożliwia wirówkom lekkie odchylenia w trakcie obracania się, a jednocześnie zapewnia stabilizację. Jednak za duże odchylenia mogą zdestabilizować wirówkę i spowodować zniszczenie części.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

fałszywych danych przekazywanych operatorom technicy nie dostrzegali nadchodzących problemów. Nie byli też w stanie później stwierdzić, co stanowiło przyczynę uszkodzenia urządzeń.

Druga metoda ataku, zmniejszająca częstotliwość pracy wirówek do 2 Hz na 50 min, oznaczała, że napastnicy oprócz niszczenia urządzeń próbowali też obniżać jakość wzbogacanego uranu. Spowolnienie wirówki obracającej się z częstotliwością 1064 Hz do 2 Hz wymaga czasu. Albright i jego zespół ustalili, że w 50 min — do momentu zakończenia sabotażu i przywrócenia normalnej szybkości — można zmniejszyć częstotliwość tylko do ok. 864 Hz. Nawet zmniejszając częstotliwość pracy wirówki o 50 – 100 Hz, Stuxnet mógł zmniejszyć poziom wzbogacenia o połowę. W procesie wzbogacania uranu wirówki muszą stale kręcić się z dużą szybkością, by rozdzielić izotopy ^{235}U i ^{238}U. Zmiana częstotliwości, a zwłaszcza jej zmniejszenie, zakłóca proces rozdzielania. Technicy w Natanzie oczekiwali, że uzyskają w kaskadzie uran o określonej jakości, jednak otrzymywali gaz o zupełnie innych parametrach. Ten efekt był dużo bardziej subtelny niż niszczenie wirówek i sam w sobie nie wystarczyłby do spowolnienia irańskiego programu. Jednak w połączeniu z innymi działaniami pozwalał na sabotaż na innej płaszczyźnie. Spowolnienie wirówek prowadziło nie tylko do spadku poziomu wzbogacenia, ale też do zmian w ilości wzbogacanego uranu. W lutym 2009 r. wirówki osiągnęły poziom ok. 0,62 SWU, natomiast w maju ta wartość spadła do 0,49. W czerwcu i sierpniu te wartości wynosiły od 0,51 do 0,55.

W Stanach Zjednoczonych Albright i jego współpracownicy z ISIS czytali raporty MAEA, zwracając uwagę na zmiany w Natanzie. Nie byli zaskoczeni problemami Irańczyków, ponieważ ich zdaniem technicy zbyt szybko instalowali kaskady w jednostce A26. Albright dowiedział się od informatorów, że technicy w Natanzie, próbując rozwiązać problemy, zmniejszyli prędkość wirówek. Badacz podejrzewał, że chodziło o coś więcej niż standardowe awarie i trudności techniczne. Skontaktował się z informatorami z jednostek rządowych i MAEA, aby ustalić, co się dzieje. Nie otrzymał jednak zadowalających odpowiedzi.

Wraz z nadejściem 2010 r. wskaźniki w Natanzie wciąż spadały. Liczba zainstalowanych wirówek wynosiła 8692, jednak liczba wirówek wzbogacających uran zmalała do 3772, co oznaczało spadek o 1148 urządzeń od czerwca. Do tego czasu problemy występowały głównie w jednostce A26,

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

a teraz zaczęły rozszerzać się na jednostki A24 i A28. Na przykład z jednej z kaskad w jednostce A24 usunięty został gaz[14].

Najbardziej wymowne było to, że technicy zaczęli odłączać i usuwać wirówki w niektórych kaskadach. W sierpniu MAEA zainstalowała w podziemnej hali dodatkowe kamery, aby nadążyć za rozbudową wyposażenia zakładu związaną z instalacją nowych kaskad. Teraz rejestrowała pracowników pospiesznie usuwających wirówki z jednostek. W styczniu MAEA poinformowała, że technicy wymontowali nieokreśloną liczbę wirówek z 11 kaskad z jednostki A26, a ponadto usunęli wszystkie 164 wirówki z kaskady z jednostki A28. Żadna z pozostałych 16 kaskad w jednostce A28 nie wzbogacała uranu[15]. „Washington Post" poinformował później, że w tym czasie wymienione zostały 984 wirówki, co odpowiadało sześciu kompletnym kaskadom.

Jednak zadanie Stuxneta wciąż nie zostało ukończone.

WRAZ ZE ZBLIŻANIEM się końca 2009 r. Stany Zjednoczone wywierały coraz większą presję na Iran, by zakończył program nuklearny.

Pod koniec września wskaźniki w Natanzie wciąż spadały, a prezydent Obama poinformował na szczycie Rady Bezpieczeństwa ONZ-etu dotyczącym nierozprzestrzeniania broni atomowej i rozbrojenia jądrowego, że w Iranie został odkryty nowy tajny zakład wzbogacania uranu. Obiekt był zlokalizowany w bazie wojskowej i znajdował się ponad 45 m pod górą w ośrodku Fordo, ok. 30 km od świętego miasta Kom.

[14] W przeprowadzonych przez autorkę wywiadach kilku informatorów zasugerowało, że wirówki w jednostce A24 mogły być skonfigurowane inaczej niż w jednostce A26. Możliwe, że tych jednostkach używane były różne modele konwerterów częstotliwości. Jeśli tak było, niewykluczone, że Stuxnet 0.5, atakujący zawory w wirówkach i kaskadach, został zastosowany przeciwko jednostce A24, natomiast późniejsze wersje robaka, wymierzone w konwertery częstotliwości, posłużyły przeciw kaskadom z jednostki A26. To wyjaśniałoby, dlaczego kaskady w jednostce A24 powodowały problemy w 2008 r., kiedy wypuszczony został Stuxnet 0.5, a zaczęły działać lepiej w 2009 r., gdy do sabotażu przystąpiła nowsza wersja Stuxneta.

[15] MAEA, „Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolution 1737 (2006), 1747 (2007), 1803 (2008) and 1835 (2008) in the Islamic Republic of Iran", 18 lutego 2010 (*https://www.iaea.org/sites/default/files/gov2010-10.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ten zakład był znacznie mniejszy od obiektu w Natanzie i mógł pomieścić tylko 3000 wirówek (w porównaniu z 47 tys. w Natanzie). Był jednak wystarczająco duży, by w ciągu roku wzbogacić uran do jednej lub dwóch bomb, gdyby Iran zdecydował się wykorzystać materiał w tym celu. „Iran ma prawo do korzystania z energii atomowej w celach pokojowych, aby zaspokoić potrzeby energetyczne kraju. Jednak wielkość i konfiguracja tego obiektu wskazują na to, że celem nie jest program pokojowy" — powiedział Obama, informując o zakładzie w Fordo[16].

Irańczycy poinformowali Muhammada el-Baradeia z MAEA, że nowy zakład jest tylko obiektem rezerwowym dla kompleksu w Natanzie. Stwierdzili, że zagrożenie Natanzu atakami skłoniło ich do stworzenia obiektu awaryjnego. Nowy zakład wciąż był w budowie i miał zostać ukończony w 2011 r. Jednak według amerykańskiego wywiadu prace nad nim zaczęły się między 2002 a 2004 r. Oznaczało to, że inspektorzy z MAEA przez lata w drodze do Natanzu wielokrotnie mijali ten tajny obiekt, nie wiedząc o jego istnieniu. Obama dowiedział się o nim w trakcie rozmowy w Białym Domu odbytej przed inauguracją, jednak agencje wywiadowcze miały informacje na ten temat przynajmniej od 2007 r., kiedy to szef irańskiej gwardii rewolucyjnej zbiegł na Zachód i powiadomił CIA, że Iran gdzieś na terenie kraju buduje drugi tajny zakład wzbogacania uranu. Później za pomocą satelitów udało się znaleźć obiekt w Fordo[17].

Zakład w Fordo, choć mniejszy od kompleksu w Natanzie, stanowił znacznie większe zagrożenie. Natanz był ściśle monitorowany przez inspektorów z MAEA, dlatego było mało prawdopodobne, że Iran potajemnie

[16] „Statements by President Obama, French President Sarkozy, and British Prime Minister Brown on Iranian Nuclear Facility", 25 września 2009, Centrum Kongresowe w Pittsburghu w stanie Pensylwania (*https://obamawhitehouse.archives.gov/the-press-office/2009/09/25/statements-president-obama-french-president-sarkozy-and-british-prime-mi*).

[17] Na obrazach satelitarnych początkowo zauważono w Fordo coś, co wyglądało jak tunele i podziemne prace budowlane. W 2008 r. zobaczono robotników montujących duże cementowe płyty przy wejściu do tunelu. Te płyty przypominały cementowe platformy używane do montażu kaskad w zakładach wzbogacania uranu. Stany Zjednoczone rozważały przez pewien czas wysłanie do Iranu zespołu komandosów w celu uszkodzenia platform, aby spowodować w przyszłości zniszczenie wirówek. Jednak nigdy nie zrealizowano tego ryzykownego planu. Zob. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Crown, Nowy Jork 2012, s. 152 i 155.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wykorzysta materiał nuklearny z tego zakładu w celu wzbogacenia go i uzyskania materiału umożliwiającego budowę broni. Dużo bardziej niepokojące były tajne zakłady, takie jak w Fordo, gdzie Irańczycy mogli bez wiedzy MAEA wzbogacać uran do poziomu pozwalającego uzyskać bombę.

Zakład w Fordo budził tym większe obawy, że został zbudowany pod ponad 30 m skały. Był więc poza zasięgiem dostępnych wówczas bomb penetrujących, a nawet bomb nowej generacji, nad którymi Stany Zjednoczone pracowały[18].

Gordon Brown, premier Wielkiej Brytanii, w reakcji na wiadomości o zakładzie w Fordo nazwał irański program nuklearny „najpilniejszym wyzwaniem w obszarze nierozprzestrzeniania broni jądrowej, przed jakim stoi obecnie świat". Powiedział, że społeczność międzynarodowa nie ma innego wyjścia i musi „postawić wyraźne granice" w związku z irańskim „wieloletnim konsekwentnym zwodzeniem"[19].

Jednak irańscy oficjele wydawali się niewzruszeni ujawnieniem informacji o Fordo i prowokacyjnie stwierdzili, że w następnych latach zamierzają zbudować dziesięć kolejnych zakładów wzbogacania uranu, aby zapewnić paliwo dla planowanego systemu elektrowni atomowych[20]. Szef irańskiej Agencji Energii Atomowej powiedział też, że wszystkie te zakłady miały być ukryte głęboko pod górami, aby były bezpieczne przed atakami[21].

W obliczu informacji o Fordo Izrael zaczął intensywnie nalegać na to, by zrobić coś z irańskim programem nuklearnym. W trakcie listopadowego

---

[18] Rada naukowa ds. obronności, która w 2004 r. doradzała Pentagonowi budowę takiej broni, napisała, że obiekt z tunelami zlokalizowany głęboko pod skałami może stanowić „poważne wyzwanie" nawet dla nowych bomb. „Potrzebnych będzie kilka tysięcy kilogramów materiałów wybuchowych, aby wybić drzwi i wygenerować destrukcyjną falę uderzeniową" — napisano w raporcie. William Broad, *Iran Shielding Its Nuclear Efforts in Maze of Tunnels*, „New York Times", 5 stycznia 2010.

[19] „Statements by President Obama, French President Sarkozy, and British Prime Minister Brown on Iranian Nuclear Facility", Biały Dom.

[20] Rok później, we wrześniu 2010 r., gdy badacze z Symanteca i Ralph Langner wciąż odszyfrowywali ładunek ze Stuxneta, irańska grupa dysydentów, która ujawniła zakład w Natanzie, poinformowała, że posiada informacje o jeszcze jednym tajnym obiekcie wzbogacania uranu. Miał on być budowany w pobliżu miejscowości Abyek, ok. 120 km na zachód od Teheranu. Zob. David E. Sanger, *Dissidents Claim Iran Is Building a New Enrichment Site*, „New York Times", 9 września 2010.

[21] Broad, *Iran Shielding Its Nuclear Efforts*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

spotkania w Tel Awiwie jeden z izraelskich dowódców wojskowych powiedział urzędnikom amerykańskim, że rok 2010 będzie „krytycznym rokiem" w rozgrywce z Iranem. Jeśli inne kraje czegoś szybko nie zrobią, Iran umocni swoje obiekty nuklearne i będzie trudniej je zlikwidować[22]. Stany Zjednoczone w sekrecie obiecały już Izraelowi dostawę produkowanych bomb penetracyjnych nowej generacji, jednak miały one zostać dostarczone dopiero za sześć miesięcy.

W styczniu 2010 r. napięcie wzrosło jeszcze bardziej, gdy w dokumentach, które wyciekły do mediów, ujawnione zostało tajne wojskowe odgałęzienie irańskiego programu badań nuklearnych — FEDAT. Za szefa tego podprogramu uznawany był Mohsen Fakhrizadeh, profesor teherańskiego Imam Hossein University[23]. Miesiąc później MAEA ogłosiła, że otrzymała „ogólnie spójne i wiarygodne" informacje, że Iran pracuje nad bronią atomową. „Rodzi to obawy o to, że Iran prowadził lub prowadzi tajne prace związane z budową ładunku nuklearnego"[24].

Ponadto negocjacje, które miały rozwiać obawy dotyczące rosnących irańskich zapasów nisko wzbogaconego uranu, załamały się. Iran latami utrzymywał, że potrzebuje uranu do produkcji prętów paliwowych do reaktora badawczego w Teheranie, by prowadzić badania nad nowotworami i leczeniem onkologicznym. Mimo to Stany Zjednoczone i inne państwa od zawsze bały się, że uran w pewnym momencie zostanie dodatkowo wzbogacony na potrzeby budowy broni. Dlatego w połowie 2009 r. doradca Białego Domu zaproponował pomysłowy kompromis. Zgodnie z planem Białego Domu Iran miał przesłać większość nisko wzbogaconego uranu do Rosji i Francji, aby te dwa państwa przekształciły materiał na pręty paliwowe dla irańskiego reaktora. Była to bardzo sprytna propozycja, ponieważ zapewniała Iranowi całe potrzebne mu — według deklaracji jego przedstawicieli — paliwo, a jednocześnie uniemożliwiała Irańczykom dalsze wzbogacanie zapasów uranu i uzyskanie materiału pozwalającego na budowę broni.

[22] Depesza Departamentu Stanu USA, „40th Joint Political-Military Group: Executive", 18 listopada 2009. Opublikowana w serwisie WikiLeaks (*https://wikileaks.org/plusd/cables/09TELAVIV2500_a.html*).

[23] Dieter Bednarz, Erich Follath, Holger Stark, *Intelligence from Tehran Elevates Concern in the West*, „Der Spiegel", 25 stycznia 2010.

[24] Erich Follath, Holger Stark, *The Birth of a Bomb: A History of Iran's Nuclear Ambitions*, „Der Spiegel", 17 czerwca 2010.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Irańscy oficjele w 2009 r. powiedzieli, że potrzebują czasu, aby rozważyć propozycję. Dziewiętnastego stycznia poinformowali, że ją odrzucają. Nie było to jednak wszystko. Ogłosili też, że część nisko wzbogaconego uranu wyprodukowanego w podziemnej hali w Natanzie próbują wzbogacić w zakładzie pilotażowym do 20%. Utrzymywali, że taki poziom wzbogacenia jest im potrzebny do badań medycznych[25].

Sześć dni później zespół pracujący nad Stuxnetem rozpoczął przygotowania do nowej serii ataków.

W pierwszym roku urzędowania prezydent Obama uważnie śledził prace nad bronią cyfrową. Wiele zależało od jej skuteczności. Do tej pory informacje były dobre, a nawet lepsze od oczekiwanych. Choć Stuxnet atakował tylko ograniczoną liczbę wirówek, Irańczycy potęgowali działanie robaka, wyłączając całe kaskady, aby dotrzeć do źródła problemów. Skutkowało to dalszymi opóźnieniami w programie. Irańczycy najwyraźniej nadal nie wiedzieli, że problemy kryją się w komputerach kontrolujących kaskady. Nie było więc powodu, by kończyć sabotaż — zwłaszcza w obliczu rosnącej presji na podjęcie działań militarnych przeciw Iranowi.

Dwudziestego piątego stycznia napastnicy podpisali dwa pliki sterownika w Stuxnecie certyfikatem cyfrowym wykradzionym tajwańskiej firmie RealTek, a 1 marca skompilowali kod. Później najwyraźniej czekali.

Dwudziestego marca wypadało święto Nouruz, a Obama ponownie — jak w poprzedni perski Nowy Rok — wygłosił przemówienie na temat pokojowej współpracy z mieszkańcami Iranu. Tym razem mówił bezpośrednio o irańskim programie nuklearnym. „Razem ze społecznością międzynarodową Stany Zjednoczone uznają wasze prawo do energii atomowej wykorzystywanej w celach pokojowych. Nalegamy jedynie na to, abyście przestrzegali tych samych zobowiązań co inne kraje — powiedział. — Mamy świadomość waszych żalów z przeszłości. My też mamy trudną przeszłość, ale jesteśmy gotowi iść naprzód. Wiemy, przeciw czemu występujecie. Teraz powiedzcie nam, do czego dążycie".

[25] Olli J. Heinonen, „Iran Ramping Up Uranium Enrichment", blog Power and Policy, 20 lipca 2011, opublikowane przez Belfer Center w Harvard Kennedy School, 20 lipca 2011 (*https://powerandpolicy.wordpress.com/2011/07/20/iran-ramping-up-uranium-enrichment/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ton wypowiedzi stawał się coraz poważniejszy, gdy Obama czynił zawoalowane aluzje do niedawnego odrzucenia przez Iran propozycji kompromisu w związku z paliwem nuklearnym. „W odpowiedzi na naszą wyciągniętą rękę — powiedział — irańscy przywódcy pokazali nam tylko zaciśniętą pięść”[26].

W tygodniach poprzedzających to przemówienie irańscy technicy ciężko pracowali, aby naprawić problemy spowodowane przez Stuxneta. Przywrócili wzbogacanie we wszystkich 18 kaskadach z jednostki A24, a także wstawili wirówki usunięte z kilku kaskad jednostki A26. Ponadto pompowali więcej gazu do wciąż pracujących wirówek, aby nadrobić stracony czas i zwiększyć ilość wzbogaconego materiału. Nie wiedzieli jednak, że wkrótce znów zostaną zaatakowani.

Obchody perskiego Nowego Roku trwały w Iranie 13 dni, choć tylko pierwsze cztery były oficjalnie wolne od pracy. Dwudziestego trzeciego marca, czwartego dnia obchodów, kiedy większość pracowników była jeszcze w domach razem z rodzinami i przyjaciółmi, zaatakowała nowa wersja Stuxneta. Obejmowała ona ten sam ładunek co wariant z czerwca poprzedniego roku. Była jednak wyposażona w większy zestaw eksploitów typu zero-day i innych mechanizmów rozprzestrzeniania się, w tym w eksploit plików .LNK, który ostatecznie doprowadził do wykrycia robaka.

Mimo tych wszystkich dodatków napastnicy najwyraźniej zaatakowali tym razem tylko jedną firmę — Behpajooh. Nie wiadomo, kiedy uruchomili kod, jednak znalazł się on w pierwszych komputerach tej firmy mniej więcej o 6:00 23 marca. Behpajooh została zaatakowana również w 2009 r., a także była ofiarą akcji z następnego miesiąca — kwietnia 2010 r. Była to jedyna firma zaatakowana przez wszystkie trzy warianty kodu. Wskazywało to na to, że mogła się ona lepiej nadawać do dotarcia do docelowych komputerów w Natanzie niż inne firmy. Niestety, okazało się też, że Behpajooh spowodowała tysiące różnych infekcji w Iranie i innych krajach.

[26] „Remarks of President Obama Marking Nowruz”, Biały Dom, 20 marca 2010 (*https://obamawhitehouse.archives.gov/realitycheck/the-press-office/remarks-president-obama-marking-nowruz*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W kolejnych dniach, gdy pracownicy wracali ze świąt do biur, robak zaczął się bardzo szybko powielać. Najpierw rozprzestrzenił się w biurach firmy Behpajooh w Iranie, Wielkiej Brytanii i Azji, następnie wydostał się na wolność i zaczął infekować inne organizacje w wymienionych krajach i poza nimi[27]. Później, gdy badacze Symanteca analizowali różne próbki Stuxneta zebrane z zainfekowanych komputerów, zdołali powiązać tysiące infekcji z początkowymi atakami w firmie Behpajooh[28].

Nie jest jasne, dlaczego napastnicy akurat wtedy zwiększyli siłę rażenia. Możliwe, że dwa lata, jakie robak spędził w komputerach w Natanzie, sprawiły, że stali się zbyt pewni siebie i nieostrożni. Bardziej prawdopodobne wyjaśnienie jest takie, że wcześniejsze wersje Stuxneta zostały zainstalowane przez człowieka z wewnątrz lub osobę mającą dostęp do docelowych maszyn. Jeśli twórcy Stuxneta utracili później ten dostęp, zapewne uważali, że muszą poprawić możliwości robaka w zakresie rozprzestrzeniania się, by zwiększyć prawdopodobieństwo dotarcia do celu. Jedną z poszlak zgodnych z tym wyjaśnieniem są różne odstępy czasu między kompilacją kodu a zainfekowaniem pierwszych ofiar przez poszczególne wersje Stuxneta. W ataku z czerwca 2009 r. minęło tylko ok. 12 godz. od skompilowania robaka do dotarcia do pierwszej ofiary[29]. Jednak wersja z marca 2010 r. została skompilowana rankiem 1 marca, ale pierwszą maszynę zaatakowała

[27] Robak przez prawie miesiąc szukał drogi w komputerach firmy Behpajooh i 24 kwietnia dotarł do celu, gdy natrafił na komputer o nazwie Manager 115. Stuxnet zarejestrował, że ten komputer zawiera spakowany folder z plikami projektu z systemu Step 7. W ciągu następnych kilku miesięcy złośliwe oprogramowanie wydostało się z sieci firmy Behpajooh i rozprzestrzeniło po innych organizacjach. Firmy te są wymienione w pliku dziennika tylko za pomocą nazw domen (np.: MSCCO, Melal i S-Adari), które mogą, ale nie muszą odpowiadać nazwom organizacji.

[28] Znaleziono dziesięciu „pacjentów zero" w pięciu zainfekowanych firmach. Oznacza to, że napastnicy obrali za cel ataku dziesięć maszyn z tych pięciu firm. Badacze z Symanteca ustalili sieć prowadzącą z tych dziesięciu komputerów do 12 tys. innych zainfekowanych maszyn. Behpajooh była źródłem 69% z tych infekcji.

[29] Czas kompilacji i infekcji nie zawsze jest precyzyjny. Zegary systemowe w maszynie używanej do kompilacji i w komputerze ofiary mogą być nieprawidłowe. Ponadto kod mógł zostać skompilowany w strefie czasowej innej niż strefa czasowa ofiary. Porównując ilość czasu od momentu kompilacji do zainfekowania pierwszych maszyn przez trzy wersje Stuxneta, badacze zakładali, że komputer używany do kompilacji i komputer ofiary znajdują się w tej samej strefie czasowej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

dopiero 23 marca. W ostatniej znanej wersji, z kwietnia, czas między kompilacją a pierwszą infekcją też był długi — wynosił 12 dni. Szybka infekcja w 2009 r. wskazywała na to, że atakujący mogli posłużyć się wspólnikiem wewnątrz firmy lub wcześniej namierzoną nieświadomą ofiarą. Możliwe, że gdy nadszedł czas wypuszczenia następnych wersji Stuxneta, napastnicy musieli czekać dłużej na okazję do ataku.

Gdy Stuxnet rozprzestrzenił się na dużą skalę, kontaktował się z operatorami za pomocą serwerów C&C. Dlatego urzędnicy w Waszyngtonie szybko się dowiedzieli, że robak wymknął się spod kontroli. Na tym etapie było już jasne, że operacja, która przez ponad trzy lata była jednym z najściślej strzeżonych sekretów Waszyngtonu, nagle stała się zagrożona ujawnieniem.

Dlaczego tak starannie opracowana i przez tak długi czas kontrolowana broń cyfrowa została utracona? Początkowo obwiniano za to Izraelczyków. Wiosną 2010 r. Biały Dom, NSA i Izraelczycy podobno „zdecydowali się pójść na całość" i zaatakować zestaw 1000 wirówek[30]. Prawdopodobnie chodziło o grupę sześciu kaskad z jednostki A26. Poprzedni atak Stuxneta zredukował jednostkę A26 z dwunastu do sześciu kaskad wzbogacających uran. Możliwe, że tym razem napastnicy chcieli zniszczyć sześć ostatnich kaskad. Sześć kaskad po 164 wirówki każda dawało 984 urządzenia. Izraelczycy najwyraźniej dodawali ostatnie rozwiązania — nowe eksploity typu zero-day i inne mechanizmy rozprzestrzeniania — aby wzmocnić atak. Według Sangera jego informatorzy powiedzieli, że robak został wypuszczony w Natanzie i wydostał się poza zakład, gdy irański naukowiec podłączył laptopa do zainfekowanego komputera sterującego w obiekcie, a następnie przeniósł infekcję za pomocą laptopa do internetu. Jednak ten scenariusz jest niezgodny z dowodami, jakie badacze znaleźli w kodzie. Wcześniej wspomniano, że każda kopia Stuxneta obejmowała plik dziennika z zapisanymi wszystkimi zainfekowanymi maszynami. Według tych plików pierwsze infekcje miały miejsce w komputerach firmy Behpajooh i innych organizacji. Były to komputery do ogólnego przeznaczenia, a nie maszyny programistów z Natanzu zawierające pliki narzędzia Step 7 lub innego oprogramowania Siemensa. Możliwe, że były to laptopy należące do pracowników kontraktowych wykonujących zadania w Natanzie. Sanger pisze także, że robak powinien wykrywać zmiany w otoczeniu oraz to, że znalazł się na komputerach poza docelowym środowiskiem. W żadnej z wersji Stuxneta przeanalizowanych

[30] Sanger, *Confront and Conceal*, s. 204.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

przez badaczy nie było jednak nic, co służyło jako mechanizm wykrywania zmian i zapobiegania rozprzestrzenianiu się robaka poza Natanz. Jedyne ograniczenie w Stuxnecie było związane z uruchamianiem ładunku, a nie rozprzestrzenianiem.

Należy jednak zauważyć, że operatorzy zarządzający serwerami C&C komunikującymi się ze Stuxnetem *mogli* powstrzymać rozprzestrzenianie broni, gdy zobaczyli, że wymyka się ona spod kontroli. Stuxnet posiadał mechanizm zakończenia infekcji, co pozwalało napastnikom usunąć go z zainfekowanych maszyn. Gdy zaczął się nadmiernie rozprzestrzeniać i napastnicy zauważyli, że z serwerami C&C kontaktują się zainfekowane maszyny z Indonezji, Australii i innych państw, operatorzy mogli przesłać polecenie usunięcia kodu z komputerów. Jest kilka powodów, dla których nie zdecydowali się na taki krok. „Albo nie dbali o to, że się rozprzestrzenia, albo powielał się szybciej niż oczekiwano i nie potrafili go zlikwidować" — powiedział O'Murchu. Według niego zachowanie napastników nie wynikało z braku kompetencji. „Mieli pełną kontrolę nad zainfekowanymi maszynami i myślę, że [powstrzymanie się od działania] było świadomym krokiem". Nawet gdy wieści o rozprzestrzenianiu się Stuxneta trafiły do Waszyngtonu, podjęta została zaskakująca decyzja o kontynuowaniu operacji. Najwyraźniej nikt nie próbował powstrzymać rozprzestrzeniania się robaka. Choć szczegóły są niejasne, według informatorów Sangera w marcu zostały wypuszczone przynajmniej dwie nowe wersje Stuxneta. Wyeliminowany został w nich „błąd", który spowodował powielanie się poprzedniego wariantu kodu.

Czternastego kwietnia napastnicy skompilowali kolejną wersję Stuxneta, przy czym zawierała ona dokładnie ten sam ładunek co wariant marcowy. Choć w tej wersji zastosowano też te same mechanizmy rozprzestrzeniania kodu, tym razem infekcja nie była tak daleko i szeroko zakrojona jak w przypadku wersji z marca[31]. Żadne późniejsze wersje Stuxneta nie zostały wykryte.

[31] Choć atak dotknął niektóre firmy kilkakrotnie, nie zawsze infekowane były te same maszyny. Możliwe, że napastnicy za każdym razem szukali lepiej umiejscowionych maszyn lub komputerów pozwalających dotrzeć do celu różnymi drogami. Nie jest jasne, dlaczego wersja z kwietnia nie rozprzestrzeniła się w równym stopniu co wariant z marca. Oba warianty używały tych samych eksploitów typu zero-day i uderzyły w Behpajooh, firmę dotkniętą marcowym atakiem, z której Stuxnet szybko rozprzestrzenił się po świecie. Możliwe, że maszyny zaatakowane w kwietniu były połączone z mniejszą liczbą innych jednostek, co zmniejszyło szybkość powielania się kodu.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Możliwe, że pojawiły się kolejne wersje Stuxneta, jednak były na tyle ściśle kontrolowane, że nikt ich nigdy nie wykrył. Może na to wskazywać fakt, że badacze znaleźli w lipcu 2010 r. plik sterownika, który uznali za powiązany ze Stuxnetem. Był to sterownik odkryty przez ESET, podpisany certyfikatem firmy JMicron. Sterownik został znaleziony sam, bez żadnego głównego pliku robaka. Uważa się jednak, że był częścią ataku z użyciem innej wersji Stuxneta.

W kwietniowym ataku (podobnie jak w czerwcu 2009 r.) pierwszą ofiarą była firma Foolad Technique. Robak zaatakował ją 26 kwietnia i zainfekował ten sam komputer co w poprzednim roku. Kilka tygodni później, 11 maja, cyfrowa broń została zastosowana na trzech komputerach firmy używającej domeny Kala. Badacze sądzą, że była to Kala Electric lub Kala Electronics, przykrywka wykorzystywana przez Iran do zarządzania Natanzem i do potajemnego zakupu komponentów do programu nuklearnego. To właśnie tę firmę wymienił Alireza Jafarzadeh w 2002 r. w trakcie konferencji prasowej ujawniającej zakład w Natanzie[32]. Trzynastego maja ta sama wersja Stuxneta zaatakowała firmę Behpajooh.

Co ciekawe, choć Neda Industrial Group nie występuje w sprawdzonych przez badaczy dziennikach Stuxneta z 2010 r., Behrooz, inżynier systemów kontroli, który rok wcześniej zamieścił wpis na forum użytkowników produktów Siemensa, odezwał się ponownie w sprawie ciągłych problemów. Drugiego czerwca napisał, że we wszystkich komputerach z systemem Windows pojawia się ten sam kłopot co poprzedniego roku.

Dołączyli do niego pracownicy innych firm, pisząc, że mają identyczny problem. Jedna z osób napisała, że zainfekowane były wszystkie komputery PC tej firmy, a także stwierdziła, że problem jest ograniczony do Iranu, „ponieważ widać, że wiele osób z Iranu [na forum] ma ten sam problem od przynajmniej jednego [miesiąca]". Dyskusje trwały przez lipiec, a Behrooz był czasem tak sfrustrowany, że niektóre wpisy kończył symbolizującym złość emotikonem w postaci czerwonej buźki. Jednak 24 lipca nagle napisał wiadomość z informacją, że zagadka została rozwiązana. Zamieścił odsyłacz do artykułu o niedawno ujawnionym publicznie Stuxnecie i zakończył wpis trzema uśmiechniętymi buźkami. Oczywiście musiały minąć miesiące, zanim Behrooz i inni dowiedzieli się, co było celem ataku.

[32] Nazwa domeny komputera pozwala czasem zidentyfikować nazwę firmy, do której należy maszyna, ale nie zawsze tak jest.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W 2010 R., inaczej niż w operacji z 2009 r., nie wiedziano, jaki był wpływ ataku na Natanz. Sanger pisze, że po wypuszczeniu w 2010 r. trzeciej wersji Stuxneta 984 wirówki „z piskiem zakończyły pracę"[33]. W tym czasie dokładnie 984 wirówki wzbogacały uran w sześciu kaskadach jednostki A26, lecz z raportów MAEA nie wynika, że przestały one funkcjonować. We wrześniu nadal sześć kaskad w jednostce A26 wzbogacało gaz, a następnych sześć obracało się w próżni. Możliwe, że wirówki wspomniane przez Sangera przestały działać, ale zostały ponownie uruchomione lub wymienione w okresie między majowym a wrześniowym raportem MAEA. Możliwe też, że informatorzy Sangera pomylili daty i wspomnieli o 1000 wirówek, które technicy usunęli pod koniec 2009 i na początku 2010 r., co MAEA zarejestrowała za pomocą kamer.

Trudno jest dokładnie określić, co się stało z wirówkami w 2010 r. W czerwcu tego roku urzędnicy irańscy zaczęli oskarżać MAEA o udostępnianie prasie informacji o poczynaniach Irańczyków. W liście z 3 czerwca Iran ostrzegł agencję, że jeśli poufne informacje o programie nuklearnym „wyciekną w jakikolwiek sposób i/lub zostaną przekazane mediom", Irańczycy wyciągną konsekwencje, a pierwszą z nich będzie wycofanie pozwoleń dla niektórych inspektorów MAEA kontrolujących obiekty nuklearne[34]. W tym samym miesiącu Iran zrealizował swoje groźby i wykluczył dwie osoby z listy ok. 150 akceptowanych inspektorów MAEA, wskazując na „fałszywe i błędne informacje" z majowego raportu MAEA. W raporcie napisano, że w Iranie zaginął sprzęt związany z działalnością nuklearną. We wrześniu z listy usuniętych zostało dwóch następnych inspektorów. Tym razem Irańczycy uzasadnili to ujawnieniem mediom informacji przed ich publicznym udostępnieniem w raporcie MAEA[35].

---

[33] Sanger, *Confront and Conceal*, s. 206. Sanger pisze, że NSA przechwyciła informacje wskazujące na zatrzymanie pracy wirówek.

[34] Iran oskarżył MAEA o udostępnienie informacji w artykułach dla Agencji Reutera (z 14 maja) i Associated Press (z 30 maja).

[35] Fereydoon Abbasi, mianowany po zamachu na jego życie w 2010 r. szefem irańskiej Agencji Energii Atomowej, w wywiadzie z 2014 r. oskarżył Zachód o wykorzystywanie raportów MAEA o działalności nuklearnej Iranu do „kalibrowania" sabotażu wymierzonego w program nuklearny tego kraju i „zwiększania poziomu powodowanych zniszczeń" wraz z każdą serią ataków. „Dzięki dostępowi do ujawnionych danych z naszych raportów [napastnicy] mogą stwierdzić, ile wirówek działa w irańskich

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Te zarzuty wywarły negatywny wpływ na ilość upublicznianych przez MAEA informacji o Natanzie. W listopadzie MAEA przestała publikować w kwartalnych raportach szczegóły dotyczące wirówek. Zamiast podawać liczbę zainstalowanych i wzbogacających gaz wirówek z każdej jednostki, łączyła wartości z wszystkich trzech jednostek (A24, A26 i A28) w zbiorcze wyniki. W ten sposób utracone zostało podstawowe źródło informacji pozwalające ocenić wpływ Stuxneta na pracę zakładu[36].

Wiadomo jednak, że w lipcu 2010 r. wirówki wciąż działały tylko na 45 – 66% możliwości. Agencja ISIS w lipcowym raporcie po raz pierwszy stwierdziła, że przyczyną niektórych problemów w Natanzie mógł być

obiektach nuklearnych, ile ma zostać zainstalowanych i jakie części są potrzebne" — powiedział. Dodał też, że gdy Iran przekazywał do MAEA raporty na temat projektów obiektów nuklearnych i sprzętu, jaki planuje zakupić na potrzeby programu, agencje wywiadowcze wykorzystywały listy do „zastawiania pułapek w urządzeniach" i „umieszczania wirusów w systemach kontroli". Z czasem Irańczycy stali się ostrożniejsi, przekazując inspektorom MAEA informacje o sprzęcie instalowanym w salach z kaskadami. W pewnym momencie ponaklejali nawet nalepki na nazwy marek urządzeń, aby uniemożliwić inspektorom zidentyfikowanie sprzętu. Chodzili też za inspektorami z kamerą, rejestrując wszystkie poczynania kontrolerów. Abbasi powiedział również, że Stuxnet nie był pierwszym ani ostatnim atakiem przeprowadzonym przez Stany Zjednoczone i Izrael na program nuklearny oraz że państwa te wielokrotnie infiltrowały łańcuch dostaw sprzętu dla tego programu, aby dokonać sabotażu zaworów próżniowych, pomp i innego wyposażenia. „Agencje szpiegowskie dostosowują swoje ataki do naszych potrzeb; blokują nam konwencjonalne kanały dostaw i pozostawiają otwarte tylko te, nad którymi mają pełną kontrolę, aby wprowadzić zmodyfikowany sprzęt do naszych obiektów — mówił, oskarżając firmę Siemens o uczestnictwo w tym procederze. — W ten sposób przedostali się do naszej infrastruktury elektronicznej, podsłuchiwali nas i zainstalowali złośliwe oprogramowanie takie jak Stuxnet. Zainstalowali wirusa w miernikach, które zakupiliśmy od Siemensa, oraz [umieścili] materiały wybuchowe w sprzęcie". Zob. „How West Infiltrated Iran's Nuclear Program, Ex-Top Nuclear Official Explains", *Iran's View*, 28 marca 2014 (*http://www.iransview.com/west-infiltrated-irans-nuclear-program-ex-top-nuclear-official-explains/1451/*).

[36] Były urzędnik MAEA poinformował mnie, że zmiany w raportach wprowadzone pod koniec 2010 r. nie miały nic wspólnego z oskarżeniami ze strony Iranu, a wynikały z niepewności co do dokładności zebranych danych. Gdy Irańczycy w latach 2009 i 2010 usunęli gaz z niektórych wirówek oraz zdemontowali inne, część kaskad wciąż działała, choć obejmowały one mniej niż 164 pracujące urządzenia. MAEA zrozumiała wtedy, że niemożliwe jest ustalenie, ile wirówek w każdej kaskadzie pracuje i wzbogaca gaz. Wcześniej inspektorzy zakładali, że jeśli kaskada wzbogaca uran, biorą w tym udział wszystkie 164 wirówki.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„sabotaż”[37]. Stuxnet został już wtedy wykryty i ujawniony, jednak do czasu powiązania go z irańskim programem nuklearnym i zakładem w Natanzie musiało minąć jeszcze kilka miesięcy.

Wiadomo też, że liczba zainstalowanych i wzbogacających uran wirówek ulegała w 2010 r. znacznym wahaniom. W listopadzie 2009 r., w szczytowym momencie działalności zakładu, zainstalowane były 8692 wirówki. W maju 2010 r. ta liczba spadła do 8528 (z czego 3936 wzbogacało uran), we wrześniu wzrosła do 8856 (3772 wzbogacające uran), a listopadzie zmalała do 8426 (4816 wzbogacających uran). Możliwe, że wirówki psuły się nawet po wykryciu Stuxneta, co wpływało na opisane wahania. Choć znaczny wzrost liczby wzbogacających uran wirówek (o 1000 w okresie od września do listopada) wskazywał na to, że technicy wyeliminowali utrzymujące się skutki działania Stuxneta, Iran wciąż miał 3600 zainstalowanych urządzeń, które biernie czekały w kaskadach[38]. To sugerowało, że przynajmniej niektóre problemy wciąż się pojawiały. Niedługo potem, 16 listopada, kierownictwo w Natanzie całkowicie zamknęło zakład na sześć dni po ujawnieniu przez Symantec, że Stuxnet miał dokonywać sabotażu konwerterów częstotliwości[39]. W tym samym miesiącu Irańczycy dodali nowe wirówki do sześciu kaskad, co wskazywało na to, że próbowali zmienić konfigurację, by zablokować ładunek Stuxneta[40].

---

[37] David Albright, Paul Brannan, Andrea Stricker, „What Is Iran’s Competence in Operating Centrifuges?”, ISIS, 26 lipca 2010 (*http://isis-online.org/isis-reports/detail/what-is-irans-competence-in-operating-centrifuges/8*).

[38] Ivan Oelirch z organizacji Federation of American Scientists zauważył, że choć większa liczba wirówek wzbogacała uran, działały one z wydajnością tylko 20%.

[39] David Albright i współpracownicy, „Natanz Enrichment Site: Boondoggle or Part of an Atomic Bomb Production Complex?”, ISIS, 21 września 2011 (*http://isis-online.org/isis-reports/detail/natanz-enrichment-site-boondoggle-or-part-of-an-atomic-bomb-production-comp/*).

[40] W listopadzie 2010 r. technicy zwiększyli liczbę wirówek w sześciu kaskadach ze 164 do 174. Zob. Rada Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement and the Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran”, raport z 23 listopada 2010 (*https://www.iaea.org/sites/default/files/gov2010-62.pdf*). Choć niektórzy obserwatorzy uważali, że Iran zamontował dodatkowe wirówki w celu zwiększenia ilości wzbogacanego gazu (np. aby nadrobić czas stracony z powodu Stuxneta), informator z MAEA powiedział mi, że wirówki pojawiły się na dalszych etapach kaskady, co nie zwiększało ilości wzbogacanego materiału. Zasugerował, że dodatkowe wirówki miały zmienić konfigurację kaskad, aby zapobiec atakowi nieusuniętych kopii Stuxneta.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

TYMCZASEM W WASZYNGTONIE przez cały 2010 r. trwały dyskusje na temat Stuxneta. Na początku lata dyrektor CIA Leon Panetta i gen. James Cartwright przekazali informacje o niekontrolowanym rozprzestrzenianiu się robaka prezydentowi. Doprowadziło to do wielu pytań ze strony Obamy. Czy coś wskazywało na to, że Irańczycy już wykryli atak? Jeśli tak, to czy byli w stanie określić jego przeznaczenie lub wyśledzić źródło? Obama martwił się też przypadkowymi uszkodzeniami maszyn zainfekowanych poza Natanzem. Czy w tej sytuacji należało przerwać operację? Doradcy przypomnieli prezydentowi, że zastosowany robak to bardzo precyzyjna broń, uruchamiająca ładunek tylko w komputerach spełniających określone kryteria. Choć mogła w pewnym stopniu wpływać na inne maszyny, co wynikało z natury infekcji, nie wyrządzała w nich szkód.

Zadowolony z tego, że operacja na ogólnym poziomie wciąż pozostaje pod kontrolą, Obama nakazał jej kontynuowanie[41].

Z powodu złożoności Stuxneta i niskiego prawdopodobieństwa wykrycia lub odszyfrowania go ta decyzja musiała wówczas wydawać się całkiem sensowna. Rzeczywiście, nawet pierwsze reakcje ze strony Symanteca i innych firm z tej branży po ujawnieniu Stuxneta zdawały się potwierdzać, że utajniona operacja jest bezpieczna. Wszystko wskazywało na to, że społeczność zajmująca się zabezpieczeniami, przytłoczona złożonością i nieznaną strukturą odkrytego złośliwego oprogramowania, po utworzeniu wykrywających robaka sygnatur zrezygnowała z dalszej pracy nad kodem.

Waszyngton nie uwzględnił jednak determinacji badaczy Symanteca, którzy chcieli w pełni zrozumieć ten tajemniczy kod, ani bezpośredniej i głośnej szczerości Ralpha Langnera w kwestii celu ataku. Wraz z upływem miesięcy i pojawianiem się nowych informacji od Langnera i Symanteca ludzie w Waszyngtonie i Tel Awiwie mogli tylko siedzieć i patrzeć, jak wszystkie kawałki układanki dopasowują się do siebie i pojawia się kompletny obraz.

[41] Sanger pisze, że spotkanie Panetty z Obamą odbyło się w połowie lata, czyli w lipcu, mniej więcej w czasie ujawnienia Stuxneta. Jednocześnie twierdzi, że w ciągu kilku tygodni od spotkania napastnicy wypuścili dwie nowe wersje robaka. To wskazuje na to, że nowe wersje Stuxneta zostały zastosowane już po tym, jak firmy antywirusowe przygotowały wykrywające go sygnatury. Jak już wcześniej pisałam, nie natrafiono na nowsze wersje robaka.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 18

POŁOWICZNY SUKCES

Rok po tym, jak urzędnicy z MAEA zauważyli, że technicy usuwają nieoczekiwanie dużą liczbę wirówek z podziemnej hali w Natanzie, tajemnica znikających urządzeń została wreszcie rozwikłana. Jednak nawet po zidentyfikowaniu Stuxneta jako przyczyny problemów i po ujawnieniu szczegółów dotyczących zainwestowania w niego poważnych zasobów kilka pytań wciąż pozostawało bez odpowiedzi. Jak skuteczny okazał się Stuxnet w realizacji celów? Czy warto było ponosić ryzyko, koszty i konsekwencje jego zastosowania?

„Jeśli celem Stuxneta było zniszczenie wszystkich wirówek [w Natanzie]", operacja zakończyła się niepowodzeniem, jak pisał David Albright z ISIS w raporcie z 2010 r. Jeżeli jednak zadanie polegało na uszkodzeniu ograniczonej liczby urządzeń, aby nieco spowolnić irański program wzbogacania uranu, to „atak zakończył się sukcesem — napisał Albright — przynajmniej na pewien czas"[1].

Irański program nuklearny w 2010 r., kiedy Stuxnet został wykryty, z pewnością nie był realizowany tam, gdzie Irańczycy by sobie tego życzyli. Dwie olbrzymie podziemne hale w Natanzie mogły pomieścić 47 tys. wirówek,

[1] David Albright, Paul Brannan, Christina Walrond, „Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment", ISIS, 22 grudnia 2010 (*http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

jednak mimo że od czasu zakończenia budowy minęło ponad dziesięć lat, tylko jedna z nich zawierała urządzenia, a nawet ona była zapełniona jedynie w jednej trzeciej. „Jeśli uwzględnić to, co Iran pierwotnie planował i gdzie program był realizowany obecnie, sytuacja tego kraju się pogorszyła […]" — napisał Albright.

Nie jest jasne, w jakim stopniu był to wynik działania Stuxneta, a w jakim innych czynników: sankcji, nacisków dyplomatycznych i efektów innych utajnionych akcji sabotażowych. Ralph Langner uważał, że atak na Natanz był wielkim sukcesem i okazał się „prawie równie skuteczny jak operacja wojskowa", ale bez zagrożeń i kosztów związanych z akcjami militarnymi. „New York Times" stwierdził, że Stuxnet wydaje się być „najważniejszym czynnikiem dającym nam więcej czasu na zegarze nuklearnym"[2].

Pojawiały się jednak różne opinie na temat tego, ile wirówek Stuxnet uszkodził i w jakim stopniu przyczyniło się to do spowolnienia irańskiego programu nuklearnego.

W 2003 r. izraelscy urzędnicy ostrzegali, że Iran — jeśli jego program nuklearny nie zostanie powstrzymany — do 2007 r. wzbogaci wystarczająco dużo uranu do zbudowania bomby. Dwa okresy dobrowolnego wstrzymania prac i wiele innych czynników doprowadziły do zmiany tej daty. Izraelczycy najpierw oszacowali, że bomba może powstać w 2008 r., a potem podali rok 2010. Po ujawnieniu Stuxneta ten termin znów został przesunięty.

Gdy ustępujący szef Mosadu, Meir Dagan, na początku 2011 r. odchodził ze stanowiska, poinformował izraelski Knesset, że Iran nie zdoła zbudować arsenału nuklearnego przed 2015 r.[3]. Urzędnicy amerykańscy nie byli równie optymistyczni w swoich szacunkach i stwierdzili, że program został cofnięty w czasie tylko o 18 – 24 miesiące, a nie o cztery lata. Według sekretarz stanu Hillary Clinton program nuklearny został „spowolniony" przez problemy technologiczne i sankcje, ale nie do tego stopnia, by wszyscy mogli odetchnąć. „Mamy czas — powiedziała — ale nie jest go dużo"[4].

---

[2] William J. Broad, John Markoff, David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, „New York Times", 15 stycznia 2011.

[3] Yossi Melman, *Outgoing Mossad Chief: Iran Won't Have Nuclear Capability Before 2015*, „Ha'aretz", 7 stycznia 2011.

[4] Mark Landler, *U.S. Says Sanctions Hurt Iran Nuclear Program*, „New York Times", 10 stycznia 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ivanka Barzashka, pracownik naukowy w Centre for Science and Security Studies w londyńskim King's College, uważała, że program nuklearny w ogóle nie został cofnięty w czasie. Zbadała korelacje między liczbą wirówek z raportów MAEA a datami aktywności Stuxneta w 2009 r. i stwierdziła, że dowody na skuteczność ataku są poszlakowe i nie prowadzą do jednoznacznych wniosków. Jej zdaniem jeśli Stuxnet wywarł jakiś wpływ na program wzbogacania uranu, było to krótkotrwałe.

„Jeżeli sabotaż miał miejsce, był krótkotrwały i najprawdopodobniej odbywał się od maja do listopada 2009 r. — napisała w podsumowaniu. — Złośliwe oprogramowanie nie cofnęło w czasie irańskiego programu wzbogacania uranu, choć prawdopodobnie mogło tymczasowo spowolnić jego rozwój"[5].

Irańczycy rzeczywiście wykazali się zaskakującą zdolnością do odzyskiwania równowagi po uszkodzeniach i opóźnieniach spowodowanych przez Stuxneta i inne czynniki.

Na przykład na początku 2010 r. technicy w Natanzie krótko po tym, jak wymienili powodujące problemy wirówki, przyspieszyli proces wzbogacania, przesyłając do urządzeń więcej gazu. W efekcie produkcja nisko wzbogaconego uranu w 2010 r. *wzrosła* i od tamtej pory pozostawała na mniej więcej stałym poziomie. Jesienią 2008 r., gdy Stuxnet 0.5 manipulował zaworami kaskad, wirówki produkowały tylko 90 kg nisko wzbogaconego uranu miesięcznie. Pod koniec 2009 r., gdy uderzyła następna wersja Stuxneta, ta liczba nieco spadła (do 85 kg miesięcznie). Jednak w 2010 r., mimo wypuszczenia dwóch nowych wersji Stuxneta, produkcja wzrosła do 120 – 150 kg miesięcznie. W 2011 r. Iran uzyskał stabilny poziom 150 kg nisko wzbogaconego uranu na miesiąc.

Warto przy tym zauważyć, że poziom produkcji wciąż był znacznie poniżej tego, co wirówki powinny produkować. W 2010 r. podane wartości dało 4820 wirówek. Jednak w 2011 r. Iran używał 5860 urządzeń, a produkcja pozostała na tym samym poziomie. Wynika z tego, że wirówki działały mniej wydajnie niż wcześniej — możliwe, że z powodu długotrwałych efektów działania Stuxneta[6].

---

[5] Ivanka Barzashka, „Are Cyber-Weapons Effective?", Royal United Services Institute for Defense and Security Studies, 23 lipca 2013 (*http://tandfonline.com/doi/pdf/10.1080/03071847.2013.787735*). Warto zauważyć, że Barzashka zbadała tylko raporty MAEA z 2009 r. i nie uwzględniła wersji Stuxneta z lat 2008 i 2010.

[6] David Albright, Christina Walrond, „Performance of the IR-1 Centrifuge at Natanz", ISIS, 18 października 2011 (*http://isis-online.org/isis-reports/detail/test1*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Ostatecznie Iran i tak robił postępy i produkował wzbogacony uran. Do połowy 2011 r. wirówki wyprodukowały w sumie 4400 kg nisko wzbogaconego uranu[7]. Ponadto Iran przynajmniej 1950 kg przetransportował do zakładu pilotażowego w celu wzbogacenia materiału do poziomu 19,75%. Na początku 2011 r. dysponował 33 kg uranu wzbogaconego w tym stopniu i planował potroić tę wartość.

Irańczycy zaczęli wzbogacać uran do wyższego poziomu po zniszczeniu wirówek przez Stuxneta. Irańscy urzędnicy utrzymywali, że potrzebują wysoko wzbogaconego uranu do badań nad leczeniem raka. Jednak wysoko wzbogacony uran oznaczał większe problemy dla przeciwników programu wzbogacania, ponieważ osiągnięcie poziomu 20% zbliżało Iran do uzyskania poziomu 90% potrzebnego do budowy bomb. „Rozpoczęcie od wyższego poziomu wzbogacenia oznaczało, że Iran o ponad połowę skracał czas potrzebny do wyprodukowania wysoko wzbogaconego do ok. 90% uranu do zastosowań bojowych" — pisała Barzashka. Dlatego jeśli „celem [Stuxneta] było zmniejszenie irańskiego potencjału do budowy broni atomowej, operacja zdecydowanie zakończyła się porażką"[8].

Jednocześnie technicy zaczęli instalować w pilotażowym zakładzie w Natanzie bardziej zaawansowane wirówki IR-2m i IR-4. Były one dużo bardziej wydajne niż model IR-1. Wirówki IR-1 potrafiły wykonać jedną jednostkę pracy dziennie (choć rzadko osiągały nawet ten poziom), natomiast bardziej zaawansowane modele były od trzech do pięciu razy wydajniejsze. Były też odporniejsze niż model IR-1, co oznaczało, że są mniej narażone na uszkodzenie pod wpływem obciążenia generowanego przez Stuxneta.

Choć Iran najwyraźniej szybko odzyskał równowagę po ataku Stuxneta, cyfrowa broń miała przynajmniej dwa długotrwałe efekty związane z programem wzbogacania. Po pierwsze, naruszyła irańskie zapasy uranu w formie gazowej. W trakcie dokonywania sabotażu przez Stuxneta kilka ton wzbogaconego uranu trafiło do kolektorów na odpady. Prawdopodobnie nie wszystkie straty były spowodowane przez Stuxneta, ponieważ technicy mieli wiele różnych problemów z wirówkami. Robak z pewnością przyczynił się

[7] Olli J. Heinonen, „Iran Ramping Up Uranium Enrichment", blog Power and Policy, 20 lipca 2011, opublikowane przez Belfer Center at Harvard Kennedy School, 20 lipca 2011 (*https://belferinthenews.wordpress.com/2011/07/25/olli-heinonen-on-irans-uranium-enrichment-program/*).

[8] Barzashka, „Are Cyber-Weapons Effective?".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

jednak do zmarnowania części gazu. Iran miał dostęp do ograniczonych zasobów uranu (część pochodziła od dostawców zagranicznych, część była wydobywana lokalnie), dlatego każda ilość utraconego gazu oznaczała zmniejszenie rezerw.

Po drugie, Iran posiadał ograniczoną liczbę wirówek i ilość materiałów do produkcji nowych. Wzmocnienie sankcji oznaczało, że zastępowanie uszkodzonych urządzeń stało się jeszcze trudniejsze. W 2008 r. MAEA szacowała, że Iran ma komponenty i materiały pozwalające na budowę 10 tys. wirówek[9]. Jeśli Stuxnet uszkodził 1000 z nich, zmniejszało to zasoby urządzeń o 10%. Ponadto Iran każdego roku tracił ok. 10% wirówek z powodu normalnego zużycia. Przy tym tempie „po pięciu latach ci goście będą ugotowani" — powiedział Olli Heinonen z MAEA[10].

Jednak Heinonen uważał, że Stuxnet uszkodził więcej niż 1000 wirówek. Sądził, że ta liczba jest bliższa 2000. Swoje szacunki opierał na tym, że raporty MAEA przedstawiały tylko wycinek sytuacji w Natanzie z okresu trzech miesięcy. Ponadto w zakładzie ktoś manipulował przy plombach bezpieczeństwa, dlatego możliwe było, że Iran potajemnie wymieniał niektóre uszkodzone wirówki bez wiedzy MAEA[11].

Choć inspektorzy z MAEA średnio odwiedzali zakład 24 razy w roku, raporty były publicznie udostępniane raz na kwartał, a dane z tych dokumentów odzwierciedlały tylko liczbę wirówek, jaką inspektorzy zaobserwowali w zakładzie w trakcie ostatniej wizyty. Dlatego między wizytami technicy mieli możliwość wymiany wirówek poza zasięgiem wzroku ciekawskich inspektorów — o ile potrafili uniknąć kamer MAEA, które (teoretycznie) miały uniemożliwiać tego rodzaju ukradkowe operacje.

Za każdym razem, gdy w zakładzie montowany był nowy moduł z kaskadami, technicy umieszczali wokół niego przenośne ściany. Dostęp do modułu był możliwy tylko przez jedne drzwi monitorowane kamerą MAEA.

---

[9] David Albright, Jacqueline Shire, Paul Brannan, „Enriched Uranium Output Steady: Centrifuge Numbers Expected to Increase Dramatically; Arak Reactor Verification Blocked", ISIS, 19 listopada 2008 (*http://isis-online.org/publications/iran/ISIS_analysis_Nov-IAEA-Report.pdf*).

[10] Z wywiadu przeprowadzonego przez autorkę z Heinonenem w czerwcu 2011 r.

[11] Heinonen odszedł z MAEA w październiku 2010 r., a więc przed usunięciem wirówek, dlatego nie miał dostępu do raportów inspektorów w celu sprawdzenia dokładnych danych. Był jednak pewien, że liczba uszkodzonych wirówek przekraczała 1000.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Na łączeniach ścian umieszczane były plomby, co gwarantowało, że do środka można się dostać wyłącznie przez drzwi. Technicy nie mogli więc łatwo rozsunąć ścian, aby wymontować wirówki poza zasięgiem kamer. Jednak w Natanzie pojawiły się problemy z tajemniczymi naruszeniami plomb[12]. Irańscy urzędnicy tłumaczyli, że naruszenia były przypadkowe i że operatorom nakazano „większą ostrożność". Mimo to Heinonen stwierdził, że w Iranie pojawił się „nietypowy wzorzec" naruszania plomb. Zwiększało to prawdopodobieństwo, że ściany zostały przesunięte w celu ukradkowego usunięcia i wymiany uszkodzonych urządzeń[13].

Jeśli nawet liczba uszkodzonych wirówek przekraczała 1000, Stuxnet najwyraźniej nie był cudownym rozwiązaniem, którym mógłby być, gdyby zaprojektowano go w celu natychmiastowego i szeroko zakrojonego niszczenia urządzeń (wtedy mógłby uszkodzić tysiące wirówek za jednym posunięciem), a nie do powolnego, stopniowego działania.

Część osób zastanawiała się, dlaczego Stuxnet *nie* został zaprojektowany w celu szybkiego wyrządzenia poważnych szkód. Jednak tak agresywna operacja mogła mieć poważniejsze konsekwencje. Gdyby Stuxnet w jednym kroku zniszczył 3000 – 4000 urządzeń, nie byłoby wątpliwości, że nastąpił sabotaż. Iran zapewne potraktowałby to jak atak wojskowy, na który należy odpowiedzieć. Dlatego powolne i ukradkowe działanie Stuxneta było kompromisem. Utrudniał on osiągnięcie poważnych efektów, a jednocześnie nie dawał Iranowi silnych argumentów do odwetu.

---

[12] W liście z lipca 2010 r. do Iranu MAEA zwróciła uwagę na „liczne incydenty" związane z naruszeniem plomb w zakładzie. Zob. Rada Gubernatorów MAEA, „Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran", raport z 6 września 2010, s. 3 (*https://www.iaea.org/sites/default/files/gov2010-46.pdf*). Z raportu nie wynika, czy chodziło o plomby na ścianach, czy na cysternach z gazem i innym sprzęcie. Informator z MAEA poinformował mnie jednak, że były to plomby na ścianach.

[13] Informator z MAEA powiedział mi, że to Iran poinformował o zerwanych plombach. MAEA zbadała sprawę i nie dopatrzyła się uchybień ze strony Irańczyków. Jednak śledztwo dotyczyło tylko tego, czy Iran mógł uszkodzić plomby w celu wyniesienia z pomieszczeń materiału nuklearnego poza zasięgiem kamer. Nie sprawdzano, czy wirówki nie zostały ukradkowo wyniesione z sal. Gdy inspektorzy stwierdzili, że cały uran pozostał na miejscu, uznali, że plomby nie zostały umyślnie zerwane w niedozwolonym celu. Nie zbadali jednak możliwości, czy plomby nie zostały celowo uszkodzone, by wynieść zepsute wirówki.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Nie wiadomo było też, co cyfrowa broń zdołałaby osiągnąć, gdyby nie została wykryta w 2010 r. Gdy uderzył Stuxnet, irański program wzbogacania uranu był w początkowej fazie. Ponadto atak został ujawniony na wczesnym etapie jego działania. Trudno stwierdzić, czego Stuxnet dokonałby w przyszłości, po zainstalowaniu przez Iran dodatkowych wirówek i kaskad. Dlatego Barzashka uważała, że napastnicy zbyt szybko przeprowadzili atak. Gdyby poczekali do czasu zainstalowania większej liczby wirówek i wtłoczenia do nich większej ilości gazu, wpływ Stuxneta na program mógłby być znacznie większy.

Jedno było pewne: powtórzenie całej akcji stało się znacznie trudniejsze. Stuxnet, jak zauważył Langner, był bronią jednorazową. Wykrycie ataku wzmogło czujność Irańczyków, przez co trudniej było przeprowadzić podobne operacje w przyszłości. Teraz za każdym razem, gdy sprzęt w Natanzie zawodził, Irańczycy od razu podejrzewali sabotaż i reagowali szybciej. Przy pierwszych oznakach problemów technicy zamykali systemy i dokładnie je badali pod kątem złośliwego oprogramowania lub manipulacji.

Mimo czynników, które ograniczyły efektywność Stuxneta i przyspieszyły jego wykrycie, ten skryty atak bardzo ucieszył przynajmniej jedną grupę.

„W społeczności działającej na rzecz nierozprzestrzeniania broni Stuxnet jest mile widzianą nowością — powiedział David Albright. — Oznacza, że nie będziemy musieli toczyć wojny przeciw Iranowi”[14].

JEDNAK NAWET JEŚLI Stuxnet zapewnił dyplomatom trochę więcej czasu, nie zakończył politycznego kryzysu i nie wykluczył możliwości wojny. W 2011 r. ONZ nałożyła piąty zestaw sankcji na Iran, a Stany Zjednoczone rozmieszczały na Bliskim Wschodzie pociski Patriot, aby chronić swoich sojuszników na wypadek wojny. Wrogowie Iranu nadal zabijali naukowców, starając się powstrzymać prace nad programem nuklearnym. W lipcu 2011 r. 35-letni fizyk Darioush Rezaeinejad został zastrzelony (kula trafiła w gardło), gdy odbierał swoją córkę z przedszkola w Teheranie. Dwóch zamachowców uciekło na motocyklach. MAEA stwierdziła, że Rezaeinejad

[14] Z wywiadu przeprowadzonego przez autorkę z Albrightem w lutym 2011 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

uczestniczył w pracach nad przełącznikami wysokiego napięcia wyzwalającymi eksplozje potrzebne do odpalenia głowicy atomowej[15].

Później, w styczniu 2012 r., zaledwie dzień po tym, jak izraelski szef sztabu powiedział, że rok 2013 będzie kluczowy dla irańskiego programu nuklearnego, w Iranie ponownie uderzyli zamachowcy na motocyklach. Tym razem napastnicy zastosowali ładunek przyczepiony do samochodu, a ofiarą był Mostafa Ahmadi-Roshan. Początkowo podawano, że był on 32-letnim chemikiem pracującym w Natanzie. Później irański urzędnik ujawnił, że Ahmadi-Roshan w rzeczywistości zarządzał zakładem w Natanzie, a do tego odpowiadał za zakupy wyspecjalizowanego sprzętu na potrzeby irańskiego programu nuklearnego. Ahmadi-Roshan zajmował stanowisko wicedyrektora ds. handlowych w Kala Electronic Company dostarczającej części do Natanzu. Kala była jedną z firm, o których uważano, że zostały zaatakowane przez Stuxneta[16].

Ponadto w Iranie wydarzyła się seria tajemniczych eksplozji. W listopadzie 2011 r. poważny wybuch w centrum testów pocisków dalekiego zasięgu zabił ponad 30 członków irańskiej gwardii rewolucyjnej, w tym generała uważanego za architekta irańskiego programu budowy pocisków[17]. Iran zaprzeczył, że eksplozja była spowodowana sabotażem. Utrzymywał, że przyczyną był wypadek. Jednak informator z zachodniego wywiadu powiedział gazecie „New York Times", że powód wybuchu miał niewielkie znaczenie. „Wszystko, co daje nam dodatkowy czas i odracza dzień, w którym

[15] Ulrike Putz, „Mossad Behind Tehran Assassinations, Says Source", *Spiegel Online*, 2 sierpnia 2011 (*http://www.spiegel.de/international/world/sabotaging-iran-s-nuclear-program-mossad-behind-tehran-assassinations-says-source-a-777899.html*). Zob. także „Israel Responsible for Iran Killing: Report", *Global Security Newswire*, 2 sierpnia 2011 (*http://www.nti.org/gsn/article/israel-responsible-for-iran-killing-report/*).

[16] Ahmadiego-Roshana po śmierci nazwano młodym nuklearnym męczennikiem. Jego imieniem nazywano ulice i place. Saeed Kamali Dehghan, Julian Borger, *Iranian Nuclear Chemist Killed by Motorbike Assassins*, „Guardian", 11 stycznia 2012. Zob. także Zvi Bar'el, *Iran Domestic Tensions Boil as West Battles Its Nuclear Program*, „Ha'aretz", 8 kwietnia 2014. David Albright poinformował mnie, że gdy zabijany jest naukowiec związany z programem nuklearnym, ma to na celu wyeliminowanie wiedzy eksperta i zaszkodzenie pracom. Jednak morderstwo osoby zaangażowanej w zakupy na rzecz programu jest komunikatem i ma odstraszyć innych od pełnienia podobnej funkcji.

[17] David E. Sanger, William J. Broad, *Blast That Leveled Base Seen as Big Setback to Iran Missiles*, „New York Times", 4 grudnia 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Irańczycy zdołają umieścić broń nuklearną w precyzyjnym pocisku, oznacza małe zwycięstwo — mówił. — Na tym etapie bierzemy to, co możliwe, niezależnie od okoliczności".

W tym samym miesiącu w zakładzie przetwarzania uranu w Isfahanie nastąpił wybuch, który podobno zniszczył obiekt, gdzie przechowywano surowce do programu wzbogacania uranu[18]. Później, w sierpniu 2012 r., eksplozje spowodowały uszkodzenie linii przesyłających elektryczność z miasta Kom do podziemnego zakładu wzbogacania w Fordo. Z informacji wynikało, że jedna z eksplozji nastąpiła, gdy ochrona znalazła elektroniczne urządzenie monitorujące zamaskowane jako skała i próbowała je przesunąć. To urządzenie z pułapką podobno służyło do przechwytywania danych z komputerów i linii telefonicznych z zakładu wzbogacania uranu[19]. Opisując ten incydent, irański urzędnik ujawnił, że także linie zasilania zakładu w Natanzie zostały uszkodzone, choć nie podał daty ani szczegółów

[18] Sheera Frenkel, *Second Blast Aimed at Stopping Tehran's Nuclear Arms Plans*, „Times" (Londyn), 30 listopada 2011. Irańskie agencje informacyjne początkowo informowały o wybuchu, lecz potem raporty zostały usunięte z witryn, a oficjele odwołali wypowiedzi potwierdzające eksplozję. W lutym 2012 r. w izraelskiej reklamie pojawił się żart dotyczący tego wybuchu. Była to zdjęta później reklama izraelskiego operatora telewizji kablowej HOT. Występowali w niej aktorzy z izraelskiego serialu komediowego *Asfur*, przedostający się do Iranu w przebraniu muzułmańskich kobiet. Jest to szydercze nawiązanie do czasów, gdy były palestyński lider Jasir Arafat podobno uniknął schwytania dzięki podobnemu przebraniu. Czwórka z reklamy dociera do Isfahanu, lokalizacji zakładu przetwarzania uranu, gdzie nastąpiła tajemnicza eksplozja. Gdy bohaterowie idą przez miasto, za nimi widoczny jest obiekt nuklearny. Jeden z aktorów rozsmarowuje po twarzy krem przeciwsłoneczny. Kiedy jego towarzysze pytająco spoglądają na niego, odpowiada: „No co? Nie wiecie, jak wysokie jest tu promieniowanie?". Później nieporadni wędrowcy natrafiają na znudzonego agenta Mosadu. Agent siedzi w ogródku kawiarnianym i opowiada im, że od dwóch miesięcy przebywa w mieście, prowadząc obserwację, i w tym czasie zabija czas, oglądając odcinki serialu *Asfur* na tablecie Samsung Galaxy, który szpieg wraz z żoną dostali w prezencie za skorzystanie z usług firmy HOT. „Reaktor nuklearny reaktorem, ale nie przegapię *Asfura*" — mówi. Jeden z wędrowców bierze tablet i pyta: „A co to za aplikacja?". Naciska coś na ekranie, po czym za nimi widać wybuch w obiekcie nuklearnym. Jego towarzysze patrzą na niego zszokowani, a ten odpowiada: „No co? To tylko następna tajemnicza eksplozja w Iranie".

[19] „Sources: Iran Exposed Spying Device at Fordo Nuke Plant", Ynet (internetowy serwis informacyjny izraelskiej gazety „Yediot Ahronot"), 23 września 2012 (*http://www.ynetnews.com/articles/0,7340,L-4284793,00.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

tego zdarzenia[20]. Efekty działania Stuxneta najwyraźniej nie pozwalały Zachodowi odetchnąć.

Henry Sokolski, dyrektor wykonawczy ośrodka Nonproliferation Policy Education Center, twierdzi, że te wydarzenia nie powinny być dla nikogo zaskoczeniem. Powiedział „New Republic", że każdy prezydent od czasu Billa Clintona próbował za pomocą utajnionych operacji zakłócić irański program nuklearny i żadnemu się to nie udało. „Robił tak Bush, robi Obama" — opowiadał. Jednak utajnione operacje nigdy nie zastąpią dobrej polityki zagranicznej. Mogą być tylko „działaniami na przeczekanie", ale nie rozwiązaniem[21].

Bez odpowiedzi pozostały pytania o prawdziwą naturę działań nuklearnych Iranu. Pod koniec 2011 r. w dokumencie MAEA uznanym za „najbardziej obciążający raport kiedykolwiek opublikowany" przez tę agencję na temat Iranu napisano, że Irańczycy pracują nad bronią nuklearną od 2003 r., choć wcześniej wywiad amerykański przekonywał, że Iran w tym właśnie roku wstrzymał program zbrojeń[22].

Raport MAEA nie był oparty na nowych informacjach, ale na starszych dokumentach otrzymanych przez agencję, w tym na danych od irańskiego „kreta" o pseudonimie Delfin. Choć informacje nie były nowe, zmianą była gotowość MAEA do stwierdzenia, że dokumenty są dowodem na budowę broni atomowej[23]. Premier Izraela Beniamin Netanjahu jeszcze raz wezwał do nalotów na Iran. Tym razem Irańczycy się tym nie przejęli. Ali Akbar Salehi, minister spraw zagranicznych Iranu, powiedział wyzywająco, że Iran jest „gotowy na wojnę" z Izraelem[24].

---

[20] Fredrik Dahl, „Terrorists Embedded in UN Nuclear Watchdog May Be Behind Power Line Explosion", Reuters, 17 września 2012 (*http://news.nationalpost.com/news/terrorists-embedded-in-un-nuclear-watchdog-may-be-behind-power-line-explosion-iran*). Irański urzędnik ujawnił oba incydenty w trakcie konferencji MAEA w Wiedniu, oskarżając MAEA o współudział. Stwierdził, że dzień po tym, jak eksplozja uszkodziła linie zasilania dostarczające prąd do Fordo, inspektor z MAEA zażądał przeprowadzenia niezapowiedzianej kontroli. „Kto oprócz inspektora z MAEA mógł uzyskać dostęp do kompleksu w tak krótkim czasie, by zarejestrować i opisać uszkodzenia?" — pytał irański urzędnik.

[21] Eli Lake, *Operation Sabotage*, „New Republic", 14 lipca 2010.

[22] George Jahn, „UN Reports Iran Work »Specific« to Nuke Arms", Associated Press, 8 listopada 2011 (*https://www.yahoo.com/news/un-reports-iran-specific-nuke-arms-184224261.html*).

[23] Ali Vaez, *It's Not Too Late to Peacefully Keep Iran from a Bomb*, „The Atlantic", 11 listopada 2011.

[24] *Iran Says United and „Ready for War" with Israel*, „Ha'aretz", 3 listopada 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

JEŚLI MOŻNA POWIEDZIEĆ coś dobrego o Stuxnecie, to jest tym to, że cyfrowa broń wraz z innymi utajnionymi operacjami pozwoliła uniknąć nierozważnego ataku wojskowego na Iran. Dzięki Stuxnetowi, mimo ciągłego napięcia i licznych wybiegów, nikt nie chciał się do tego posunąć. Zostawiło to otwarte drzwi do historycznych negocjacji z Iranem dotyczących programu nuklearnego, które rozpoczęły się w 2013 r. Początkowe rozmowy sprawiły, że Iran — w zamian za rozluźnienie sankcji — zgodził się zamrozić ważne części programu, w tym wstrzymał instalowanie nowych wirówek i ograniczył ilość produkowanego wzbogaconego uranu[25].

Jednak korzyści, jakie przyniósł Stuxnet, trzeba analizować w kontekście jego negatywnych efektów. W czasie gdy Stany Zjednoczone walczyły z epidemią ataków cyberszpiegowskich ze strony Chin, atak na Iran utrudniał potępianie innych państw za cyberagresję na Stany. Jako strona, która zastosowała pierwszą znaną broń cyfrową, Stany Zjednoczone nie mogły już wygłaszać na ten temat kazań innym.

Ostatni i bardziej długotrwały skutek zastosowania Stuxneta trzeba ocenić z perspektywy ograniczonych i niepewnych korzyści jego użycia. Wypuszczenie tego złośliwego oprogramowania rozpoczęło cyfrowy wyścig zbrojeń między wielkimi i małymi państwami, co na zawsze zmieni środowisko cyberataków. Autorzy Stuxneta wyznaczyli nowe szlaki, którymi niewątpliwie podążą inni hakerzy i napastnicy sponsorowani przez państwo, a pewnego dnia cel sabotażu będzie znajdował się w Stanach Zjednoczonych.

[25] Anne Gearan, Joby Warrick, *Iran, World Powers Reach Historic Nuclear Deal*, „Washington Post", 23 listopada 2013 (*https://www.washingtonpost.com/world/national-security/kerry-in-geneva-raising-hopes-for-historic-nuclear-deal-with-iran/2013/11/23/53e7bfe6-5430-11e3-9fe0-fd2ca728e67c_story.html?utm_term=.ea5328c9c6c9*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ROZDZIAŁ 19

CYFROWA PUSZKA PANDORY

Trzydziestego maja 2009 r., kilka dni przed umieszczeniem nowej wersji Stuxneta na komputerach w Iranie, prezydent Barack Obama stanął przed ekipą prasową Białego Domu w Gabinecie Wschodnim, aby wypowiedzieć się na temat złego stanu cyberbezpieczeństwa w Stanach Zjednoczonych. „Spotykamy się w przełomowym momencie — powiedział. — Momencie historii, kiedy połączony siecią wzajemnych powiązań świat jednocześnie daje nam wielkie nadzieje i stawia przed nami wielkie trudności".

Obama oświadczył, że podobnie jak w przeszłości zaniedbaliśmy inwestycje w infrastrukturę fizyczną (drogi, mosty i tory kolejowe), tak teraz ignorujemy inwestycje w bezpieczeństwo infrastruktury cyfrowej. Ostrzegł, że cyberwłamywacze już sprawdzali odporność sieci elektrycznej, a w innych państwach całe miasta zostały pogrążone w ciemności. „Nie możemy dłużej akceptować takiego stanu rzeczy — mówił. — Nie kiedy stawka jest tak wysoka"[1].

[1] „Remarks by the President on Securing Our Nation's Cyber Infrastructure", 29 maja 2009 (*https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure*). Stwierdzenie, że cyberwłamywacze pogrążyli zagraniczne miasta w ciemności, było powtarzane przez wielu oficjeli, ale też podważane (co jednak nie powstrzymało urzędników przed przytaczaniem go). Pierwszy raz mówił o nim Tom Donahue, starszy analityk z CIA, w trakcie konferencji dla specjalistów od cyberbezpieczeństwa w 2008 r. „Mamy informacje, że cyberataki zakłóciły pracę systemów zasilania w kilku regionach poza USA — powiedział. — W przynajmniej jednej sytuacji

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Jego słowa okazały się cyniczne, gdy rok później wykryto, że Stuxnet rozprzestrzenia się po świecie, a opinia publiczna dowiedziała się, że Stany Zjednoczone nie tylko naruszyły przestrzeń innego państwa w agresywnym cyberataku, ale też prowokują tym samym do podobnych akcji wymierzonych w podatne na to amerykańskie systemy.

---

uszkodzenia spowodowały awarię zasilania obejmującą kilka miast". Dodał też, że po atakach „nastąpiły żądania okupu" (zob. Thomas Claburn, „CIA Admits Cyberattacks Blacked Out Cities", *InformationWeek*, 18 stycznia 2008, *http://www.informationweek.com/cia-admits-cyberattacks-blacked-out-cities/d/d-id/1063513*). Donahue nie wymienił wtedy nazwy państwa, w którym wystąpiły te ataki, jednak w 2009 r. w programie *60 Minutes* jako ofiarę podał Brazylię. Stwierdził, że awaria w Espirito Santo w 2007 r., która pozbawiła prądu 3 mln osób, została spowodowana przez hakerów (zob. „Cyber War: Sabotaging the System", *60 Minutes*, 6 listopada 2009, *http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/*). Inni uważali, że Donahue miał na myśli awarię w Brazylii z 2005 r. Według dwóch informatorów, z którymi rozmawiałam w 2009 r. (i którzy udzielili wywiadów dla programu *60 Minutes*), do Brazylii został wysłany reporter. Miał on zweryfikować twierdzenia o hakerach i okupie, co mu się nie udało, jednak widzowie się o tym nie dowiedzieli. Rząd Brazylii po emisji programu *60 Minutes* podważył wersję, którą przekazał Donahue, i odesłał zainteresowanych do długiego raportu na temat awarii z 2007 r., gdzie za jej przyczynę uznano sadzę i problemy ze sprzętem. Furnas, brazylijska firma energetyczna, której dotknęła awaria, jest klientem Marcela Branquinho, prowadzącego jedyną wówczas w Brazylii firmę z branży zabezpieczeń systemów kontroli procesów przemysłowych. Branquinho uważał, że nie było dowodów na to, iż awaria została spowodowana przez coś innego niż kłopoty sprzętowe. „Mamy pełny dostęp do dokumentacji i [raportów rządowych ze śledztwa badającego], co stało się w trakcie obu awarii — powiedział mi w październiku 2011 r., nawiązując do incydentów z lat 2005 i 2007. — Żadne dowody nie wskazują na aktywność hakerów. Oba zdarzenia były spowodowane problemami ze sprzętem, a nie z oprogramowaniem". Co więcej, Branquinho stwierdził, że podstacja uszkodzona w trakcie awarii z 2007 r. nie była nawet zautomatyzowanym systemem SCADA, nad którym hakerzy mogliby przejąć kontrolę. „To sam sprzęt, dlatego nie da się do niego włamać — wyjaśnił. — Nie mówię, że nie da się do nas włamać. Można to zrobić całkiem łatwo. Uważam, że większość instalacji elektrycznych — nie tylko u nas, ale na całym świecie — ma bardzo słabe zabezpieczenia w porównaniu np. do banków, gdzie infrastruktura zabezpieczeń jest na wysokim poziomie. Ale […] w omawianym przypadku dowody przemawiają za tym, że nie było włamania". Możliwe, że historie o awarii zasilania spowodowanej przez hakerów zostały pomylone z rzeczywistym cyberszantażem, który miał miejsce w 2005 lub 2006 r., ale nie był związany z wyłączeniem prądu. Dyrektor brazylijskiego Departamentu Bezpieczeństwa Informatycznego i Komunikacyjnego powiedział serwisowi *Wired.com*, że w owym incydencie napastnicy włamali się do maszyny agencji rządowej za pomocą domyślnego hasła i skasowali z niej pliki. Zażądali też okupu za zwrot danych. Jednak ten incydent nie był związany z awarią zasilania. Zob. Marcelo Soares, „WikiLeaked Cable Says 2009 Brazilian Blackout Wasn't Hackers, Either", *Wired.com*, 6 grudnia 2010 (*https://www.wired.com/2010/12/brazil-blackout*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W czasie gdy Obama i inni oficjele alarmowali, że wrogowie badają amerykańskie systemy i przygotowują się do przyszłych ataków na sieć zasilania, agencje wojskowe i wywiadowcze tego kraju penetrowały systemy w Iranie i innych państwach, budowały magazyny broni cyfrowej i wchodziły w nową erę wojen, a wszystko to bez publicznych dyskusji na temat przeprowadzania takich ataków lub ich konsekwencji. Może to wiedza o tym, co Stany Zjednoczone robią w Iranie i innych krajach, stała za ostrzeżeniami prezydenta przed zagrożeniem dla amerykańskich systemów.

Michael V. Hayden, dyrektor CIA w trakcie rozwijania i stosowania Stuxneta, po ujawnieniu tej cyfrowej broni powiedział reporterom, że „ktoś przekroczył Rubikon", wypuszczając ją[2]. Tym kimś okazały się Stany Zjednoczone. A gdy Stany Zjednoczone pokazują drogę, inne państwa idą za nimi.

Obecnie w różnych krajach świata widoczne jest zaangażowanie w rozbudowywanie lub tworzenie cyfrowej broni. Kilkanaście państw, w tym Chiny, Rosja, Wielka Brytania, Izrael, Francja, Niemcy i Korea Północna, realizuje programy prac nad bronią cyfrową lub ogłasza plany ich rozpoczęcia. Chiny rozpoczęły przygotowywanie operacji ofensywnych pod koniec lat 90., kiedy Stany Zjednoczone robiły pierwsze przymiarki do tego nowego frontu walk. Nawet Iran prowadzi program budowy broni cyfrowej. W 2012 r. ajatollah Ali Chamenei ogłosił rozpoczęcie w tym obszarze programów defensywnego i ofensywnego oraz powiedział grupie studentów, że powinni przygotować się na epokę cyberwojen z wrogami Iranu[3].

W Stanach Zjednoczonych Cyberdowództwo w Departamencie Obrony posiada obecnie roczny budżet przekraczający 3 mld dolarów i planuje pięciokrotne zwiększenie zatrudnienia, z 900 do 4900 osób zajmujących się operacjami zarówno defensywnymi, jak i ofensywnymi[4]. Agencja DARPA (ang. *Defense Advanced Research Projects Agency*) uruchomiła kosztujący 110 mln dolarów projekt badawczy Plan X. Jego celem jest opracowanie technologii cyberwojennych, które pomogą Pentagonowi zdominować cyfrowe pole bitwy. Lista planowanych technologii obejmuje aktualizowany na

[2] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, „New York Times", 1 czerwca 2012.

[3] „Iran's Supreme Leader Tells Students to Prepare for Cyber War", *Russia Today*, 13 lutego 2014 (*https://www.rt.com/news/iran-israel-cyber-war-899/*).

[4] Ellen Nakashima, *Pentagon to Boost Cybersecurity Force*, „Washington Post", 27 stycznia 2013.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

bieżąco system mapowania, śledzący wszystkie systemy i węzły w cyberprzestrzeni w celu wyświetlania przepływu danych, identyfikowania celów do ataku i wykrywania zbliżających się napaści. Pentagon chce też opracować system, który będzie potrafił błyskawicznie przeprowadzać ataki i kontrataki na podstawie wstępnie zaprogramowanych scenariuszy, dzięki czemu nie będzie potrzebna interwencja człowieka[5].

Spośród wszystkich krajów prowadzących programy cyberwojenne tylko o Stanach Zjednoczonych i Izraelu wiadomo, że zastosowały niszczycielską cyberbroń przeciw suwerennemu państwu, i to takiemu, z którym nie były w stanie wojny. W ten sposób utraciły moralne podstawy do krytykowania innych krajów za podobne poczynania i ustanowiły niebezpieczny precedens usprawiedliwiania cyfrowych ataków celami politycznymi lub związanymi z bezpieczeństwem narodowym.

„Pomysł był dobry — powiedział Hayden w programie *60 Minutes* o Stuxnecie. — Jednak przyznaję też, że to poważna sprawa. Reszta świata patrzy na nas i mówi: »Najwidoczniej ktoś usankcjonował tego typu działania jako akceptowalne«"[6].

Ataki cyfrowe mogą być teraz rozważane przez inne państwa jako sensowny sposób rozwiązywania sporów.

Robert E. Lee, generał z czasów wojny secesyjnej, powiedział kiedyś, że to dobrze, iż wojna jest tak przerażająca, „ponieważ w przeciwnym razie mogłaby nam się za bardzo spodobać"[7]. Okropności i koszty wojny zachęcają państwa do wyboru dyplomacji zamiast walk. Ponieważ cyberataki eliminują wiele kosztów i konsekwencji, a napastnicy mogą pozostać anonimowi, znacznie bardziej kuszące jest przeprowadzanie cyfrowych ataków niż angażowanie się w długotrwałe działania dyplomatyczne, które mogą nie przynieść żadnych rezultatów.

Jednak opisana tu cyfrowa broń nie tylko rozpoczęła nową epokę wojen, ale też zmieniła środowisko dla wszystkich cyberataków, otwierając drzwi do przeprowadzanych przez jednostki państwowe i prywatne operacji nowej

[5] Ellen Nakashima, *With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace*, „Washington Post", 30 maja 2012.

[6] Wywiad z Michaelem V. Haydenem w: „Stuxnet: Computer Worm Opens New Era of Warfare", *60 Minutes*, CBS, pierwsza emisja 4 czerwca 2012 (*http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/*).

[7] Z przemówienia z 1862 r. po bitwie pod Fredericksburgiem.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

generacji, które mogą powodować fizyczne zniszczenia, a nawet zabijać ludzi w niespotykany wcześniej sposób. „Przewiduję, że wszyscy zatęsknimy jeszcze za czasami robaków internetowych i szukających rozgłosu twórców wirusów do masowego rozsyłania e-maili" — napisał Kevin Haley z Symanteca o przyszłości po Stuxnecie[8]. LoveLetter, robak Conficker, a nawet trojan bankowy Zeus będą przypominać nam dni, kiedy ataki były prostsze i stosunkowo nieszkodliwe.

Stuxnet był wyjątkowym osiągnięciem, jeśli wziąć pod uwagę jego złożoność i ściśle określony cel. Był też posunięciem niezwykle nieostrożnym. Podobnie jak bomby atomowe zdetonowane w Hiroszimie i Nagasaki zapoczątkował stosowanie potężnej technologii, co będzie miało długotrwałe konsekwencje. Kennette Benedict, dyrektor wykonawcza organizacji „Bulletin of the Atomic Scientists", zwróciła uwagę na kilka analogii między Stuxnetem a pierwszymi bombami atomowymi. Przedstawiła je w artykule zamieszczonym w wydawanym przez organizację magazynie, opisując brak perspektywicznego myślenia związany z opracowaniem i zastosowaniem obu tych technologii. W obu sytuacjach rząd i naukowcy spieszyli się, by uzyskać broń dla Stanów Zjednoczonych w obawie przed tym, że przeciwnicy zbudują i zastosują ją pierwsi. Długoterminowe konsekwencje zrzucenia bomb atomowych były w latach 40. równie mało zrozumiałe co dziś skutki zastosowania broni cyfrowej. Chodzi tu nie tylko o możliwe szkody, ale też o globalny wyścig zbrojeń. „Teraz wiemy już, że broń atomowa może zniszczyć społeczeństwo i ludzką cywilizację — pisze Benedict. — Ale nie zaczęliśmy nawet rozumieć, w jaki sposób cyberwojny mogą zniszczyć nasz model życia".

Innym podobieństwem do bomb atomowych jest to, że Stany Zjednoczone — mimo ostrzeżeń — kontynuowały prace nad bronią nuklearną (a teraz cyfrową) bez publicznej debaty na temat tego, jak należy ją stosować oraz jaki będzie jej wpływ na bezpieczeństwo i pokój na świecie[9]. Dlatego zdaniem Benedict na ironię zakrawa to, „że pierwsze potwierdzone militarne zastosowanie cyberbroni ma rzekomo zapobiec rozprzestrzenianiu

[8] Kevin Haley, „Internet Security Predictions for 2011: The Shape of Things to Come", blog Symanteca, 17 listopada 2010 (*https://www.symantec.com/connect/blogs/internet-security-predictions-2011-shape-things-come*).

[9] Kennette Benedict, *Stuxnet and the Bomb*, „Bulletin of the Atomic Scientists", 15 czerwca 2012 (*http://thebulletin.org/stuxnet-and-bomb*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

broni atomowej. Nowa epoka masowego zniszczenia rozpoczyna się próbą zamknięcia rozdziału z pierwszej ery broni masowej zagłady".

Mimo tych analogii występuje przynajmniej jedna istotna różnica między bombami atomowymi z lat 40. a Stuxnetem. Zbudowanie lub zdobycie broni atomowej (podobnie zresztą jak pocisków konwencjonalnych lub bomb innego typu) było trudne. Jednak cyberbroń może zostać łatwo zakupiona na czarnym rynku lub, w zależności od poziomu złożoności docelowego systemu, samodzielnie zbudowana od podstaw przez uzdolnionego nastoletniego programistę. Jest to o tyle prostsze, że każda cyberbroń zawiera w sobie projekty jej budowy. Zastosowanie cyberbroni oznacza nie tylko wypuszczenie jej przeciw wrogom, ale też udostępnienie własności intelektualnej i umożliwienie zwrócenia broni przeciw jej twórcom[10]. Można to porównać z sytuacją, gdyby w 1945 r. wraz z opadem radioaktywnym z bomb na Hiroszimę i Nagasaki spadły wszystkie naukowe równania i schematy potrzebne do zbudowania takiej broni.

Najbardziej narażone na niszczycielskie ataki cyfrowe są oczywiście państwa o najbardziej rozwiniętych sieciach. Marcus Ranum, jeden z innowatorów w dziedzinie zapór komputerowych, nazwał Stuxneta kamieniem rzuconym przez ludzi mieszkających w szklanym domu[11].

---

[10] Istnieją sposoby na ograniczenie ryzyka. Wymaga to starannego zaszyfrowania broni cyfrowej, aby zapobiec zastosowaniu inżynierii odwrotnej kodu przez przypadkowe jednostki, które uzyskają do niego dostęp. Broń cyfrowa musi odszyfrować samą siebie, aby uruchomić ładunek po znalezieniu docelowego systemu. Jednak potrzebne do tego klucze nie muszą znajdować się w samej broni (jak w Stuxnecie). Lepszy jest projekt zastosowany w Gaussie, gdzie wykorzystano złożony schemat szyfrowania z generowaniem klucza deszyfrującego na podstawie konfiguracji docelowego systemu. Gauss dostarczał i odszyfrowywał ładunek tylko po znalezieniu konkretnej konfiguracji. Ta technika nie sprawdzi się, jeśli konfiguracja docelowego systemu ulegnie zmianie, co zdezaktywuje broń. Opisana metoda jest natomiast przydatna w sytuacjach, gdy modyfikacja konfiguracji jest mało prawdopodobna. Zob. omówienie Gaussa na s. 304 – 305. Ponadto aby ograniczyć widoczność cyfrowej broni po jej odszyfrowaniu w docelowym systemie, powinna się ona sama usuwać po zakończeniu misji, tak by nie pozostawać w systemie dłużej, niż jest to konieczne. Ale nie we wszystkich scenariuszach jest to dobre rozwiązanie. Na przykład Stuxnet musiał pozostawać w systemie przez długi czas, aby wykonać swoje zadanie. Ta technika jest szczególnie przydatna w broniach, które szybko wyrządzają szkody.

[11] Marcus Ranum, „Parsing Cyberwar — Part 4: The Best Defense Is a Good Defense", opublikowane na blogu Fabius Maximus autora, 20 sierpnia 2012 (*https://fabiusmaximus.com/2012/08/20/41929/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Stuxnet był dowodem na to, że cyfrowy atak składający się wyłącznie z binarnych rozkazów pozwala wyrządzić podobne zniszczenia co konwencjonalna bomba. Jednocześnie pokazał, że nawet potężne państwa, takie jak Stany Zjednoczone, o niezrównanych siłach powietrznych i morskich, mogą być podatne na analogiczne ataki ze strony przeciwników, którzy nigdy nie będą musieli przekraczać granic, by przeprowadzić taką operację. Mike McConnell, były dyrektor wywiadu narodowego, w 2011 r. powiedział amerykańskiej komisji senackiej: „Gdybyśmy dziś przystąpili do wojny, cyberwojny, przegralibyśmy. Jesteśmy najbardziej podatni na ataki. Mamy najbardziej rozwinięte sieci. Mamy najwięcej do stracenia”[12].

W Stanach Zjednoczonych najbardziej narażone na ataki są nie systemy militarne, ale cywilne: sieci transportowe, komunikacyjne i finansowe, zakłady chemiczne i spożywcze, gazociągi, przedsiębiorstwa wodociągowe i kanalizacyjne, elektrownie, a nawet zakłady wzbogacania uranu[13]. „Żyjemy w świecie, w którym systemy kontroli procesów przemysłowych mogą zostać zaatakowane w kryzysowej sytuacji — powiedział Stewart Baker, były zastępca sekretarza Departamentu Bezpieczeństwa Wewnętrznego. — Nie mamy skutecznego planu obrony naszych systemów kontroli procesów przemysłowych, choć wszyscy mieszkańcy są od nich zależni”[14].

Infrastruktura krytyczna zawsze stanowiła potencjalny cel w czasach wojny. Natomiast infrastruktura cywilna w Stanach Zjednoczonych była przez długi czas bezpieczna dzięki dużej odległości tego kraju od jego wrogów i pól walki. Jednak gdy polem walki jest cyberprzestrzeń, ta przewaga zostaje utracona. W sieci podłączonych do internetu komputerów każdy system może okazać się linią frontu. „Nie istnieją »bezpieczne strefy« ani »tyły«;

---

[12] Grant Gross, „Security Expert: US Would Lose Cyberwar”, IDG News Service, 23 lutego 2010 (*http://computerworld.com/article/2520058/security0/security-expert--us--would-lose-cyberwar.html*).

[13] Choć systemy kontroli Siemensa nie są stosowane w Stanach Zjednoczonych równie często jak w innych częściach świata, systemy najpowszechniej używane w Stanach działają wedle tych samych zasad i mają te same wady. Napastnik musi tylko zbadać system, aby znaleźć sposób na zaatakowanie go. Po wypuszczeniu Stuxneta wielu badaczy zabezpieczeń przeprowadziło już takie analizy.

[14] Gerry Smith, „Stuxnet: U.S. Can Launch Cyberattacks but Not Defend Against Them, Experts Say”, *Huffington Post*, 1 czerwca 2012 (*http://www.huffingtonpost.com/2012/06/01/stuxnet-us-cyberattack_n_1562983.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

wszyscy jesteśmy w równym stopniu podatni na atak" — powiedział Kongresowi gen. Kevin Chilton, szef Dowództwa Strategicznego Stanów Zjednoczonych[15].

Prawo wojenne nie zezwala na bezpośrednie ataki na szpitale i inną infrastrukturę cywilną, chyba że wymagają tego działania wojenne. Złamanie tych zasad skutkuje oskarżeniem dowódców o zbrodnie wojenne. Jednak ochrona prawna nie sprawdza się, gdy trudno jest wskazać sprawcę. Ponieważ włamanie dokonane przez cyberarmię z Teheranu lub Pekinu można łatwo przeprowadzić tak, aby jego źródłem wydawało się Ohio, trudno będzie odróżnić atak ze strony Iranu od akcji grupy hakerów mającej na celu wywołanie chaosu lub protest obywatelski. Stuxnet był zaawansowany i nosił wszelkie oznaki akcji przeprowadzonej przez państwo. Niestety, nie każdy atak będzie równie oczywisty[16].

Zdaniem niektórych osób ataki ze strony państw będą łatwe do zauważenia, ponieważ nastąpią w okresie napięcia między określonymi krajami.

---

[15] Wystąpienie przygotowane dla Podkomisji ds. Sił Strategicznych Komisji Sił Zbrojnych na 17 marca 2009 r. (*https://www.gpo.gov//fdsys/pkg/CHRG-111hhrg51759/html/CHRG-111hhrg51759.htm*).

[16] W sierpniu 2012 r. niszczycielski wirus Shamoon zaatakował maszyny w Saudi Aramco (państwowej firmie z Arabii Saudyjskiej, zajmującej się wydobyciem ropy i gazu), usuwając wszystkie dane z ponad 30 tys. maszyn. Atak ten był brutalnym przypomnieniem, jak wiele komputerów podłączonych do internetu może znaleźć się w „strefie zero" w sytuacji konfliktu politycznego i jak trudno jest później zidentyfikować napastników. Wirus nie ograniczył się do usunięcia danych z maszyn. Ponadto zastąpił każdy plik rysunkiem płonącej amerykańskiej flagi, choć błąd w kodzie uniemożliwił wyświetlenie całej grafiki. Zamiast tego po otwarciu plików pojawiał się tylko fragment rysunku. Amerykańscy oficjele oskarżyli o ten atak Iran, choć nie przedstawili na to dowodów. Operacja mogła zostać przeprowadzona przez Iran w odwecie za atak Wipera, który cztery miesiące wcześniej wykasował dane z maszyn irańskiego ministerstwa ropy naftowej i firmy Iranian National Oil Company. Mogła to być także zemsta za Stuxneta wymierzona w sojusznika Stanów Zjednoczonych, który miał mniejsze możliwości rewanżu. Jeszcze inna możliwość to przeprowadzenie akcji przez haktywistów sprzeciwiających się polityce zagranicznej Stanów Zjednoczonych na Bliskim Wschodzie. Do ataku przyznała się grupa hakerów nazywająca się Cutting Sword of Justice (czyli „siekący miecz sprawiedliwości"). Możliwe też, że była to przeprowadzona przez inny kraj operacja „pod fałszywą flagą", która miała wyglądać, jakby napastnikiem był Iran. Z dokumentów agencji NSA ujawnionych przez Edwarda Snowdena wynika, że Wielka Brytania czasem przeprowadza takie akcje, by obwiniać o nie innych.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dzięki temu tożsamość napastników będzie oczywista — tak jak w przypadku ataków DoS, które spowodowały zablokowanie gruzińskich witryn rządowych w 2008 r. przed rosyjską inwazją na Osetię Południową. Nawet wtedy łatwo będzie trzeciej stronie wykorzystać spory między dwoma państwami i przeprowadzić na jedno z nich anonimowy atak wyglądający jak operacja drugiego kraju, co może skutkować dodatkowym zaognieniem sytuacji[17].

W listopadzie 2013 r. Izrael przeprowadził na Uniwersytecie Telawiwskim ćwiczenia, które pokazały, jak trudno jest zidentyfikować napastnika, zwłaszcza gdy trzecia strona miesza się w konflikt z zamiarem eskalacji napięcia. W scenariuszu tej gry wojennej (nazwanym skrajnym, ale realistycznym) Iran i wspierany przez to państwo na terenie Libanu i Syrii Hezbollah starły się z Izraelem, przeprowadzając przeciw Izraelczykom serię symulowanych fizycznych akcji, które zostały wyeskalowane do postaci cyberataków grożących wciągnięciem w konflikt Stanów Zjednoczonych i Rosji chcących bronić swoich sojuszników.

Symulacja rozpoczęła się od eksplozji na platformie wiertniczej i wystrzelenia rakiet z Libanu na północny Izrael i Tel Awiw. Po tym nastąpiło uszkodzenie sieci paraliżujące pracę szpitala w Izraelu. Wyśledzono, że źródłem cyberataków był serwer w Iranie, jednak państwo to wyparło się odpowiedzialności i utrzymywało, że Izraelczycy próbują je obwinić, aby zyskać wsparcie Zachodu dla ataku na Teheran. Później ataki w sieci rozprzestrzeniły się na Stany Zjednoczone, co wymusiło wstrzymanie handlu na Wall Street i kontroli ruchu lotniczego na lotnisku JFK. Biały Dom ogłosił stan wyjątkowy po tym, jak dwa samoloty rozbiły się przy lądowaniu, co spowodowało śmierć 700 osób. Tym razem ataki prowadziły najpierw do serwera w Kalifornii, a dalej, co zaskakujące, do Izraela.

W momencie zakończenia gry Izrael był gotowy do przeprowadzenia fizycznych ataków na Hezbollah w Syrii i Libanie (z powodu cyberataków przypisywanych Hezbollahowi i Iranowi), przy czym napięcie między Stanami Zjednoczonymi a Izraelem wzrosło do niebezpiecznego poziomu

[17] W sierpniu 2008 r. armia komputerów z rosyjskimi adresami IP przeprowadziła rozbudowany atak DoS, który zablokował gruzińskie witryny rządowe i informacyjne, uniemożliwiając rządowi komunikowanie się z mieszkańcami. Moment przeprowadzenia ataku, tuż przed rosyjską inwazją na Osetię Południową, był dla wielu osób wystarczającym dowodem na to, że ta cyfrowa operacja jest częścią akcji militarnej.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

z powodu pytań o to, kto odpowiadał za ataki na Stany[18]. „Gdybyśmy nie zatrzymali się w tym momencie, cały region mógł stanąć w płomieniach" — powiedział Haim Assa, ekspert od teorii gier, który zaprojektował te ćwiczenia.

Ta symulacja okazała się pouczająca dla uczestników na kilku poziomach. Stany Zjednoczone „zdały sobie sprawę, jak trudne, jeśli nie niemożliwe, jest pewne określenie źródła ataku" — powiedział Wesley Clark, emerytowany generał armii Stanów Zjednoczonych, który uczestniczył w tych ćwiczeniach. Izraelski oficjel zauważył, że „lokalne cyberincydenty mogą szybko stać się niebezpiecznie kinetyczne, gdy dowódcy nie są przygotowani do działań w cyberprzestrzeni". Pod tym względem uczestnicy nauczyli się, że w cyfrowym świecie najlepszą obroną jest nie dobry atak, ale dobre zabezpieczenie, ponieważ bez odpowiednio chronionej infrastruktury krytycznej dowódcy mają niewielkie pole manewru, gdy nastąpi atak. Jeśli systemy cywilne zostaną zaatakowane i spowoduje to śmierć obywateli, dowódcy znajdą się pod presją szybkiego podejmowania decyzji, często na podstawie fałszywych lub niekompletnych wniosków[19].

ŁATWO JEST ZROZUMIEĆ, dlaczego wojsko i rząd chcą stosować cyberbroń. Oprócz zapewniania anonimowości i — przynajmniej w założeniu — zmniejszenia liczby przypadkowych ofiar cyberbroń działa szybciej niż pociski i może dotrzeć do celu w ciągu sekund. Ponadto można ją na bieżąco modyfikować, by zwalczyć zbudowane zabezpieczenia. Jeśli luka typu zero-day zostanie załatana, napastnicy mogą skorzystać z innych eksploitów ze swojego arsenału (jak zrobili to twórcy Stuxneta) lub zmodyfikować i ponownie skompilować kod, aby zmienić sygnatury i uniknąć prób wykrycia.

[18] Twórcy symulacji ujawnili później, że wprawiające w konsternację możliwości przypisania źródeł cyberataków różnym jednostkom były bardzo ważnym aspektem gry. Według planu twórców to Al-Kaida przeprowadziła pierwsze ataki wymierzone w Iran, chcąc zwiększyć napięcie między Izraelem a wspieranym przez Iran Hezbollahem w Libanie. Jednak to Iran zaatakował Stany Zjednoczone. Te ataki miały wyglądać tak, jakby przeprowadził je Izrael, chcąc obwinić o nie Irańczyków. Stany Zjednoczone miały uznać, że Izrael posłużył się brudną sztuczką i zaatakował Stany, aby zrzucić winę na Iran i zyskać poparcie Amerykanów dla nalotów na Teheran.

[19] Barbara Opall-Rome, „Israeli Cyber Game Drags US, Russia to Brink of Mideast War", *Defense News*, 14 listopada 2013 (*http://strategicstudyindia.blogspot.com/2013/11/israeli-cyber-game-drags-us-russia-to.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Moim skromnym zdaniem cyberprzestrzeń zostanie wkrótce uznana za największą rewolucję w sztuce wojennej, większą niż proch i wykorzystanie sił powietrznych w ubiegłym wieku" — powiedział Aviv Kochavi, izraelski generał dywizji[20].

Jednak cyberbroń ma ograniczone zastosowania. Jeśli, tak jak Stuxnet, jest ściśle wyspecjalizowana, by uniknąć przypadkowych zniszczeń, można ją zastosować tylko do niewielkiej grupy celów. Inne ataki będą wymagały jej przeprojektowania. Ponadto, w odróżnieniu od bomb penetrujących i pocisków typu stealth, cyberbroń może błyskawicznie stać się przestarzała, gdy zmieni się konfiguracja docelowego systemu lub sieci. „Nie znam w historii wojskowości żadnego innego systemu broni, który po dotarciu do celu może zostać zablokowany kliknięciem myszy" — zauważył Marcus Ranum[21]. Za każdym razem, gdy cyberbroń jest ujawniana, zostaje spalona nie tylko ona sama, ale też inne operacje wykorzystujące te same nowatorskie techniki i metody. „Obecnie możemy mieć pewność, że każdy, kto buduje kaskadę z wirówkami gazu, zachowa większą niż zwykle ostrożność w kwestii oprogramowania" — powiedział Thomas Rid, naukowiec z londyńskiego King's College zajmujący się sztuką wojenną[22].

Inny problem z bronią cyfrową polega na tym, że może być trudna do kontrolowania. Dobra cyberbroń powinna działać przewidywalnie — powodować kontrolowane skutki i za każdym razem dawać oczekiwane wyniki, wyrządzając jak najmniej przypadkowych szkód. Trzeba ją precyzyjnie zaprojektować, by działała tylko na rozkaz lub automatycznie w reakcji na wykrycie celu. Powinna też umożliwiać odwołanie jej lub obejmować mechanizm autodestrukcji na wypadek zmiany warunków albo konieczności zakończenia misji. Andy Pennington, cytowany wcześniej były oficer systemów broni w Siłach Powietrznych, porównuje niekontrolowaną cyberbroń do czynnika biologicznego, nad którym twórcy utracili panowanie. „Jeśli nie masz pełnej kontroli nad bronią […] nie masz broni; zostaje ci tykająca bomba. Opracowaliśmy konwencje i zgodziliśmy się, że nie

[20] „Israel Combats Cyberattacks, »Biggest Revolution in Warfare«", UPI, 31 stycznia 2014 (*http://www.upi.com/Israel-combats-cyberattacks-biggest-revolution-in-warfare/24501391198261/*).

[21] Marcus Ranum, „Parsing Cyberwar — Part 3: Synergies and Interference", opublikowane na blogu Fabius Maximus autora, 13 sierpnia 2012 (*https://fabiusmaximus.com/2012/08/13/41567/*).

[22] Thomas Rid, *Think Again: Cyberwar*, „Foreign Policy", marzec – kwiecień 2012.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

będziemy stosować broni biologicznej ani chemicznej, ponieważ nie potrafimy nią precyzyjnie sterować, nie mamy mechanizmów kontroli dostępu do niej, nie da się jej odwołać i nie ma ona mechanizmu autodestrukcji"[23].

Stuxnet posiadał wbudowane pewne mechanizmy kontrolne, jednak innych w nim zabrakło. Był precyzyjną bronią uwalniającą ładunek wyłącznie w specyficznych systemach, które miał atakować. Posiadał też aktywator czasowy i rozpoczynał sabotaż tylko wtedy, gdy w docelowych maszynach spełnione były określone warunki. Jednak po uwolnieniu Stuxneta nie dało się odwołać. Robak nie miał też mechanizmu autodestrukcji. Określono jedynie datę zakończenia infekcji, zapobiegającą powielaniu kodu po upływie ustalonego dnia oddalonego o trzy lata naprzód. Ponadto choć pierwsze wersje Stuxneta miały ograniczone możliwości rozprzestrzeniania się, wersja z marca 2010 r. zdecydowanie stała się „tykającą bombą", choć rozbrojoną, ponieważ rozprzestrzeniła się w niekontrolowany sposób po tysiącach maszyn, które nie były jej celem, ale nie dokonała ich sabotażu.

Czy inne bronie cyfrowe będą równie dobrze zaprojektowane i czy ich twórcy będą mieli tyle samo szczęścia? Przypadkowe szkody w cyberprzestrzeni mogą objąć większy obszar niż w świecie fizycznym. Bomba zrzucona na cel może zniszczyć przypadkowe obiekty, ale jej zasięg jest lokalny. Natomiast sieci komputerowe to skomplikowane labirynty wzajemnych połączeń, a ścieżka i wpływ cyberbroni po jej uwolnieniu nie zawsze są przewidywalne. „Nie potrafimy jeszcze dla wszystkich cyberataków określić zasięgu przypadkowych szkód — zauważył Jim Lewis z Centrum Studiów Strategicznych i Międzynarodowych. — W atakach wyłączających sieci mogą wystąpić nieoczekiwane szkody nie tylko po stronie wroga, ale też w jednostkach cywilnych i neutralnych, a nawet po stronie napastnika. Dlatego polityczne ryzyko związane z niezamierzonymi skutkami jest w tym przypadku nieprzewidywalne (np. atak na serbskie sieci może zaszkodzić działalności handlowej sojuszników NATO) i grozi eskalacją konfliktu (atak na Koreę Północną może wyłączyć usługi w Chinach)"[24].

[23] Z wywiadu przeprowadzonego przez autorkę z Andym Penningtonem w listopadzie 2011 r.

[24] James A. Lewis, *Cyberwar Thresholds and Effects*, „IEEE Security and Privacy", wrzesień 2011, s. 23 – 29.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

MIMO WIDOCZNEGO ZMIERZANIA w kierunku broni cyfrowej, co zapoczątkował Stuxnet, warto zadać pytanie o prawdopodobieństwo wystąpienia katastroficznych zdarzeń cyfrowych. Sekretarz obrony Leon Panetta powiedział, że Stany Zjednoczone znajdują się „w momencie sprzed 11 września", a przeciwnicy tworzą plany i czekają na dobrą okazję do przeprowadzenia niszczycielskich cyberataków na systemy tego kraju. Jednak Thomas Rid nazwał cyberwojnę bardziej rozdmuchaną sprawą niż zagrożeniem, nową błyskotką, która przyciągnęła uwagę wojskowych podobnie jak lśniący nowy zestaw zabawkowych kolejek pod choinką w Wigilię. Rid uważa, że w rzeczywistości cyfrowa broń będzie miała znacznie mniejszy wpływ, niż ludzie sądzą[25]. W przyszłości broń cyfrowa będzie raczej wspomagać konwencjonalne działania na polu walki zamiast je zastępować. Krytycy głosicieli cyfrowej apokalipsy wskazują też na fakt, że do dziś nie nastąpił żaden katastroficzny atak. Ich zdaniem jest to dowód na to, że wszelkie przestrogi są przesadne.

Mimo to inni przekonują, że do 11 września też żaden samolot pasażerski nie został skierowany w wieżowiec. „Uważam, że […] jest zdecydowanie zbyt wcześnie, by mówić, iż coś jest niemożliwe lub nieprawdopodobne. W ciągu następnych kilku lat może wydarzyć się wiele rzeczy — powiedział Jason Healey, szef programu Cyber Statecraft Initiative w Radzie Atlantyckiej w Waszyngtonie, członek pierwszej wojskowej cybernetycznej grupy roboczej. — Ponieważ coraz więcej systemów jest podłączanych do internetu, a cyberataki przechodzą od uszkadzania zer i jedynek do niszczenia obiektów z betonu i stali, sytuacja się zmieni. Czasy, kiedy nikt nie ginął od cyberataków lub ich efektów, przeminą"[26].

Zdaniem części specjalistów zagrożenie jest wyolbrzymiane, ponieważ większość podmiotów zdolnych do przeprowadzenia ataku nie zrobi tego z obaw przed kontratakiem. Niektóre osoby po wykryciu Stuxneta zastanawiały się nawet, czy ten robak nie został celowo spalony przez Izrael i Stany Zjednoczone, by przesłać Iranowi i innym państwom komunikat dotyczący możliwości tych krajów w zakresie cyfrowych ataków. To, że Stuxnet pozostawał w ukryciu przez tak długi czas i został znaleziony przez mało znaną firmę antywirusową z Białorusi, sprawiło, że niektórzy

[25] Rid, *Think Again: Cyberwar*.

[26] Te i inne słowa Healeya pochodzą z wywiadu przeprowadzonego przez autorkę w październiku 2013 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

eksperci uznali, iż robak został nie tyle odkryty, ile ujawniony. Generał James Cartwright, były wiceprzewodniczący Kolegium Połączonych Szefów Sztabów — uważany za człowieka, który odegrał istotną rolę w operacji Olympic Games — był zwolennikiem ujawniania amerykańskich cybermożliwości w celu odstraszania wrogów.

„Aby cyberodstraszanie zadziałało — mówił Cartwright w 2012 r. — musimy pamiętać o kilku rzeczach: po pierwsze o tym, że mamy cel, po drugie o tym, że mamy możliwości, po trzecie o tym, że ćwiczymy i że inni o tym wiedzą"[27]. Cartwright był później przesłuchiwany przez Departament Sprawiedliwości w sprawie podejrzeń o ujawnienie poufnych informacji o Stuxnecie gazecie „New York Times". Jednak do momentu powstania tej książki nie został oskarżony o żadne wykroczenia i nie przyznał się do stawianych zarzutów.

Choć taka strategia może zadziałać w przypadku niektórych państw — o ile uznają one, że ktoś zdoła powiązać z nimi atak — irracjonalnych podmiotów, np. wrogich państw lub grup terrorystycznych, może to nie odstraszać. „Gdy tylko grupa terrorystyczna zdobędzie umiejętność przeprowadzania cyberataków, wykorzysta ją" — powiedział Jim Lewis Kongresowi w 2012 r.[28].

Lewis spodziewa się, że w przyszłości między Stanami Zjednoczonymi a Rosją lub Chinami mogą nastąpić drobne cyfrowe konflikty zakłócające pracę systemów C&C, jednak państwa te „z powodu ryzyka eskalacji" zapewne nie będą atakować infrastruktury krytycznej. Jednak gdy kraje takie jak Iran lub Korea Północna zdobędą możliwości przeprowadzania cyberataków, operacje wymierzone w cele cywilne w Stanach Zjednoczonych staną się bardziej prawdopodobne. Skoro Siły Powietrzne Stanów Zjednoczonych bombardują obiekty na ich terenach, kraje te „będą miały niewielkie lub zerowe opory przed zaatakowaniem celów u nas", napisał Lewis w pracy z 2010 r.[29]. Groźby odwetu wygłaszane przez Stany Zjednoczone w celu odstraszenia wrogów od takich akcji będą miały niewielki wpływ na tego rodzaju grupy, ponieważ „ich rachunki w trakcie podejmowania

[27] Julian Barnes, *Pentagon Digs In on Cyberwar Front*, „Wall Street Journal", 6 lipca 2012.

[28] James A. Lewis, wystąpienie przed Podkomisją ds. Cyberbezpieczeństwa, Zabezpieczania Infrastruktury i Technologii Związanych z Ochroną, 16 marca 2012.

[29] James A. Lewis, „Thresholds for Cyberwar", Centrum Studiów Strategicznych i Międzynarodowych, wrzesień 2010 (*https://www.csis.org/analysis/thresholds-cyberwar*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

decyzji o ataku są oparte na innym postrzeganiu zagrożeń i zysków". Ponadto gdy mniejsze kraje i inne podmioty zdobędą cyfrowe środki do ataków na oddalone cele, „zakłócenia wywoływane w celach politycznych, a nawet cyberataki mające wyrządzać szkody lub zniszczenia mogą stać się codziennością". Talibowie w Afganistanie lub bojownicy Asz-Szabab w Somalii mają niewielkie szanse przeprowadzenia konwencjonalnych odwetowych uderzeń na tereny Stanów Zjednoczonych, ale gdy zdobędą umiejętność przeprowadzania skutecznych cyberataków (lub wynajmą do tego odpowiednich ludzi), sytuacja się zmieni. „Takie uderzenia będą dla nich atrakcyjne, ponieważ umożliwiają przeniesienie wojny na terytorium USA" — stwierdził Lewis. Jego zdaniem możliwe jest, że takie jednostki wprawdzie nie będą potrafiły przeprowadzać ataków na masową skalę, ale prowadzenie „nękających działań" wymierzonych w konkretne cele, jak np. miasto Waszyngton, z pewnością będzie w ich zasięgu. W zależności od dotkliwości ataków i ich kaskadowych efektów ważne systemy i usługi mogą zostać zablokowane na długi czas.

Lewis zauważa też, że gdy inne podmioty zdobędą cyberbroń, możliwe, że Stany Zjednoczone w trakcie planowania konwencjonalnych ataków będą musiały zacząć uwzględniać ryzyko odwetu. W 2003 r. siły amerykańskie w Iraku napotkały niewielki opór, co by się jednak stało, gdyby Irakijczycy posiadali cyberbroń i w rewanżu ją zastosowali? „Nie zmieniłoby to wyniku inwazji, ale pozwoliłoby [Irakowi] wywrzeć jakąś zemstę" — uznał Lewis[30].

Pojawiają się więc różne opinie na temat prawdopodobieństwa ataków cyfrowych wymierzonych w infrastrukturę krytyczną. Specjaliści nie zgadzają się też co do zakresu szkód, jakie taki atak może spowodować. Leon Panetta i inni przestrzegali przed cyfrowym Pearl Harbor i cybernetycznym 11 września, które mogą wywołać strach w całym kraju. Jednak zdaniem części osób wyrządzenie cyfrowych zniszczeń, o jakich piszą katastrofiści, wcale nie jest łatwe. Przeprowadzenie niszczycielskiego ataku o długotrwałych efektach „jest dużo bardziej skomplikowanym przedsięwzięciem niż nakierowanie samolotu na budynek lub wysadzenie ciężarówki pełnej materiałów wybuchowych na zatłoczonej ulicy" — stwierdził W. Earl Boebert, były ekspert ds. cyberbezpieczeństwa w Laboratorium Narodowym Sandia, którego praca polegała m.in. na analizowaniu scenariuszy tego rodzaju.

[30] *Ibid.*

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Sieci i systemy można wyłączyć, ale stosunkowo szybko można też je ponownie uruchomić. „Trzeba przygotować solidny plan, aby zwiększyć prawdopodobieństwo sukcesu do poziomu, na którym można podjąć racjonalną decyzję o kontynuowaniu działań" — napisał Boebert[31]. Choć zdaniem niektórych wydarzenia z 11 września i niszczycielskie ataki wymagają porównywalnie dużo planowania i koordynacji, to dobrze przygotowana cyfrowa operacja, nawet powodująca szkody fizyczne, zapewne nigdy nie dorówna wizualnemu wpływowi lub przerażającym skutkom emocjonalnym odrzutowców wlatujących w wieżowce Twin Towers.

MIMO ZAGROŻEŃ I możliwych konsekwencji związanych ze stosowaniem broni cyfrowej nie było prawie żadnej debaty publicznej na temat wątpliwości wzbudzonych przez ofensywne operacje rządowe. Krytycy zwracali uwagę, że administracja Obamy z większą otwartością dyskutowała o zabójstwie Osamy bin Ladena niż o ofensywnej cyberstrategii i operacjach w tym obszarze. Gdy w 2010 r. w trakcie przesłuchania zatwierdzającego mianowanie gen. Keitha Alexandra na szefa Cyberdowództwa Stanów Zjednoczonych padły pytania o zasady zaangażowania się w ataki cyfrowe, Alexander odmówił publicznego udzielenia odpowiedzi i powiedział, że ustosunkuje się do tych kwestii tylko w ramach tajnego posiedzenia[32]. Ponadto choć

[31] W. Earl Boebert, „A Survey of Challenges in Attribution", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*, opublikowane przez National Academy of Sciences (*https://www.nap.edu/read/12997/chapter/5*).

[32] Zasady zaangażowania to przestrzegane przez wojsko reguły uwzględniające prawo międzynarodowe i politykę Stanów Zjednoczonych opisane w jednym dokumencie, do którego stosuje się armia, prowadząc operacje. Istnieją zasady zaangażowania dotyczące różnych działań. Reguły zmieniają się w zależności od tego, czy prowadzona jest misja pokojowa w Bośni, czy ofensywna inwazja na Irak. Oprócz nich istnieje też ogólny zestaw zasad zaangażowania obowiązujący wojskowych w codziennych działaniach. Te ostatnie zasady, w dużej części niejawne, obejmują działania cybernetyczne. Według Gary'ego Browna, radcy prawnego Cyberdowództwa Stanów Zjednoczonych w latach 2009 – 2012, w trakcie jego współpracy z dowództwem trwały prace nad zmianami tych reguł. W 2014 r. Brown stwierdził, że nie wie, czy zostały one ukończone. Gdy współpracował z armią, wojsko posługiwało się drugą wersją zasad, opracowaną w 2005 r. i nazywaną wersją Bravo. Trzecia wersja, Charlie, miała zostać ukończona w 2010 r., jednak do czasu odejścia Browna w 2012 r. wciąż nie była gotowa. W wersji Bravo uwzględniono kwestie cybernetyczne, ale tylko na ogólnym poziomie. W wersji Charlie mają być one opisane bardziej szczegółowo.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

dostępnych jest wiele podręczników dotyczących doktryn konwencjonalnych działań wojennych, nie istnieją analogiczne materiały poświęcone cyberoperacjom. Nawet osoby, których kariera jest zbudowana na poufności, zauważyły niezwykłą tajemniczość w dziedzinie cyberataków. „Może się to wydać zaskakujące, jeśli wziąć pod uwagę moją karierę w NSA i CIA, ale uważam, że te informacje mają zdecydowanie za wysoki poziom tajności — powiedział gen. Michael Hayden, były dyrektor CIA i NSA. — Podstawą amerykańskiej cyberpotęgi jest amerykański wywiad, gdzie naprawdę jesteśmy przyzwyczajeni do pracy w świecie, w którym wszystko jest tajne. Obawiam się, że ta kultura wpłynęła na to, jak traktujemy wszystkie cyberkwestie"[33].

Bez większej transparentności, bez gotowości do dyskusji na temat operacji ofensywnych jednostkom niezainteresowanym bezpośrednio ich kontynuowaniem trudno będzie ocenić sukcesy, porażki i zagrożenia związane z takimi akcjami.

„Stuxnet spowodował wypuszczenie dżina z butelki, jeśli chodzi o to, jak przeprowadzać tego rodzaju ataki. Teraz można obrać za cel także wiele innych urządzeń — powiedział jeden z byłych pracowników rządowych. — Dokąd to zmierza? Nie wygląda na to, by prowadzone programy były przez kogoś nadzorowane. Niestety, naukowcy nie hamują zapędów innych jednostek. Są podekscytowani faktem, że ktoś daje im pieniądze na badania. Nie przypominam sobie, by ktokolwiek kwestionował to, co się dzieje. Moim zdaniem ludzie są w niewielkim stopniu świadomi rozwoju sytuacji".

Nie odbyła się nawet publiczna debata na temat skutków w postaci cyfrowego wyścigu zbrojeń zapoczątkowanego przez Stuxneta lub konsekwencji wypuszczenia broni, która może być nieprzewidywalna i zostać zwrócona przeciw Stanom Zjednoczonym.

W raporcie dla Kongresu z 2011 r. wywiad stwierdził, że osoby zabezpieczające sieci komputerowe w Stanach Zjednoczonych są regularnie pokonywane przez napastników i nie mogą nadążyć za zmianami stosowanych przez nich taktyk. Eksploity i techniki ataków zmieniają się zbyt szybko, aby dostosować do nich metody wykrywania włamań i środki zaradcze. Problem ten będzie się jeszcze nasilał, gdy państwa zaczną rozwijać i stosować

[33] Chris Carroll, „Cone of Silence Surrounds U.S. Cyberwarfare", *Stars and Stripes*, 18 października 2011 (*https://www.stripes.com/news/cone-of-silence-surrounds-u-s-cyberwarfare-1.158090*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

coraz bardziej zaawansowane sposoby ataku. Do tej pory ewolucja ataków komputerowych była napędzana innowacjami wprowadzanymi przez przestępcze podziemie. To się jednak zmieni, gdy prowadzone przez państwo ataki (takie jak z użyciem Stuxneta i Flame'a) zaczną napędzać przyszłe postępy. Wtedy to nie hakerzy rządowi będą uczyć się nowatorskich technik od podziemia, ale przestępcy będą się uczyć od jednostek rządowych. Ponadto wraz z pojawieniem się środków zaradczych przeciw broni cyfrowej konieczne stanie się budowanie jeszcze bardziej zaawansowanych broni, co dodatkowo będzie przyspieszać innowacje. Jeden z urzędników amerykańskich nazwał Stuxneta bronią pierwszej generacji, porównywalną z „pierwszymi żarówkami Edisona lub komputerem Apple II". Zasugerował w ten sposób, że Stuxnet został już zastąpiony bardziej zaawansowanymi rozwiązaniami[34].

Przestępcze podziemie skorzysta na wielu sponsorowanych przez rząd badaniach i pracy włożonej w broń cyfrową i narzędzia szpiegowskie. Już tak się stało w przypadku Stuxneta i arsenału używanych razem z nim narzędzi. Na przykład po wykryciu Duqu w 2011 r. eksploity wykorzystujące tę samą lukę związaną z wyświetlaniem czcionki pojawiły się w różnych gotowych zestawach narzędzi sprzedawanych w przestępczym podziemiu. W ciągu roku od zastosowania eksploita w Duqu była to luka najczęściej atakowana przez przestępców w celu ukradkowego instalowania trojanów bankowych i innego złośliwego oprogramowania[35]. Nawet jeśli prywatni hakerzy nie zdołają w całości odwzorować zaawansowanego ataku rządowego, mogą czegoś się z niego nauczyć i odnieść korzyści. Dowodzi tego odkrycie Microsoftu, że przestępcy potrzebowaliby tylko trzech dni, aby zastosować prostszą odmianę używanego przez Flame'a przejęcia mechanizmu Windows Update.

---

[34] David E. Sanger, *America's Deadly Dynamics with Iran*, „New York Times", 5 listopada 2011.

[35] Duqu został upubliczniony we wrześniu 2011 r., ale choć Microsoft załatał lukę związaną z wyświetlaniem czcionki, do końca 2012 r. „liczba ataków przeciw tej luce znacznie wzrosła" — napisała fińska firma z branży zabezpieczeń, F-Secure, w dorocznym raporcie z 2013 r. Ta jedna luka „odpowiadała za zdumiewające 69% wszystkich raportów o wykryciu eksploitów". Zob. s. 36 w: „Threat Report H1 2013", F-Secure (*https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2013.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Brad Arkin, dyrektor ds. bezpieczeństwa produktu i prywatności w firmie Adobe, powiedział, że obecnie najbardziej obawia się nie przestępców, ale zaawansowanych, sponsorowanych przez państwo hakerów, dysponujących dużymi pieniędzmi i walizką pełną eksploitów typu zero-day atakujących oprogramowanie firmy. „W ciągu ostatnich 18 miesięcy jedyne [luki typu zero-day] znalezione w naszym oprogramowaniu zostały wykryte przez […] przeciwników »klasy lotniskowca« — powiedział w trakcie konferencji w 2011 r. — Są to grupy posiadające wystarczająco dużo pieniędzy, aby zbudować lotniskowiec. To właśnie oni są naszymi przeciwnikami"[36]. Eksploity atakujące oprogramowanie firmy Adobe są „bardzo, bardzo kosztowne i trudne do zbudowania" — dodał Arkin. Gdy już zostaną zaprojektowane i zastosowane przez hakerów rządowych, przenikają do narzędzi cyberprzestępców.

Naczelny cyberżołnierz kraju, gen. Alexander z NSA, potwierdził ten trend w wystąpieniu przed komisją senacką z 2013 r. „Uważamy, że tylko kwestią czasu jest, aż zaawansowane narzędzia rozwijane przez posiadające duże fundusze jednostki państwowe trafią do grup lub nawet jednostek, którym będzie bardzo zależeć na zaprezentowaniu swoich poglądów politycznych, ale nie będą rozumiały lub uwzględniały przypadkowych szkód, jakie mogą wyrządzić postronnym osobom i infrastrukturze krytycznej" — powiedział[37]. Alexander miał na myśli odpowiednio finansowane narzędzia, które kraje takie jak Chiny tworzą na potrzeby ataków na Stany Zjednoczone. Nikt z komisji nie zapytał go jednak o wkład jego własnej agencji w powiększanie puli narzędzi i technik, z jakich mogą korzystać przestępcy i haktywiści. Nikt nie zapytał też o aspekty etyczne i o konsekwencje tworzenia zasobów eksploitów typu zero-day oraz ukrywania informacji o lukach w zabezpieczeniach przed właścicielami amerykańskich systemów, aby rząd mógł wykorzystać te luki do ataków na systemy wroga.

[36] Dennis Fisher, „Nation-State Attackers Are Adobe's Biggest Worry", ThreatPost, blog poświęcony bezpieczeństwu publikowany przez firmę Kaspersky Lab, 20 września 2011 (*https://threatpost.com/nation-state-attackers-are-adobes-biggest-worry-092011/75673/*).

[37] Wystąpienie przed Senacką Komisją Budżetową, „Cybersecurity: Preparing for and Responding to the Enduring Threat", 12 czerwca 2013 (*https://www.gpo.gov/fdsys/pkg/CHRG-113shrg81526/pdf/CHRG-113shrg81526.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Michael Hayden zauważył, że od zawsze konieczny był strategiczny kompromis między rozwijaniem zdolności ofensywnych a wzmacnianiem zabezpieczeń. Jedna z podstawowych koncepcji stosowanych przez rząd w związku z kompromisami w świecie broni kinetycznej (znajdująca zastosowanie także w cyberprzestrzeni) nosi nazwę NOBUS (ang. *Nobody But Us*, czyli „tylko my").

„Tylko my o tym wiemy i tylko my możemy to wykorzystać — powiedział mi Hayden. — Na ile unikatowa w porównaniu z innymi jest nasza wiedza w tym obszarze i umiejętności jej wykorzystania? […] Tak, może to być słaby punkt, jeżeli musisz posiadać półtora akra [superkomputerów] Cray, aby go wykorzystać […]". Stwierdził, że jeśli była to sytuacja typu NOBUS, urzędnicy mogli „zignorować problem" i przez pewien czas wykorzystywać lukę, dobrze przy tym wiedząc, że „im dłużej to trwa, tym więcej osób będzie mogło ją zaatakować"[38].

Hayden uznał jednak, że jeśli wziąć pod uwagę obecny stan zabezpieczeń komputerowych i zakres szkód powodowanych przez cyberataki w Stanach Zjednoczonych, jest gotów przyznać, że może przyszła pora na ponowne przemyślenie całego procesu.

„Jeśli zwyczaje powstałe w czasach analogowych, przed erą cyfrową […] są nawykami agencji kulturowo zorientowanej nieco zbyt mocno na ofensywę w świecie, w którym wszyscy są podatni na atak — powiedział — rząd może zechcieć ponownie ocenić swoje podejście".

W raporcie wydanym przez radę ds. reformy metod inwigilacji utworzoną przez Biały Dom w wyniku danych ujawnionych przez Edwarda Snowdena bezpośrednio poruszono tę kwestię i zalecono, aby Rada Bezpieczeństwa Narodowego opracowała proces oceny wykorzystywania eksploitów typu zero-day przez rząd. „Ogólnie polityka Stanów Zjednoczonych powinna podążać w kierunku zapewniania szybkiego blokowania luk typu zero-day, tak aby te luki były eliminowane w sieciach rządu amerykańskiego i innych" — napisano w raporcie. Jego autorzy zwrócili też uwagę na to, że tylko „w rzadkich sytuacjach polityka Stanów Zjednoczonych może na krótki czas upoważniać do wykorzystywania luk typu zero-day do pozyskiwania informacji nadrzędnej wagi. Powinno to się odbywać po

[38] Wszystkie słowa Haydena z tej i następnej strony pochodzą z wywiadu przeprowadzonego przez autorkę w lutym 2014 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

międzyagencyjnej ocenie z udziałem wszystkich zainteresowanych departamentów"[39]. Napisali również, że w prawie wszystkich sytuacjach „w narodowym interesie leży eliminowanie luk w oprogramowaniu, a nie wykorzystywanie ich do zbierania danych przez amerykański wywiad". Rada zarekomendowała też, aby cyberoperacje prowadzone przez Cyberdowództwo Stanów Zjednoczonych i NSA były oceniane przez Kongres w taki sam sposób, jak dzieje się to z utajnionymi operacjami CIA. Zapewni to większą jawność i lepszy nadzór nad takimi akcjami.

Richard Clarke, były główny doradca ds. cyberbezpieczeństwa z czasów administracji Busha i członek wspomnianej rady, później uzasadniał zwrócenie w raporcie uwagi na wykorzystanie luk typu zero-day. „Jeśli rząd Stanów Zjednoczonych odkryje lukę typu zero-day, jego podstawowym obowiązkiem jest poinformowanie o tym Amerykanów, aby mogli załatać system, a nie zabieranie się za [wykorzystywanie jej do] włamywania się do pekińskiego systemu telefonicznego — oświadczył na poświęconej bezpieczeństwu konferencji. — Podstawowym obowiązkiem rządu jest obrona"[40].

W przemówieniu dotyczącym raportu rady prezydent Obama zignorował oba zalecenia (dotyczące postępowania z lukami typu zero-day i nadzoru). Jednak w marcu 2014 r. w trakcie przesłuchania zatwierdzającego wiceadm. Michaela Rogersa, który zastępował na stanowisku szefa NSA i Cyberdowództwa Stanów Zjednoczonych odchodzącego na emeryturę gen. Alexandra, Rogers poinformował komisję senacką, że agencja NSA posiada już dojrzały proces oceny zasobów. Uwzględnia on zarządzanie lukami typu zero-day wykrytymi w produktach i systemach komercyjnych. Powiedział też, że agencja współpracuje z Białym Domem, aby opracować nowy międzyagencyjny proces zarządzania takimi lukami. Stwierdził, że zgodnie z polityką NSA każda luka jest dokładnie dokumentowana. Pozwala to ocenić możliwości zaradzenia jej oraz przedstawić propozycje co do jej

[39] The President's Review Group on Intelligence and Communications Technologies, „Liberty and Security in a Changing World", raport z 12 grudnia 2013, s. 37 (*https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf*).

[40] Clarke przemawiał na konferencji RSA Security w San Francisco w lutym 2014 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

ujawnienia[41]. Dodał, że w zarządzaniu lukami typu zero-day „trzeba położyć większy nacisk na łagodzenie poważnych zagrożeń stojących przed sieciami Stanów Zjednoczonych i sojuszników tego kraju". Stwierdził również, że w sytuacjach, gdy NSA decyduje się wykorzystać lukę, zamiast ją ujawniać, stara się znaleźć inne sposoby na ograniczenie ryzyka w amerykańskich systemach, współpracując z Departamentem Bezpieczeństwa Wewnętrznego i innymi agencjami.

Miesiąc później serwisy informacyjne doniosły, że prezydent Obama po cichu ogłosił nową strategię rządu w kwestii luk typu zero-day. Było to spowodowane rewelacjami ujawnionymi przez Snowdena i raportem rady doradczej[42]. Zgodnie z nową polityką NSA po wykryciu poważnego problemu w oprogramowaniu musiała ujawnić lukę producentowi i innym jednostkom, aby umożliwić wyeliminowanie błędu. Dokument zdecydowanie nie był jednak zgodny z zaleceniami rady i sam zawierał luki[43]. Dotyczył wyłącznie problemów wykrytych przez NSA — nie wspominano w nim o lukach znalezionych przez firmy pracujące na zlecenie rządu. Ponadto każda luka o „oczywistym zastosowaniu w zakresie bezpieczeństwa narodowego i dla organów ścigania" mogła zostać zachowana przez rząd w ukryciu i wykorzystana. Rada stwierdziła, że eksploity powinny być używane tylko tymczasowo i tylko „do pozyskiwania informacji nadrzędnej wagi", po czym lukę należy ujawnić. Natomiast strategia Obamy dawała rządowi swobodę nieujawniania dowolnej liczby krytycznych luk tak długo, jak długo możliwe będzie uzasadnienie ich wykorzystywania. Ponadto w strategii nie wspominano o tym, co rząd zamierza zrobić z lukami i eksploitami typu zero-day, które już znajdują się w należącym do państwa arsenale cyfrowej broni.

---

[41] „Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command". Tekst jest dostępny w witrynie Senackiej Komisji ds. Sił Zbrojnych (*https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf*).

[42] David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, „New York Times", 12 kwietnia 2014.

[43] Kim Zetter, „Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA", *Wired.com*, 15 kwietnia 2014.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

RADA NIE PORUSZYŁA jednak pewnej istotnej kwestii. Były nią skutki naruszenia zaufania do certyfikatów cyfrowych i systemu Windows Update, co stało się w wyniku realizowania ofensywnych celów przez robaki Stuxnet i Flame.

Christopher Soghoian z ACLU porównał przejęcie systemu Windows Update do opanowania przez CIA systemu szczepień w celu zabicia Osamy bin Ladena. Agencja podobno zrekrutowała w Pakistanie lekarza, aby dostarczał szczepionki mieszkańcom określonej okolicy. Dzięki temu mógł ukradkowo zbierać próbki DNA od osób żyjących na ogrodzonym terenie, gdzie — jak podejrzewano — mieszkał bin Laden.

W analogiczny sposób przejęcie systemu Windows Update i podobne ataki szkodzą zaufanym systemom i mogą doprowadzić do kryzysu wiarygodności. Może to skutkować tym, że użytkownicy przestaną korzystać z systemów, które mają ich chronić.

„Automatyczne aktualizacje bezpieczeństwa są dobre. Zapewniają nam ochronę. Dzięki nim wszyscy są bezpieczni — powiedział Soghoian uczestnikom konferencji odbywającej się po wykryciu Flame'a[44]. — Jakiekolwiek krótkotrwałe zyski z przejęcia mechanizmu Windows Update nie są warte wykorzystywania go".

Hayden uważa, że czasem zaszkodzenie zaufanym systemom *jest* tego warte. Mówi, że podjąłby tę samą decyzję co dyrektor CIA Leon Panetta, aby wykorzystać system szczepień do zlokalizowania bin Ladena. „Chcę powiedzieć, że [podejmowanie decyzji] miało miejsce cały czas" — dodaje. Jednocześnie przyznaje, że „[niekiedy] zdarzają nam się błędy"[45].

Jeśli, jak wynika z raportów, to Stany Zjednoczone odpowiadały za przejęcie systemu Windows Update przez Flame'a, pojawiają się pytania, czy takie akcje powinny wymagać powiadomienia Microsoftu i uzyskania zgody od tej firmy. Amerykańskie agencje wywiadowcze nie mogą podejmować działań narażających firmy w Stanach na ryzyko, chyba że wysoko postawione osoby autoryzują taką akcję i firma wyrazi na nią zgodę. Nie mogą np. zrobić z IBM-u nieświadomego wspólnika CIA, nakazując agentowi podszywać się za pracownika tej firmy, jeśli nie poinformują o tych

[44] Soghoian przemawiał w Nowym Jorku na konferencji Personal Democracy Forum w czerwcu 2012 r.

[45] Z wywiadu przeprowadzonego przez autorkę w 2014 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

działaniach osoby pełniącej obowiązki powiernicze. „CIA *może* to zrobić — mówi Catherine Lotrionte, profesor prawa na Georgetown University i była prawniczka w Biurze Głównego Radcy Prawnego CIA — ale musi powiadomić CEO, ponieważ pełni on obowiązki powiernicze wobec rady nadzorczej firmy”[46].

Jeśli użycie cyfrowo podpisanego certyfikatu Microsoftu zostało uznane za „operacyjne wykorzystanie” amerykańskiej firmy — ponieważ obejmowało posłużenie się prawidłowymi danymi Microsoftu do przesyłania szkodliwego pliku jako poprawnego pliku tej firmy — możliwe, że Microsoft należało o tym poinformować. „Zależy to od tego, co zostanie uznane za operacyjne wykorzystanie w świecie technicznym — powiedziała Lotrionte. — Wiemy, jak wygląda to w przypadku ludzi, [ale] w branży technicznej nie jest to takie proste”.

Gdy ta operacja została po raz pierwszy ujawniona, niektórzy badacze zastanawiali się, czy przedstawiciele Microsoftu wiedzieli wcześniej o ataku na mechanizm Windows Update. Inni zauważyli, że gdyby Microsoft zaaprobował taką operację, napastnicy nie musieliby uciekać się do stosowania kolizji skrótów MD5 w celu uzyskania certyfikatu — chyba że miało to pozwolić Microsoftowi na wyparcie się współudziału w akcji.

„Pytanie brzmi: czy Microsoft pozwoliłby na coś takiego? — zastanawia się Lotrionte. — To byłoby dla mnie niepokojące. Wywiad jest gotów stosować wszelkie rozwiązania. Często zastanawiam się jednak, dlaczego firmy narażają się na ryzyko. Wydaje mi się, że jeśli było to operacyjne wykorzystanie i Microsoft o tym wiedział, jest to ciekawa sprawa”.

Dobrze poinformowane źródła donoszą, że Microsoft nie wiedział o operacji i nie wydał na nią zezwolenia. „Gdyby Microsoft się na to zgodził, byłby to koniec firmy — powiedział jeden z informatorów. — Jest to ryzyko, jakiego nikt [w firmie] nie podejmie”. Informator nazwał przejęcie przez jednostki rządowe procesu certyfikacji Microsoftu nieodpowiedzialnym i więcej niż szokującym.

[46] Lotrionte pracowała dla CIA do 2002 r., po czym została konsultantem w prezydenckiej radzie ds. wywiadu zagranicznego przy Białym Domu i radcą prawnym senackiej komisji specjalnej ds. wywiadu. Odeszła ze stanowisk rządowych w 2006 r., mniej więcej w czasie, gdy zaproponowano użycie Stuxneta i rozpoczęto nad nim prace.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„Pływaliśmy po bardzo niebezpiecznych wodach — powiedział. — Ludzie robiący tego typu rzeczy przysporzą sektorowi prywatnemu problemów, których ci ostatni pewnie nawet sobie nie wyobrażali".

Przejęcie zaufanego systemu Microsoftu nie tylko podważyło relację tej firmy z jej klientami. Było też sprzeczne z deklarowanym przez rząd zaangażowaniem w poprawę bezpieczeństwa informatycznego w Stanach Zjednoczonych.

W 2011 r. Biały Dom opublikował Międzynarodową strategię dla cyberprzestrzeni — kompleksowy dokument opisujący wizję internetu według prezydenta. W dokumencie podkreślono odpowiedzialność rządu za zwiększanie bezpieczeństwa i odporności systemów. Drogą do tego celu miało być m.in. opracowanie norm odpowiedzialnego postępowania i zbudowanie mechanizmów wymiany informacji o lukach między sektorami publicznym i prywatnym w celu ochrony systemów. Jednak zdaniem Jasona Healeya działania rządu sprawiają, że jego uczciwość staje się wątpliwa.

„Jeśli opracowujesz politykę, która prowadzi do przejmowania certyfikatów Microsoftu i mechanizmu Windows Update w celu rozprzestrzeniania złośliwego oprogramowania, trudno doprowadzić do zwiększenia bezpieczeństwa i odporności cyberprzestrzeni — powiedział Healey. — Mam wrażenie, że pod pewnymi względami ludzie z Fortu Meade są jak izraelscy osadnicy w cyberprzestrzeni. Nie ma znaczenia, jak brzmią oficjalne reguły — osadnicy mogą zająć wzgórza i postawić wszystkich przed faktem dokonanym. […] Jeśli kiedykolwiek mamy mieć lepsze zabezpieczenia niż możliwości ofensywne, pewne rzeczy powinny być nienaruszalne. [Ale] jeśli przyjmujemy za normę, że można przeprowadzać takie operacje, jeśli powodujemy kryzys zaufania […] zwróci się to przeciwko nam".

Healey uważa, że „kawaleryjskie" podejście do operacji ofensywnych, naruszające bezpieczeństwo i zaufanie do systemów krytycznych, grozi ulicznymi potyczkami i walkami partyzanckimi na cyfrowej autostradzie. „Możemy sobie wyobrazić, że ataki będą nie tylko lepsze, ale zdecydowanie skuteczniejsze. Cyberprzestrzeń stanie się nie tyle Dzikim Zachodem, ile Somalią".

Nie wszyscy zgadzają się z Healeyem i Soghoianem co do tego, że niektóre systemy powinny być nietykalne. Istnieją pewne analogie w rzeczywistym świecie. CIA wykorzystuje np. słabe punkty zamków, sejfów i systemów

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

bezpieczeństwa w budynkach, aby zdobyć dostęp do informacji. Nikt nigdy nie sugerował, że powinna informować o tych słabych punktach producentów, by wyeliminowali wady.

Jednak bez prawodawców lub niezależnych jednostek zadających odpowiednie pytania, służące ochronie długoterminowo ocenianego bezpieczeństwa i zaufania w internecie, dyskusje na temat ofensywnych operacji państwa będą przebiegały tylko między ludźmi z wewnątrz, w których interesie leży zwiększanie możliwości ofensywnych, a nie ich ograniczanie, i stałe przesuwanie granic tego, co jest możliwe. „[Decyzje podejmują] sami ludzie z najwyższymi uprawnieniami. Prawdopodobnie niewielu [z nich] przepracowało choćby dzień w sektorze prywatnym, gdzie naprawdę musieliby chronić amerykańską infrastrukturę krytyczną — powiedział Healey. — Dlatego takim ludziom bardzo łatwo jest podejmować decyzje o tym, by iść dalej i dalej […] ponieważ to rządowi przypadną wszystkie korzyści. Jeśli wykorzystujemy lukę typu zero-day we Flamie, rząd odnosi z tego korzyść. Ale to sektor prywatny będzie się zmagał z kontratakami i ucierpi z powodu norm, jakie tworzą obecnie Stany Zjednoczone, twierdząc, że akcje ofensywne są dozwolone".

Jeśli Biały Dom i Kapitol nie przejmują się tym, że działania rządu podkopują bezpieczeństwo systemów komputerowych, mogą zmartwić się innymi konsekwencjami ofensywnych działań państwa. Stephen Cobb, starszy badacz w ESET, firmie z branży zabezpieczeń, stwierdził: „Gdy nasz rząd nasila zagrożenie złośliwym oprogramowaniem, narusza przez to zaufanie, co szkodzi cyfrowej ekonomii"[47].

PONIEWAŻ RZĄDOWE CYBEROPERACJE są wysoce poufne, nie jest jasne, jakiego rodzaju nadzór (ze strony wojska lub prawodawców) jest obecnie sprawowany, aby zapobiegać problemom, lub jakiego rodzaju śledztwa (jeśli w ogóle) są przeprowadzane po wystąpieniu wypadków.

Hayden twierdzi, że sprawowany jest kompleksowy nadzór. „Gdy pracowałem dla rządu, cyberbroń była tak bacznie kontrolowana, że uważałem, iż będzie cudem, jeśli kiedykolwiek ją zastosujemy. […] Była to przeszkoda

[47] Stephen Cobb, „The Negative Impact on GDP of State-Sponsored Malware Like Stuxnet and Flame", blog We Live Security, 13 czerwca 2012 (*https://www.welivesecurity.com/2012/06/13/impact-on-gdp-of-state-sponsored-malware-like-stuxnet-and-flame/*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

do właściwego zastosowania nowej klasy broni, dlatego tak trudno było znaleźć wspólny punkt widzenia".

Jednak w 2009 r., na długo po zastosowaniu Stuxneta przeciw Iranowi, Narodowa Akademia Nauk Stanów Zjednoczonych stwierdziła, że „polityka i ramy prawne w obszarze wytycznych i regulacji zdolności Stanów Zjednoczonych do cyberataków są źle skonstruowane, niepełne i wysoce niepewne"[48]. Mimo dekady planowania i prowadzenia ofensywnych cyberoperacji (pierwszą jednostkę specjalną powołano w 1998 r.) rozwiązano niewiele problemów dotyczących reguł angażowania się w działania cyfrowe.

W 2011 r., ponad trzy lata od wypuszczenia Stuxneta, Pentagon i Biały Dom wreszcie podjęły kroki, aby zaradzić tej sytuacji. Stało się to, gdy Departament Obrony stworzył podobno poufną listę wszystkich dostępnych mu cyberbroni i narzędzi oraz zaczął opracowywać dalece spóźnione reguły opisujące, jak i kiedy można z nich korzystać[49]. „Wojsko regularnie tworzy listy akceptowanych broni konwencjonalnych, jednak tym razem po raz pierwszy sporządzono wykaz cyberbroni" — powiedział gazecie „Washington Post" wysoko postawiony oficjel z armii, nazywając to najważniejszym od lat krokiem w dziedzinie doktryny cyberwojskowej.

Następnie w 2012 r. prezydent podpisał tajną dyrektywę określającą reguły ataków na sieci komputerowe. Szczegóły tego dokumentu znamy tylko dzięki ujawnieniu go przez Edwarda Snowdena[50]. Zgodnie z dyrektywą stosowanie cyberbroni bez wypowiedzenia wojny wymaga zgody prezydenta. Jednak w trakcie działań wojennych dowódcy wojskowi mogą podejmować szybkie działania wedle swojego uznania. Cyfrowe ataki muszą być proporcjonalne do zagrożenia. Należy też unikać przypadkowych zniszczeń i ofiar wśród cywili. Te wytyczne nadal pozostawiają wojsku dużo swobody[51].

---

[48] William A. Owens, Kenneth W. Dam, Herbert S. Lin (red.), *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, National Academies Press, 2009 (*http://www.steptoe.com/assets/attachments/3785.pdf*).

[49] Ellen Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, „Washington Post", 31 maja 2011.

[50] Lolita Baldor, „Pentagon Gets Cyberwar Guidelines", Associated Press, 22 czerwca 2011 (*http://usatoday30.usatoday.com/news/military/2011-06-22-pentagon-cyber-war_n.htm*).

[51] Glenn Greenwald, Ewen MacAskill, *Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks*, „Guardian", 7 czerwca 2013. Według gazety dokument *Presidential Policy Directive 20* został wydany w październiku 2012 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Zgody prezydenta wymaga też każda cyfrowa operacja, która może obejmować zaburzenie pracy komputerów, zniszczenie ich lub manipulowanie nimi albo „ze sporym prawdopodobieństwem spowodować poważne konsekwencje". Poważne konsekwencje obejmują: utratę życia, uszkodzenie mienia, istotne skutki ekonomiczne, a także możliwy odwet na Stanach Zjednoczonych lub negatywny wpływ na politykę zagraniczną.

Zgoda prezydenta jest potrzebna także do umieszczenia w obcym systemie bomby logicznej lub nadajnika naprowadzającego na cel w późniejszym ataku. Nie jest jednak wymagana do operacji szpiegowskich przeprowadzanych w celu zbierania informacji lub tworzenia map sieci, chyba że akcja obejmuje robaka lub inne złośliwe oprogramowanie, które może się rozprzestrzeniać. Przed podjęciem działań wojsko musi ocenić możliwy wpływ operacji na stabilność i bezpieczeństwo internetu, a także określić, czy działania nie spowodują ustanowienia niepożądanych norm postępowania na arenie międzynarodowej. Choć zdaniem niektórych specjalistów Stuxnet i Flame naruszyły te wytyczne i ustanowiły niepożądane normy, Herbert Lin, ekspert od cyberbezpieczeństwa w Narodowej Radzie Naukowej, podkreśla, że dyrektywa stwierdza tylko, iż dowódcy wojskowi muszą zadać pytanie o to, czy operacja może prowadzić do powstawania takich norm, natomiast nie muszą uwzględniać tego w trakcie podejmowania decyzji. „Stworzenie niepożądanej normy mogło być ceną, jaką byli gotowi zapłacić za cofnięcie irańskiego programu nuklearnego" — powiedział Lin o Stuxnecie i Flamie[52].

Jednak prezydencka dyrektywa nr 20 dotyczy tylko *militarnych* operacji cyfrowych. Lista wyjątków w dokumencie obejmuje agencje wywiadowcze takie jak NSA i CIA, a także organy ścigania, np. FBI i Secret Service. Ponadto choć dyrektywa ustanawia ogólne reguły prowadzenia ofensywnych cyberoperacji przez wojsko, nie uwzględnia pytań związanych z reakcją Stanów Zjednoczonych na atak cyfrowy. W 2011 r. przedstawiciele Pentagonu zrobili przynajmniej jeden krok w tym kierunku, stwierdzając, że każdy cyfrowy atak na Stany Zjednoczone, który spowoduje wyłączenie fragmentów sieci elektrycznej lub doprowadzi do ofiar, zostanie uznany za wypowiedzenie wojny i spotka się z odpowiednią reakcją, w tym — jeśli sytuacja będzie tego wymagać — kinetycznym atakiem wojskowym z użyciem

[52] Wszystkie słowa Lina w tym rozdziale pochodzą z wywiadu przeprowadzonego przez autorkę w styczniu 2014 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

„wszystkich niezbędnych środków”[53]. Jeden z wojskowych ujął to tak: „Jeśli wyłączycie naszą sieć zasilania, możliwe, że wystrzelimy pociski w jedną z waszych fabryk”[54]. W omawianej dyrektywie przynajmniej nie zapisano, jak zrobiło to Kolegium Połączonych Szefów Sztabów w doktrynie z 2004 r., że Stany Zjednoczone rezerwują sobie prawo do użycia broni atomowej w reakcji na niektóre cyberataki. Lin zauważył, że ten punkt zniknął z późniejszych doktryn kolegium, jednak rada naukowa Departamentu Obrony najwyraźniej chciała go przywrócić, gdy w 2013 r. stwierdziła, że Stany Zjednoczone nie powinny wykluczać reakcji z użyciem broni atomowej. Chyba dobrze, że to ciało jest tylko jednostką doradczą i nie ma wpływu na stanowienie prawa.

Choć prezydencka dyrektywa ujawniona przez Snowdena wskazywała na to, jakie pytania rząd zadawał sobie w związku z omawianymi sprawami, opinia publiczna w niewielkim stopniu wie, na które pytania administracja znalazła już odpowiedzi, a które kwestie nadal pozostają nierozwiązane. Lin uważa, że dla przejrzystości niektóre ważne dyskusje warto upublicznić, nie narażając przy tym tajnych operacji na szwank. „Moglibyśmy zacząć debatę o tym, co jest możliwe, nie rozmawiając na temat tego, co Stany Zjednoczone rzeczywiście robią” — mówi. Cyberdowództwo Stanów Zjednoczonych i NSA mogłyby też przedstawić przykładowe scenariusze stosowania cyberbroni lub wyjaśnić, w jakich warunkach zatrzymują informacje o lukach typu zero-day dla siebie, a w jakich je ujawniają, aby umożliwić rozwiązanie problemu. Ważne jest też, by wiedzieć przynajmniej to, gdzie rząd stawia granicę (jeśli w ogóle ją stawia), gdy decyduje się na atak na zaufane systemy krytyczne dla funkcjonowania internetu.

„Senatorzy i kongresmeni muszą się o tym dowiedzieć — mówi Lin — nie wspominając nawet o opinii publicznej. Potrzebne są też raporty na temat wszystkich ataków przeprowadzanych przez Stany Zjednoczone w różnych celach […] informujące, co zostało zaatakowane i w jakich okolicznościach. […] Te dane mogą być tajne, ale przynajmniej będą stanowiły

[53] „International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”, Biały Dom, maj 2011 (*https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*).

[54] Siobhan Gorman, Julian E. Barnes, *Cyber Combat: Act of War*, „Wall Street Journal”, 30 maja 2011.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

pierwszy krok w kierunku lepszego zrozumienia tego, co Stany Zjednoczone rzeczywiście robią". Prawodawcy tacy jak Mike Rogers (kongresmen ze stanu Michigan) twierdzą, że Kongres *prowadził* prywatne rozmowy na temat cyberdziałalności rządu. Jednak dotychczas Kapitol wykazywał niewielkie zainteresowanie choćby ograniczonymi *publicznymi* debatami dotyczącymi ofensywnych operacji rządowych.

„Jestem w pełni przekonany, że konieczne są szczegółowe rozmowy na temat doktryny i zasad zaangażowania — powiedział w 2011 r. generał Sił Powietrznych Robert Kehler, obecny szef Dowództwa Strategicznego Stanów Zjednoczonych, przed podpisaniem dyrektywy prezydenckiej nr 20. — Nie twierdzę jednak, że o tym wszystkim należy mówić publicznie"[55].

GDY STANY ZJEDNOCZONE i inne państwa szykują się do cyberwojny, bez odpowiedzi pozostają nie tylko zagadnienia polityczne. Także liczne kwestie prawne są nadal nierozwiązane.

Niektórzy eksperci, np. Eugene Kaspersky, założyciel firmy Kaspersky Lab, nawołują do podpisywania traktatów dotyczących cyfrowych zbrojeń. Takie dokumenty mają pozwolić na kontrolę rozprzestrzeniania broni cyfrowej i ustanowić normy jej stosowania. Niestety, z próbą kontrolowania zasobów broni niefizycznej związane są oczywiste problemy. Rządy mogą podpisywać traktaty o nierozprzestrzenianiu broni atomowej oraz dzięki zdjęciom satelitarnym i inspektorom ONZ-etu śledzić przemieszczanie się materiałów nuklearnych. Lecz satelity nie wyśledzą drogi nielegalnej broni cyfrowej, a wyrywkowe kontrole nie pozwolą wykryć przemytu szkodliwego kodu przez granice. Nikt nie zdoła też obserwować wszystkich niebezpiecznych podmiotów, które mogą chcieć wykorzystać luki w systemach infrastruktury krytycznej ujawnione przez Stuxneta.

Jeśli chodzi o tworzenie nowych praw dotyczących dokonywania cyberataków przez państwa, specjaliści od prawa są zgodni, że obecne zasady prowadzenia działań wojennych sprawdzą się wystarczająco dobrze. Trzeba tylko zinterpretować je w nowy sposób, aby uwzględnić broń cyfrową.

W 2013 r. spróbował się z tym zmierzyć zespół 20 międzynarodowych ekspertów z dziedziny prawa międzynarodowego powołany przez instytut powiązany z NATO. W efekcie powstał 300-stronicowy dokument *Tallinn*

[55] Carroll, „Cone of Silence".

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Manual, który ma pomóc doradcom prawnym wojska w krajach członkowskich NATO w opracowaniu cyberdoktryn dla armii tych państw[56]. Wprawdzie dokument jest obszerny, mimo to wiele pytań pozostawia bez odpowiedzi. Eksperci stwierdzili, że choć niektóre ataki w cyberprzestrzeni są analogiczne do konwencjonalnych ataków w przestrzeni fizycznej, inne są bardziej skomplikowane.

Na przykład zgodnie z prawem dotyczącym konfliktów zbrojnych opisanym w Karcie Narodów Zjednoczonych zespół uznał, że włamanie do systemu kontroli tamy w celu spuszczenia wody w dolinę jest równoważne z wysadzeniem tamy za pomocą materiałów wybuchowych. Przeprowadzenie ataku za pomocą systemu pośredniczącego z kraju neutralnego jest zabronione, podobnie jak armia nie może przemaszerować przez terytorium neutralnego państwa w celu przeprowadzenia inwazji na wroga. Zespół stwierdził też, że atak musi powodować fizyczne lub osobowe szkody, aby został uznany za akt przemocy. Samo skasowanie danych z dysków twardych, jeśli nie doprowadziło do fizycznych uszkodzeń lub urazów, nie wystarczy. Co jednak z atakiem na Wall Street, który zaszkodzi ekonomii państwa lub zostanie przeprowadzony w tym celu? Tu sytuacja jest mniej jasna. Niektórzy eksperci uważali, że jest to akt przemocy, natomiast inni nie byli co do tego przekonani.

Eksperci wprowadzili też rozróżnienie między aktem przemocy (ang. *act of force*) a napaścią zbrojną (ang. *armed attack*). Choć ten ostatni można uznać za poważniejszy, nie jest to jednoznacznie zdefiniowane. Ogólnie za napaść zbrojną uznaje się tylko najpoważniejsze przypadki użycia siły, co jest oceniane na podstawie skutków operacji. Według art. 24 Karty Narodów Zjednoczonych państwa mogą odpowiadać na akty przemocy tylko z użyciem środków dyplomatycznych. Mogą np. złożyć wniosek o nałożenie sankcji ekonomicznych lub zerwać stosunki dyplomatyczne z agresorem.

Jednak według art. 51 każdy kraj ma prawo bronić się z użyciem dowolnej siły — samodzielnie lub wraz z sojusznikami — jeśli on sam lub sojusznik padnie ofiarą napaści zbrojnej. Reakcja musi być przy tym konieczna i proporcjonalna do pierwotnego ataku, a także wystąpić w czasie, gdy wciąż istnieje zagrożenie związane z pierwotnym atakiem lub dalszymi

[56] Michael N. Schmitt, red. naczelny, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence (*https://ccdcoe.org/cyberwarfare/249.html*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

działaniami wroga. Jeśli chodzi o *poziom* szkód kwalifikujący się do uznania operacji za napaść zbrojną (i usprawiedliwiający odpowiedź z użyciem dowolnej siły), to ofiara ustala go i broni swojej decyzji przed ONZ-em[57]. Co jednak z atakami, które miały wyrządzić poważne szkody, ale zakończyły się niepowodzeniem? Rakieta wystrzelona przez jedno państwo w drugie i przechwycona przez pocisk Patriot to nadal próba napaści zbrojnej. Czy tak samo jest w cyberprzestrzeni? Catherine Lotrionte sądzi, że nie, ponieważ ważne są skutki ataku, a nie zamiary. Jednak Gary Browne, starszy doradca prawny Cyberdowództwa Stanów Zjednoczonych w latach 2010 – 2012, uważa, że taką sytuację *można* uznać za napaść zbrojną, „jeśli możliwe jest uargumentowanie [za pomocą dowodów], że celem operacji było spowodowanie skutków kinetycznych"[58].

[57] Wiele osób z mediów i rządu nazwało ataki DoS na estońskie witryny cyberwojną, jednak nie kwalifikują się one do tej kategorii. Ta operacja, przeprowadzona w 2007 r. za pomocą botnetu obejmującego 85 tys. maszyn, trwała trzy tygodnie i w szczytowym okresie objęła atakiem prawie 50 witryn. Spowodowała zablokowanie witryny największego estońskiego banku, a także serwisów rządowych. Jednak gdy Estonia oskarżyła o atak Rosję i wystąpiła o pomoc ze strony NATO, powołując się na porozumienie o obronie kolektywnej na mocy art. 5 NATO, jej prośba została odrzucona. NATO uznało, że według porozumienia operacja nie stanowiła napaści zbrojnej. Problem polegał na tym, że Unia Europejska i NATO nie zdefiniowały wcześniej zobowiązań państw członkowskich w sytuacji przeprowadzenia cyberataku na jedno z nich. Ponadto NATO nie definiowało cyberataku jako operacji jednoznacznie militarnej, dlatego art. 5 nie znajdował tu automatycznie zastosowania. Zgodnie z tym artykułem „napaść zbrojną wymierzoną w jednego [członka] lub więcej [członków] w Europie lub Ameryce Północnej należy uznać za atak przeciw wszystkim krajom". W reakcji na taki atak od każdego członka oczekuje się „wsparcia Strony lub Stron zaatakowanych w ten sposób i niezwłocznego podjęcia działań uznanych za konieczne, włączając w to użycie sił zbrojnych, w celu przywrócenia i zachowania bezpieczeństwa regionu północnoatlantyckiego". Estoński premier Andrus Ansip podważył jednak wnioski NATO i zadał pytanie: „Czym różni się blokada portów lub lotnisk suwerennych państw od blokady witryn instytucji rządowych i prasy?" (zob. Thomas Rid, *Think Again: Cyberwar*, „Foreign Policy", 27 lutego 2012, *http://foreignpolicy.com/2012/02/27/think-again-cyberwar/*). To dobre pytanie i nie udzielono na nie zadowalającej odpowiedzi. Skoro blokowanie komercyjnych dostaw może być aktem wojny, to czy blokowanie handlu elektronicznego jest tego odpowiednikiem w cyberprzestrzeni? Jaka odpowiedź jest uzasadniona w takiej sytuacji? W 2010 r. NATO próbowało odpowiedzieć na to pytanie i doszło do wniosku, że gdy jeden z sojuszników stanie się ofiarą cyberataku, NATO pomoże w ochronie sieci, ale nie udzieli wsparcia w zakresie kontrataku.

[58] Z wywiadu przeprowadzonego przez autorkę w lutym 2014 r.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

A co z akcjami szpiegowskimi? Według prawa międzynarodowego i polityki Stanów Zjednoczonych szpiegostwo nie jest aktem wojny. Ponieważ jednak może stanowić wprowadzenie do niszczycielskich ataków, tak jak w przypadku Stuxneta i narzędzi szpiegowskich, jakie napastnicy wykorzystywali do zbierania danych na potrzeby tej operacji, to czy wykrycie takich narzędzi w systemie wskazuje na zamiar przeprowadzenia napaści zbrojnej? Według obecnej doktryny, aby uzasadnić zastosowanie w reakcji dowolnej siły, napaść zbrojna musi trwać lub być bliska. Jak jednak ocenić bliskość napaści? Po 11 września Stany Zjednoczone stwierdziły, że inwazja na Afganistan była aktem samoobrony (według art. 51), ponieważ w tym kraju znajdowali się liderzy Al-Kaidy, podejrzewani o planowanie kolejnych uderzeń na Stany Zjednoczone.

Jedyną kwestią, w której eksperci tworzący *Tallinn Manual* byli jednogłośni, jest to, że Stuxnet stanowił akt przemocy i zapewne naruszał prawo międzynarodowe. Specjaliści byli jednak podzieleni w sprawie oceny, czy była to napaść zbrojna. Jeśli uznać to za napaść zbrojną, Iran miał prawo bronić się przed cyfrową operacją za pomocą kontrataku (cyfrowego lub kinetycznego), przy czym musiał on być proporcjonalny do szkód wyrządzonych przez Stuxneta i pojawić się w trakcie trwania operacji. Po zakończeniu operacji, gdy nie było już zagrożenia dla wirówek i ryzyka kolejnych ataków (czyli po wykryciu i zdezaktywowaniu broni), odpowiednimi reakcjami były dyplomacja i inne działania bez użycia siły.

Należy zauważyć, że oficjalna polityka Stanów Zjednoczonych, w odróżnieniu od interpretacji autorów dokumentu *Tallinn Manual*, nie rozróżnia aktów przemocy i napaści zbrojnej. Amerykanie obie te kategorie traktują tak samo. W tym podejściu Stuxnet był nielegalną napaścią zbrojną i Iran mógł odpowiedzieć samoobroną. Oznacza to też, że jeśli ktoś zastosuje broń taką jak Stuxnet przeciw Stanom Zjednoczonym, rząd amerykański może to uznać za napaść zbrojną, co — według Lotrionte — jest niepokojące[59].

[59] Harold Koh, były doradca prawny Departamentu Stanu, na konferencji US CyberCom InterAgency Legal Conference w Forcie Meade we wrześniu 2012 r. stwierdził, że według rządu użycie siły jest tym samym co napaść zbrojna. „Naszym zdaniem w zastosowaniu śmiertelnej broni nie ma progu, który pozwalałby zakwalifikować to jako »napaść zbrojną« uzasadniającą odpowiedź z użyciem siły". Zob.: *https://2009-2017.state.gov/s/l/releases/remarks/197924.htm*.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Niektóre wnioski z dokumentu *Tallinn Manual* wzbudziły sprzeczne reakcje. Martin Libicki, ekspert od cyberbroni w korporacji RAND, podważa zasadność rozwiązywania cyberkonfliktów za pomocą ataków kinetycznych. Zastanawia się, czy nie mądrzej byłoby zastosować tu „regułę Las Vegas" i przyjąć, że to, co dzieje się w cyberprzestrzeni, pozostaje w cyberprzestrzeni. „Możliwość eskalacji po przejściu do kontekstu kinetycznego jest znacznie większa niż w przypadku pozostania w cyberprzestrzeni — mówi. — Dlatego reguła głosząca, że na ataki cyfrowe można reagować tylko środkami cyfrowymi, ogranicza ryzyko"[60].

Jednak Lotrionte uważa, że metody kontrataku nie mają tu znaczenia, ponieważ eskalacja jest kontrolowana dzięki temu, że kontruderzenie musi być konieczne i proporcjonalne do ataku. „Konieczność oznacza, że trzeba stwierdzić, iż nie ma innej możliwości poradzenia sobie z zagrożeniem — argumentuje. — Że nie wystarczą rozmowy, sankcje lub zgłoszenia do Rady Bezpieczeństwa. Jeśli istnieje inny sposób na powstrzymanie ataków, trzeba zastosować go zamiast siły. W ten sposób powstrzymywana jest eskalacja"[61].

Inni zwracają uwagę na problemy ze stosowaniem tradycyjnych praw konfliktów zbrojnych do cyberprzestrzeni, gdzie trudno jest wskazać źródło ataku. Prawo konfliktów zbrojnych wymaga zidentyfikowania napastnika w celu przeprowadzenia przeciwuderzenia. Choć czasem można ustalić źródło operacji cyfrowej (jeśli nie za pomocą analiz, to dzięki akcjom wywiadu), anonimowy charakter cyberataków co najmniej utrudnia szybkie reagowanie na nie w czasie, gdy zagrożenie wciąż istnieje.

„Trudno jest znaleźć dymiące lufy w ramach zwalczania terroryzmu; wykrycie dymiących klawiatur jest dużo trudniejsze" — powiedział Kongresowi Frank Cilluffo, dyrektor Homeland Security Policy Institute przy Uniwersytecie Jerzego Waszyngtona. Dodał też, że cyberprzestrzeń „jest stworzona do wygodnego wypierania się odpowiedzialności"[62].

---

[60] Z wywiadu przeprowadzonego przez autorkę w październiku 2012 r.

[61] Wszystkie słowa Lotrionte pochodzą z wywiadu przeprowadzonego przez autorkę w lutym 2014 r.

[62] Cilluffo przemawiał podczas obrad wspólnej podkomisji w ramach komisji ds. bezpieczeństwa wewnętrznego w sprawie „Iranian Cyber Threat to the US Homeland" (*https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdyby to wszystko nie wystarczyło do skomplikowania kwestii cyberwojen, występują jeszcze problemy związane z brakiem dobrego zrozumienia, czym jest cyberbroń. W świecie kinetycznym broń to coś, co uszkadza, niszczy, zabija lub rani. Broń kinetyczna zdecydowanie różni się od narzędzi szpiegowskich. Jednak Gary Brown zauważa, że w cyberprzestrzeni wiele operacji jest wykonywanych przez „gościa siedzącego przy klawiaturze i wpisującego instrukcje", który robi wszystko: od instalowania złośliwego oprogramowania i kasowania danych, przez niszczenie systemów, po uszkadzanie sprzętu kontrolowanego przez te systemy. „Czy to oznacza, że oprogramowanie lub techniki użyte do uzyskania dostępu do systemu stają się bronią? — pyta Brown. — To obejmowałoby wszystko. Jest to bardzo skomplikowana sprawa. Myślę, że nie mamy w niej dobrego rozeznania".

Brown uważa, że brak jasności co do tego, czym jest broń cyfrowa i czym jest atak (w odróżnieniu od szpiegostwa), grozi eskalacją reakcji, ponieważ techniki i narzędzia używane do szpiegowania oraz przeprowadzania niszczycielskich ataków w cyberprzestrzeni mogą być dla ofiary nieodróżnialne[63].

„Tradycyjne szpiegostwo w mniejszym stopniu grozi eskalacją, ponieważ jest bardziej zrozumiałe — mówi. — Nawet jeśli przetniesz drut kolczasty, włamiesz się do biura i ukradniesz pliki […] nie będzie to wyglądać na początek wojny. […] Jeśli ktoś w cyberprzestrzeni uzyska dostęp do krytycznego systemu, np. serwera sterującego bronią atomową […] możliwe, że po prostu się rozgląda. Możliwe też, że planuje wyłączyć system i rozpocząć atak nuklearny. […] Tego rodzaju eskalacji się obawiam".

Najwyraźniej Stuxnet i możliwość wojny cyfrowej spowodowały powstanie wielu problemów, którym trzeba odpowiednio zaradzić. Jeśli wydaje się, że Stany Zjednoczone robią to zbyt późno, dotyczy to nie tylko tego kraju. „Są państwa [w Europie], które nawet nie zbliżyły się do opracowania reguł" — mówi Lotrionte.

[63] Brown napisał pracę na ten temat. Zob. Gary D. Brown, Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, „Journal of National Security Law and Policy", opublikowane przez Georgetown Law, 12 lutego 2014 (*http://jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf*).

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

W LATACH PO ujawnieniu Stuxneta wiele się zmieniło — nie tylko dla wojska, ale też dla łowców złośliwego oprogramowania. Dla badaczy, którzy poświęcili mnóstwo czasu na rozłożenie i analizę Stuxneta oraz powiązanych z nim narzędzi szpiegowskich, rozpracowywanie tego złośliwego oprogramowania było wielką przygodą, wykraczającą poza granice zwykłych badań nad wirusami. Jednak Stuxnet oznaczał też nieodwracalne zmiany w ich profesji, wynikające z pojawienia się nowego rodzaju zagrożeń i nieznanych wcześniej kwestii politycznych.

W jednej z ostatnich analiz Stuxneta Eric Chien z Symanteca napisał, że nie potrafi stwierdzić, czy Stuxnet zapoczątkuje nową generację ataków w świecie fizycznym wymierzonych w infrastrukturę krytyczną, czy okaże się tylko zjawiskiem występującym raz na dekadę. Badacz jednak dobrze wiedział, który z tych scenariuszy bardziej mu odpowiada. Stuxnet był zagrożeniem, z którym zespół „miał nadzieję już nigdy się nie zetknąć".

Na szczęście do czasu opublikowania tej książki nie wykryto oznak ataków na systemy kontroli procesów przemysłowych, przed czym ostrzegał Ralph Langner. Nie zauważono też podobnych ataków cyfrowych ze strony Stanów Zjednoczonych lub innych podmiotów. Stuxnet nadal ma zaszczyt być jedyną znaną cyberbronią. Lecz teraz, gdy cyfrowa puszka Pandory została już otwarta, może się to zmienić w każdej chwili.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PODZIĘKOWANIA

Gdy po raz pierwszy zaczęłam pisać o Stuxnecie po jego wykryciu latem 2010 r., nie mogłam przewidzieć, jak sytuacja się rozwinie. Dopiero po kilku miesiącach, gdy badacze z Symanteca i zespół Ralpha Langnera dokładnie zajęli się sprawą, stało się jasne, że za Stuxnetem kryje się dłuższa historia, którą warto opowiedzieć — nie tylko o ataku na irańskie wirówki i wykryciu pierwszej na świecie broni cyfrowej, ale też o społeczności osób zainteresowanych zabezpieczeniami i o zmianach następujących na początku epoki cyberwojen. Mówienie, że coś zmieniło zasady gry, to frazes, jednak Stuxnet naprawdę to zrobił. Wszystko, co wydarzyło się w świecie złośliwego oprogramowania wcześniej, można nazwać PS (czyli „przed Stuxnetem"). Dawne złośliwe oprogramowanie reprezentowało prostsze, raczej niewinne czasy, kiedy to motywy i ambicje napastników były bardziej bezpośrednie i łatwiejsze do zauważenia.

Napisanie tej książki okazało się równie trudne co rozszyfrowanie Stuxneta. Połączenie struktury narracyjnej ze skomplikowanymi szczegółami technicznymi i kontekstem polityczno-historycznym związanym z kodem przy jednoczesnym dbaniu o to, by lektura była ciekawa, i uczciwym opisaniu żmudnej pracy, jaką badacze włożyli w analizę kodu, nie było łatwym zadaniem. Było to o tyle trudniejsze, że w tej historii wciąż pojawiało się coś nowego.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Gdy na początku 2012 r. zaczynałam na dobre pisać tę książkę, wszystko, co — jak nam się zdawało — wiedzieliśmy na temat Stuxneta, trzeba było zrewidować, ponieważ badacze dokonywali coraz to nowych odkryć. Najpierw był Duqu, potem Flame, a później, na początku 2013 r., Stuxnet 0.5, pierwsza znana wersja tej cyfrowej broni. Nawet dziś nie wszystko jest jeszcze pewne.

Stuxnet i pomocnicze narzędzia szpiegowskie były najnowocześniejszymi osiągnięciami w czasach, gdy zostały opracowane i zastosowane. Jednak czasy się zmieniają i Stuxnet bez wątpienia został prześcignięty przez inne później zbudowane cyfrowe narzędzia, które dopiero zostaną wykryte, co może się stać za wiele lat.

Choć pisanie tej książki było trudne, pracę ułatwiały mi ogromna pomoc i wsparcie ze strony wielu osób.

Książka nigdy by nie powstała bez zachęty i wsparcia mojego agenta, Davida Fugate'a, który po raz pierwszy skontaktował się ze mną w 2007 r., po tym jak opublikowałam w magazynie „Wired" serię trzech artykułów na temat forów dyskusyjnych cyfrowego podziemia i fascynującej społeczności korzystających z nich złodziei kart bankowych. Choć nie zdecydowałam się rozwinąć tej serii do postaci książki, David przez kilka lat pozostawał ze mną w kontakcie — od czasu do czasu zgłaszał się do mnie, mówiąc, że wciąż jest zainteresowany współpracą, i pytając, czy planuję jakiś projekt.

W procesie oceny propozycji książki i pisania tego tekstu David pozostawał moim wytrwałym sojusznikiem. Przekazywał mi cenne opinie i punkt widzenia weterana rynku wydawniczego, a przy tym udzielał odpowiedniej zachęty, gdy najbardziej tego potrzebowałam. Jest tego rodzaju popleczni-kiem, jaki przydałby się każdemu autorowi.

Oprócz Davida ważną rolę odegrał mój redaktor z wydawnictwa Crown/Random House, Julian Pavia, który pomógł mi nadać książce kształt i trzymać się tematu. Był to trudny projekt, jednak Julian poradził z nim sobie z wdziękiem i cierpliwością, nawet gdy treść książki nieoczekiwanie się zmieniała i gdy przekraczałam kolejne terminy. Wykonał też doskonałą robotę, skracając szczegółowe opisy techniczne, aby zapewnić płynność narracji i wygładzić moją czasem niezgrabną prozę.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

Dziękuję też Kim Silverton, sekretarce redakcji w wydawnictwie Random House, za celne i pomocne uwagi dotyczące manuskryptu na etapie redakcji tekstu. Jestem wdzięczna również zespołom ds. reklamy i marketingu: Sarah Breivogel, specjalistce od reklamy w Random House, Sarah Pekdemir, starszej menedżerce ds. marketingu, i Jayowi Sonesowi, dyrektorowi marketingu w Crown, za ich entuzjastyczne wsparcie dla książki.

Książka nie powstałaby bez wszystkich utalentowanych badaczy, którzy wykonali ciężką pracę, rozszyfrowując Stuxneta i powiązany z nim arsenał narzędzi, a także okazali się niestrudzeni w pomaganiu mi w zrozumieniu szczegółów. Są wśród nich Siergiej Ulasen z VirusBlokAdy (obecnie pracujący dla firmy Kaspersky Lab) i Oleg Kupriejew z VirusBlokAdy, którzy jako pierwsi ogłosili alarm i sprawili, że reszta świata zwróciła uwagę na dziwny kod odkryty w Iranie.

Do tej grupy naturalnie należy też błyskotliwy i pracowity zespół z Symanteca — Eric Chien, Liam O'Murchu i Nicolas Falliere, których dociekliwość, wytrwałość i umiejętności pozwoliły odkryć najważniejsze części zagadki Stuxneta i sprawiły, że ten kod nie odszedł cicho do przeszłości. Cała trójka chętnie poświęcała mi czas i mimo napiętych harmonogramów znosiła liczne serie pytań, aby podzielić się swoimi poglądami i wiedzą.

Nie potrafię wyrazić, jak bardzo jestem wdzięczna zarówno im, jak i ich równie inteligentnym i niestrudzonym badaczom i analitykom z firmy Kaspersky Lab: Costinowi Raiu, Aleksowi Gostiewowi, Roelowi Schouwenbergowi, Kurtowi Baumgartnerowi, Witalijowi Kamlukowi i pozostałym pracownikom globalnego zespołu badawczego. Te osoby wielokrotnie zaskakiwały mnie swoimi umiejętnościami i oddaniem w sprawdzaniu nawet najdrobniejszych szczegółów bardzo skomplikowanych ataków. Współpraca z nimi często wymagała ode mnie rozmów o szóstej rano, aby uwzględnić różnicę czasu w stosunku do Europy Wschodniej. Szczególnie wdzięczna jestem Costinowi za wykraczanie poza swoje obowiązki, nierzadko kosztem czasu spędzanego z rodziną, i za jego niezwykłą mądrość, pamięć i dbałość o szczegóły. Pomogło mi to zrozumieć wiele irytujących mnie kwestii, które wraz z każdym nowym odkryciem stawały się coraz bardziej złożone.

Gorąco dziękuję również Gregowi Funarowi i Ryanowi Naraine'owi z firmy Kaspersky Lab, którzy posiedli niezwykłą umiejętność przewidywania, co będzie mi potrzebne, zanim ja sama o tym wiedziałam, a także z niesłabnącym zaangażowaniem dbali o to, by żadne z moich pytań nie

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

pozostało bez odpowiedzi. Ryan wcześniej był znanym dziennikarzem zajmującym się zabezpieczeniami, co w połączeniu z jego wiedzą techniczną sprawiło, że okazał się doskonałym pośrednikiem w kontaktach z zespołem badawczym.

Obok zespołów badawczych z firm Symantec i Kaspersky niezwykle ważną rolę w ujawnieniu historii Stuxneta odegrali Ralph Langner i jego współpracownicy, Ralf Rosen i Andreas Timm. Zapał Ralpha sprawił, że Stuxnet wciąż był opisywany przez prasę i przyciągał uwagę głównych mediów. Ponadto bogata wiedza Ralpha z dziedziny systemów kontroli procesów przemysłowych pomogła opinii publicznej zrozumieć ogólny wpływ Stuxneta na bezpieczeństwo infrastruktury krytycznej. Jestem wdzięczna za wiele godzin, jakie Ralph spędził na telefonicznych i bezpośrednich rozmowach ze mną, aby pomóc mi zrozumieć Stuxneta w szerszym kontekście. Szczerość i bezpośredniość badacza pozwoliły mu dotrzeć do istoty sprawy i zapewniły, że opinia publiczna nie mogła zaprzeczyć znaczeniu Stuxneta lub zignorować problemu. Dziękuję też Ralfowi Rosenowi za czas, jaki poświęcił na rozmowę ze mną o swojej pracy nad Stuxnetem i na przegląd fragmentów gotowego tekstu pod kątem poprawności.

Także Boldizsár Bencsáth bardzo hojnie dzielił się ze mną czasem i wiedzą. Był uprzejmym i nieocenionym wsparciem, pomagając mi rozwikłać kilka zagadek i zrozumieć powiązania między wszystkimi atakami.

Inną obok wymienionych badaczy osobą, której jestem winna głęboką wdzięczność, jest David Albright z ISIS, który pomógł nie tylko mnie, ale też Symantecowi i Ralphowi Langnerowi w zrozumieniu wpływu Stuxneta na Natanz i proces wzbogacania uranu. Zarówno on, jak i Olli Heinonen, były pracownik MAEA, a obecnie starszy współpracownik w Belfer Center for Science and International Affairs na Harvardzie, podzielili się bardzo cennymi informacjami na temat irańskiego programu nuklearnego, a zwłaszcza procesu wzbogacania uranu w Natanzie.

Dziękuję też Corey Hinderstein, pracującej obecnie dla Nuclear Threat Initiative, za podzielenie się ze mną wrażeniami z pierwszej ręki z konferencji prasowej poświęconej ujawnieniu zakładu w Natanzie, a także opisanie odkrycia niesławnych zdjęć satelitarnych.

Chcę też podziękować Dale'owi Patersonowi, Perry'emu Pedersonowi, Joemu Weissowi i Mike'owi Assantemu za pomoc w zrozumieniu ogólnego wpływu zastosowania Stuxneta i podobnych broni na infrastrukturę

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

krytyczną. Dale i Perry byli wyjątkowo pomocni, ponieważ przeczytali rozdział dotyczący systemów kontroli procesów przemysłowych i podzielili się opiniami na jego temat.

Dziękuję też Jasonowi Healeyowi i Marcusowi Sachsowi za informacje na temat początków rządowego programu budowy broni cyfrowej, a Jasonowi dodatkowo za wyrażenie zdania na temat implikacji zastosowania Stuxneta i Flame'a oraz na temat dalszego rozwoju sytuacji. Jestem też wdzięczna Charliemu Millerowi i Chaoukiemu Bekrarowi za szczerość w wypowiedziach na temat rynku luk typu zero-day oraz pomoc w zrozumieniu motywacji uczestników tego rynku.

Oprócz tych wszystkich osób są też inne, które udzielały wywiadów lub czytały rozdziały (albo ich fragmenty) i przekazywały mi mile widziane oraz przydatne uwagi. Niektóre z tych osób wymieniłam już z nazwiska, jednak wielu z nich prosiło o zachowanie anonimowości.

Jednym z czytelników, którym chciałabym podziękować szczególnie gorąco, jest Andrea Matwyshyn, droga mi przyjaciółka, która od wielu lat wspiera mnie w pracy i w karierze. Andrea zabierała ze sobą rozdziały książki na konferencje i wakacje, aby szybko przekazać mi informacje zwrotne, na których mi zależało. Gorące podziękowania otrzymuje też Cem Paya, inny bliski przyjaciel wspomagający mnie w pracy, który zabrał rozdziały książki na urlop do Turcji, a nawet kilkakrotnie czytał różne wersje tekstu, aby sprawdzić poprawność i spójność szczegółów technicznych.

Ta książka o Stuxnecie jest ukoronowaniem ponad dekady pisania o cyberbezpieczeństwie, hakerach i społeczności zainteresowanej zabezpieczeniami. Wszystkie wymienione obszary pomogły mi wzbogacić wiedzę i lepiej zrozumieć te skomplikowane kwestie. Dziękuję licznym znajomym, rodzinie i współpracownikom za wsparcie, inspirację, wskazówki, zachęty, staranną redakcję i głos rozsądku przez wiele ostatnich lat. Do tej grupy należą: Richard Thieme, Dan Goodin, Elinor Mills i Rob Lemos, a także moi byli i obecni współpracownicy z „Wired": Chuck Squatriglia, Jim Merithew, Kevin Poulsen, Ryan Singel i David Kravets. Dziękuję też Davidowi Zetterowi i Markowi Zetterowi za nieustające wsparcie i wiele dobrych wspomnień.

helion kopia dla: Adam Kufel adam.kufel2@gmail.com

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION

1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

http://program-partnerski.helion.pl

GRUPA WYDAWNICZA
Helion SA

helion kopia dla: Adam Kufel adam.kufel2@gmail.com