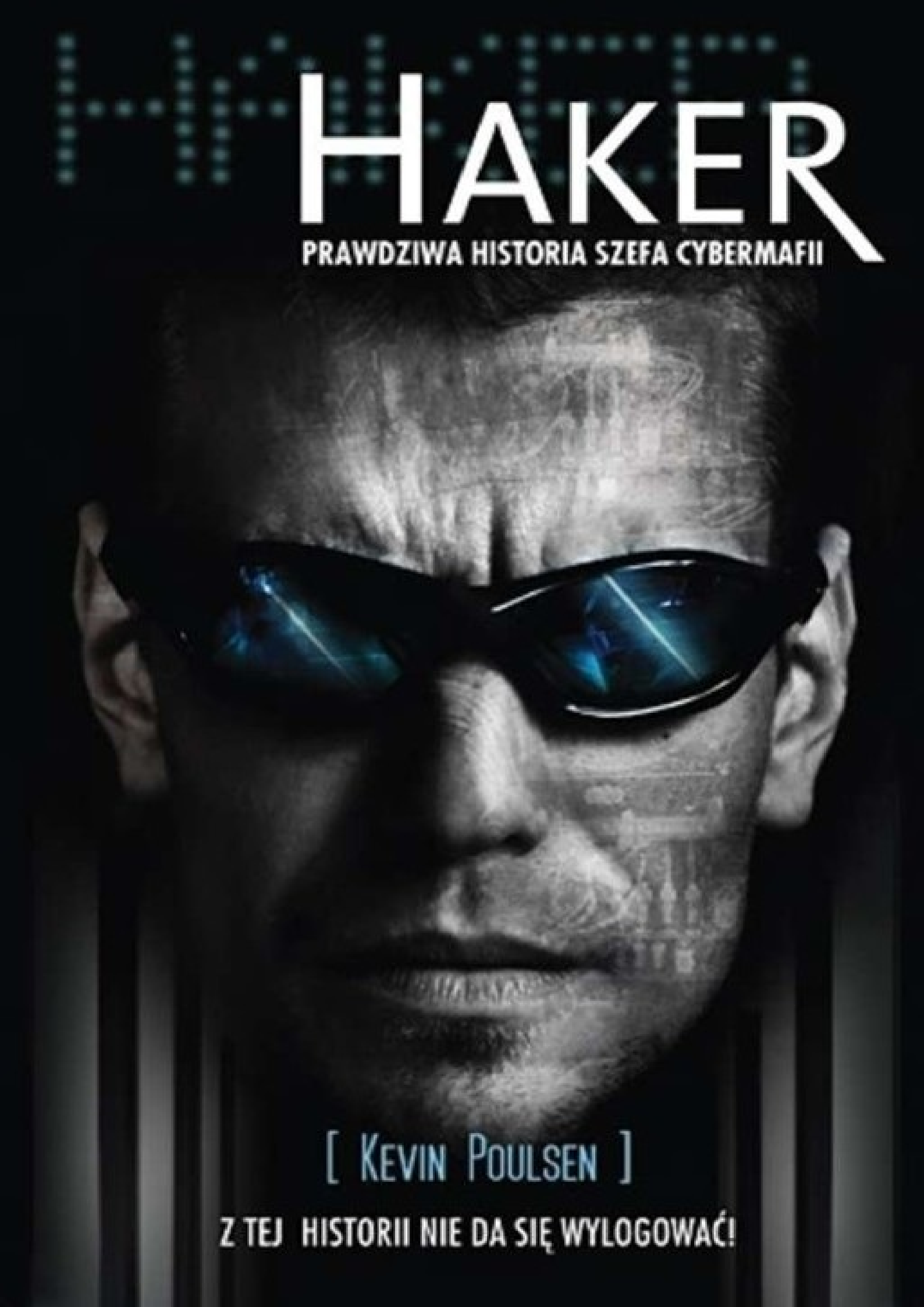
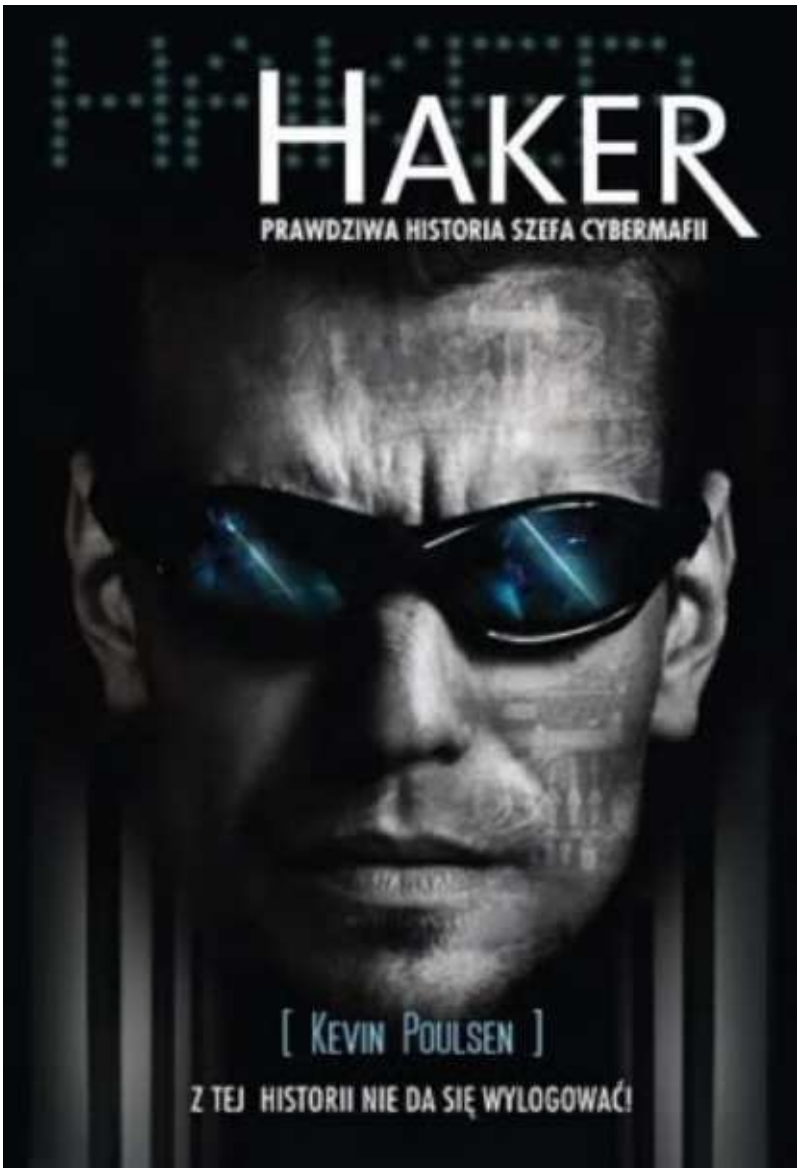
HAKER

PRAWDZIWA HISTORIA SZEFA CYBERMAFII



[KEVIN POULSEN]

Z TEJ HISTORII NIE DA SIĘ WYLOGOWAĆ!



Kevin Poulsen

HAKER

Prawdziwa historia szefa cybermafii

tłumaczenie Tomasz Macios

Kraków 2011

Tytuł oryginału

Kingpin. How One Hacker Took Over The Billion-Dollar Cybercrime Underground

Projekt okładki Magda Kuc

Opieka redakcyjna Ewa Polańska Artur Wiśniewski

Adiustacja Anastazja Oleśkiewicz

Korekta

Barbara Gąsiorowska

Opracowanie typograficzne Daniel Malak

Łamanie Irena Jagocha

ISBN 978-83-240-1659-4

Książki z dobrej strony: www.znak.com.pl

Społeczny Instytut Wydawniczy Znak, 30-105 Kraków, ul. Kościuszki 37

Dział sprzedaży: tel. 12 61 99 569, email: czytelnicyg>znak.com.pl Wydanie I, Kraków 2011

Druk: Drukarnia GS, ul. Zabłocie 43, Kraków

Dla Lauren,

mojej nieoskarżonej współsprawczyni w życiu

Gliniarze i carderzy

Max Vision - urodzony jako Max Butler. Prowadził Carders Market pod nickiem „Iceman”. Znany także jako Ghost23, Generous, Digits, Aphex i Whiz.

Christopher Aragon - znany jako Easylivin’, Karma i The Dude. Wspólnik Maksa na Carders Market, przewodził szajce czerpiącej duże zyski z fałszowania kart kredytowych, bazując na danych wykradzionych przez Maksa.

Script - ukraiński sprzedawca kradzionych danych kart kredytowych i zało-

życiel CarderPlanet, pierwszego forum carderów.

King Arthur - wschodnioeuropejski phisher i mistrz w zdobywaniu gotów-ki dzięki sfałszowanym kartom bankomatowym, który przejął CarderPlanet od Scripta.

Maksik - ukraiński carder Maksym Jastremski, zajął miejsce Scripta jako największy sprzedawca kradzionych danych kart kredytowych w półświatku.

Albert Gonzalez - znany jako Cumbajohnny i SoupNazi. Administrator Shadowcrew, największej przestępczej strony internetowej, do momentu kiedy została zlikwidowana przez Secret Service.

David Thomas - znany jako El Mariachi. Oszust weteran; prowadził forum cardingowe The Grifters będące częścią operacji zbierania informacji przez FBI.

John Giannone - znany jako Zebra, Enhance, MarkRich i The Kid. Młody carder z Long Island, pracował z Maksem online i z Chrisem Aragonem w realnym życiu.

J. Keith Mularski - znany jako Master Splyntr i Pavel Kamiński. Agent FBI z Pittsburgha, przejął DarkMarket w dużej tajnej operacji.

Greg Crabb - mentor Keitha Mularskiego, funkcjonariusz US Postal Inspection Service [USPIS, Służby Inspekcji Pocztowej Stanów Zjednoczonych], przez wiele lat tropił nieuchwytnych międzynarodowych przywódców przestępczego półświatka.

Brett Johnson - znany jako Gollumfun. Założyciel Shadowcrew, później kontynuował przestępczą działalność jako administrator Carders Market.

Tea - znana jako Alenka. Tsengeltsetseg Tsetsendelger, mongolska imigrantka, która pomagała w prowadzeniu Carders Market ze swej kryjówki w Orange County.

JiLsi - Renukanth Subramaniam, pochodzący ze Sri Lanki obywatel brytyjski, założyciel DarkMarket.

Matrix001 - Markus Kellerer, niemiecki administrator DarkMarket.

Silo - Lloyd Liske, kanadyjski haker, który został informatorem policji z Vancouver.

Th3C0rrupted0ne - były diler narkotykowy i drobny haker, pełnił funkcję administratora na Carders Market.

Prolog

Taksówka zatrzymała się naprzeciw nocnego sklepu w centrum San Francisco.

Max Vision zapłacił kierowcy i jego blisko dwumetrowa sylwetka, z gęstymi brązowymi włosami gładko zaczesanymi w kucyk, wynurzyła się z samochodu. Wszedł do sklepu, zaczekał, aż taksówkarz odjedzie, po czym skierował się do bezpiecznego mieszkania znajdującego się dwie przecznice dalej.

Wokół niego, pod zasnutym chmurami niebem, budziły się małe sklepy i stoiska z prasą, a ubrani w garnitury ludzie sunęli jeden za drugim do wznoszą-

cych się ponad nimi biurowców. Max również wybierał się do pracy, ale nie po to, by potem po dziewięciu godzinach wrócić do domu na zasłużony odpoczy-nek. Tym razem zamknie się niczym w klasztornej celi na wiele dni. Kiedy już zacznie realizować swój plan, nie będzie powrotu do domu. Żadnego wymyka-nia się na obiad czy choćby przekąskę. Żadnych nocnych randek w multiplek-sie. Nic, dopóki nie skończy.

To był dzień, w którym wypowiedział wojnę.

Posuwistym krokiem doszedł do Post Street Towers, mijając szereg iden-tycznych okien w wykuszach w kolorze mostu Golden Gate. Pojawiał się 11

na tym osiedlu przez wiele miesięcy, za wszelką cenę starając się wmieszać w tłum studentów z wymiany, których przyciągnęły tu krótkie terminy wynajmu i rozsądne ceny mieszkań. Nikt nie znał jego nazwiska, w każdym razie tego prawdziwego. Nikt nie znał też jego przeszłości.

Tutaj nie był Maksem Butlerem, małomiasteczkowym rozrabiaką, którego obsesja doprowadziła do aktu przemocy, bezpowrotnie zmieniającego jego życie, ani też Maksem Visionem, samozwańczym ekspertem od bezpieczeń-

stwa komputerowego, który brał sto dolarów za godzinę, pracując przy wzmacnianiu sieci w firmach z Doliny Krzemowej. Kiedy wjeżdżał windą na swoje piętro, Max stawał się kimś innym - Icemanem, wybijającą się postacią nielegalnego biznesu, odpowiedzialną za miliardy dolarów ukradzionych amerykańskim firmom i konsumentom.

Ale Iceman miał dość.

Przez wiele miesięcy obrabiał handlarzy z całego kraju, gromadząc mnó-

stwo numerów kart kredytowych, które na czarnym rynku powinny być warte setki tysięcy dolarów. Rynek jednak się załamał. Dwa lata wcześniej agenci Secret Service przejechali wirtualnym buldożerem przez największe miejsce spotkań komputerowego podziemia, aresztując przywódców i sprawiając, że reszta uciekła do czat roomów i małych forów naszpikowanych tajniakami i konfidentami. Panował bałagan.

Podziemny światek, czy zdawał sobie z tego sprawę czy nie, potrzebował

silnego przywódcy, który mógłby go zjednoczyć. Ktoś musiał zrobić porządek.

Po wyjściu z windy Max zatrzymał się w holu, by sprawdzić, czy nie ma ogona, po czym

wszedł w przytłaczający zaduch wynajmowanej kawalerki.

Upał był największym problemem w budynku. Serwery i laptopy stłoczone w małym pomieszczeniu wytwarzały żar, który pulsował w całym pokoju. Latem Max używał wentylatorów, lecz przynosiły one znikomą ulgę i podnosiły rachunki za elektryczność tak bardzo, że zarządca budynku podejrzewał go o uprawę konopi. Ale to były tylko maszyny oplatane siecią kabli, z których 12

najważniejszy wił się aż do gigantycznej parabolicznej anteny wycelowanej za okno niczym karabin snajpera.

Otrząsając się z nieprzyjemnego uczucia, Max zasiadł do klawiatury i zapu-

ścił się na fora, gdzie zbierali się przestępcy - do wirtualnych spelunek o na-zwach DarkMarket i TalkCash. Przez dwa dni hakował, a jego palce poruszały się z nadnaturalną prędkością, kiedy łamał zabezpieczenia stron, wykradając ich zawartość: loginy, hasła i adresy mailowe. Gdy się zmęczył, padał na rozkładane łóżko, by zdrzemnąć się przez godzinę lub dwie, a potem wracał do pracy z przekrwionymi oczami.

Skończył kilkoma uderzeniami w klawisze, wymazując bazę danych ze strony z równą łatwością, z jaką podpalacz odpala zapałkę. 16 sierpnia 2006

roku wysłał zbiorowego nonszalanckiego maila do dziesiątek stron, które splą-

drował, informując, że teraz należą one do Cardersmarket.com, stworzonego przez Icemana największego przestępczego targowiska na świecie z 6000 użytkowników - potężnego i jedynego gracza na rynku.

Jednym pociągnięciem Max zniweczył całe lata pieczołowitej pracy prawników i przywrócił do życia warte miliardy dolarów kryminalne podziemie.

W Rosji i na Ukrainie, w Turcji i Wielkiej Brytanii, w mieszkaniach, biurach i domach w całej Ameryce przestępcy obudzili się na sygnał o pierwszym wrogim przejęciu podziemnego świata. Niektórzy z nich trzymali pistolety na nocnych stolikach, by bronić zrabowanych milionów, ale przed tym nie mogli się obronić. Z równym przerażeniem czytali tę informację agenci FBI i Secret Service, którzy spędzili miesiące, a nierzadko nawet lata, infiltrując zniszczone teraz podziemne fora, i przez chwilę wszyscy oni - superhakerzy, rosyjscy ma-fiosi, mistrzowie fałszywej tożsamości i rozpracowujący ich policjanci - zada-wali sobie to samo pytanie.

Kim jest Iceman?

ROZDZIAŁ 1

Klucz

Kiedy tylko pikap wtoczył się na krawężnik, siedzący na chodniku geekowie zrozumieli, że będą kłopoty. „Pieprzeni falowcy” - krzyknął przez okno jeden z kowbojów. Z samochodu wyleciała butelka po piwie i roztrzaskała się o ziemię. Geekowie, którzy wyszli z klubu, by porozmawiać z dala od zgiełku muzyki, już dobrze to znali. W Boise roku 1988 bycie przyłapanym publicznie bez paska z szeroką klamrą i kowbojskiego kapelusza było poważnym wykrocze-niem.

Jeden z nich zrobił coś, czego kowboje się nie spodziewali: wstał. Max Butler był wysoki i szeroki w ramionach, a imponujące wrażenie, jakie robiła jego sylwetka, potęgowała jeszcze fryzura, irokez z kolców, który dodawał mu prawie dziesięć centymetrów wzrostu. „Falowiec? - zapytał spokojnie, udając, że nie zna popularnego w Boise slangowego określenia fanów muzyki nowofalo-wej i innych dziwaków. - A co to jest?” Dwaj kowboje pogrozili mu, zaklęli i ruszyli z piskiem opon i furkotem chlapaczy.

Max stał się nieoficjalnym ochroniarzem grupy kumpli, komputerowych nerdów z Meridian w stanie Idaho - „sypialni”, którą wtedy oddzielało od Boise 15

trzynastokilometrowe pstrokate pasmo pól uprawnych - odkąd spotkali się w ogólniaku. Sto lat wcześniej ojcowie miasta nadali mu nazwę Meridian (Południk), ze względu na jego umiejscowienie dokładnie na południku Boise, jednej z 37 niewidzialnych linii biegnących z północy na południe, które tworzą osie Y w systemie pomiarów amerykańskiej ziemi. Ale to była prawdopodobnie jedyna niezwykła rzecz związana z miastem, w którym wszystkie dziewczyny należały do szkolnej drużyny rodeo.

Rodzice Maksa pobrali się w młodym wieku i przenieśli do Idaho z Phoenix, gdy był niemowlakiem. W pewien sposób Max łączył w sobie ich najlepsze cechy: Robert Butler był weteranem wojny w Wietnamie i entuzjastą nowych technologii, prowadzącym sklep komputerowy w Boise. Natalie Sko-rupsky była córką ukraińskich imigrantów - humanistką i osobą miłującą po-kój; lubiła się relaksować, oglądając Weather Channel i filmy przyrodnicze.

Max przejął od matki system wartości - unikał czerwonego mięsa, papierosów, alkoholu i narkotyków, jeśli nie liczyć niefortunnego eksperymentu z żuciem tytoniu. Ojciec zaraził go wielką pasją do komputerów. Chłopak dorastał w otoczeniu egzotycznych maszyn - od gigantycznych komputerów biznesowych, które zajmowały dwa biurka, po pierwsze „przenośne” kompaktowe komputery IBM wielkości walizki. Mógł się nimi bawić do woli. Kiedy miał osiem lat, zaczął programować w BASIC-u.

Rozwód rodziców wytrącił Maksa z równowagi. Miał wtedy czternaście lat.

Ojciec został w Boise, a on z matką i młodszą siostrą Lisa zamieszkali w Meridian. W wyniku tych wydarzeń nastolatek całkiem się załamał i ograniczył do dwóch trybów funkcjonowania: relaksu i napadów szału. Kiedy jego maniakal-na strona brała górę, świat był zbyt wolny, aby za nim nadążyć. Jego mózg poruszał się z prędkością światła i koncentrował się niczym promień lasera na zadaniu, które miał wykonać. Kiedy dostał prawo jazdy, prowadził swojego nissana, nie zdejmując nogi z pedału gazu. Pędził od

jednego znaku STOP do następnego, z laboratoryjnymi goglami na nosie, niczym szalony naukowiec przeprowadzający eksperyment z zakresu fizyki newtonowskiej.

16

Max chronił swych przyjaciół, a oni próbowali chronić Maksa przed nim samym. Jego najlepszy kumpel, genialny dzieciak Tim Spencer, uważał, że świat Maksa jest ekscytujący, ale nieustannie powstrzymywał żywiołowość przyjaciela. Pewnego dnia wynurzył się ze swego domu i zobaczył go nad skomplikowanym geometrycznym wzorem płonącym na trawniku. Max znalazł

w pobliżu kanister z benzyną. „Max, to jest nasz dom!” - wykrzyknął Tim.

Max wybełkotał przeprosiny, kiedy obaj zadeptywali płomień.

To właśnie ta impulsywna strona Maksa sprawiła, że przyjaciele postanowili nie mówić mu o kluczu.

Geekowie z Meridian znaleźli pęk kluczy w niezamkniętym biurku na zapleczu laboratorium chemicznego. Przez pewien czas tylko je oglądali, wysu-wając szufladę, kiedy instruktora z laboratorium nie było w pobliżu, i spraw-dzali, czy ciągle jeszcze tam są. W końcu ukradli je, przeszmuglowali z laboratorium i zaczęli dyskretnie testować na różnych zamkach na kampusie Meridian High. W ten sposób odkryli, że jeden z nich był głównym kluczem do szkoły: otwierał drzwi frontowe i wszystkie pozostałe.

Zrobili cztery kopie, po jednej dla każdego: dla Tima, Setha, Luke’a i Johna.

Dokładnie wytarty z odcisków palców pęk kluczy powrócił w mrok biurka w laboratorium chemicznym. Wszyscy zgodnie zdecydowali, że Max nie może się o tym dowiedzieć. Główny klucz do szkoły to talizman, z którym należy się obchodzić bardzo ostrożnie, a nie marnować go na głupoty. Przysięgli więc, że zachowają go na wielki dowcip w ostatniej klasie. Wślizną się do szkoły i przejmą szkolny radiowęzeł, puszczając muzykę w każdej sali. Aż do tej chwili cztery klucze pozostaną w ukryciu - brzemię niesione w milczeniu przez każ-

dego z nich.

Nikomu nie podobało się trzymanie tego w sekrecie przed Maksem, ale widzieli, że był on już na prostej drodze do konfliktu ze szkolną administracją.

Drwił z programu zajęć, a kiedy nauczyciel nudził na temat historii lub pisał

17

równania na tablicy, Max siedział w ławce, przeglądając komputerowe wydru-ki z osiąganego dzięki modemowym połączeniom Internetu sprzed narodzin WWW i systemów bulletin board. Jego ulubioną lekturą był internetowy hakerski newsletter „Phrack”, produkt sceny hakerskiej końca lat osiemdziesią-

tych. W jego prostej, surowej wersji Max mógł śledzić wyczyny redaktorów takich jak Taran King i Knight Lightning i autorów takich jak Phone Phanatic, Crimson Death i Sir Hackalot.

Pierwsze pokolenie dorastające w erze domowych komputerów próbowało władzy, którą w miało w zasięgu ręki, a „Phrack” był dawką wywrotowej elektronicznej informacji ze

świata wykraczającego daleko poza granice sennego Meridian. Typowy numer magazynu wypełniały samouczki na temat sieci takich jak Telenet i Tymnet, opartych na komutacji pakietów, przewodniki po komputerach (takich jak COSMOS) używanych w firmach telefonicznych i szczegółowe analizy systemów operacyjnych dużej skali, na których pracowały wielkie i małe komputery w dobrze wyposażonych klimatyzowanych pomieszczeniach na całym świecie.

„Phrack” śledził również pilnie najnowsze doniesienia z frontu walki między hakerami i ich przeciwnikami w stanowej i federalnej policji, która właśnie zaczynała doceniać wyzwania rzucane przez hakerów prowadzących swą działalność dla rozrywki. W lipcu 1989 roku absolwent Cornell Robert T. Morris junior został oskarżony na podstawie świeżo przyjętego federalnego prawa dotyczącego przestępstw komputerowych, po tym jak puścił w obieg pierwszego internetowego robaka - wirusa, który zaatakował 6000 komputerów, zapy-chając łącza i powodując zawieszenie się systemu. W tym samym roku w Kalifornii młody Kevin Mitnick został po raz drugi aresztowany za działalność hakerską i skazany na rok więzienia - wówczas był to zaskakująco surowy wyrok.

Max stał się „Lordem Maksem” systemu bulletin board w Boise i zagłębił się w arkanach sztuki dzwonienia za darmo - tradycji hakerskiej sięgającej lat siedemdziesiątych. Kiedy za pomocą modemu Commodore 64 wyszukiwał

kody darmowych długodystansowych połączeń, miał pierwsze starcie z władzami federalnymi: agent Secret Service z biura w Boise odwiedził go w szkole i przedstawił dowody nielegalnych połączeń. Ponieważ Max był nieletni, nie został oskarżony. Agent ostrzegł go jednak, aby zmienił swoje postępowanie, zanim wpadnie w poważne kłopoty.

Chłopak zarzekał się, że rozumie swój błąd.

Potem wydarzyło się coś, co było nie do pomyślenia. Max zauważył dziwny kształt na kółku do kluczy Johna i spytał, co to jest. Ten wyznał mu całą prawdę.

Obaj weszli do szkoły tej samej nocy i wpadli w szał. Jeden z nich, a może obaj nagryzmolili hasła na ścianach, rozpylili pianę z gaśnicy po korytarzach i splądrowali zamkniętą szafę w laboratorium chemicznym. Max zgarnął cały asortyment chemikaliów i ułożył je na tylnym siedzeniu swego samochodu.

Telefon Setha zadzwonił nazajutrz wczesnym rankiem. To był Max; zostawił koledze prezent na podwórku przed domem. Na trawniku leżały butelki z chemikaliami. Seth spanikował, pozbierał je i zaniósł za dom, gdzie złapał za łopatę i zaczął kopać dół.

Wtedy matka przyłapała go na zakopywaniu dowodów.

- Wiesz, że muszę o tym powiadomić szkołę, tak? - powiedziała.

Seth został zaprowadzony do biura dyrektora i dokładnie przepytany, od-mówił jednak wydania wspólnika. Jeden po drugim wszyscy geekowie ze szkoły w Meridian byli ściągani przez umundurowaną straż szkolną na przesłuchanie, niektórzy z nich w kajdankach. Kiedy przyszła kolej na Johna, puścił farbę.

Wezwano policję, która znalazła alarmującą żółtą plamę po jodynie na tylnym siedzeniu samochodu Maksa.

Kradzież chemikaliów została potraktowana bardzo poważnie. Wyrzucono Maksa ze szkoły i postawiono go przed sądem dla nieletnich. Przyznał się do celowego uszkodzenia własności, włamania pierwszego stopnia i kradzieży.

Spędził też dwa tygodnie w szpitalu na obserwacji psychiatrycznej, gdzie został zdiagnozowany jako chory na psychozę dwubiegunową. Ostatecznie 19

sprawa skończyła się nadzorem sądowym. Matka wysłała go do Boise, by zamieszkał z ojcem i uczęszczał do Bishop Kelly, jedynego katolickiego liceum w całym stanie.

Pierwszy wyrok był mały, ale gwałtowność i złośliwość, które do niego doprowadziły, tkwiły głęboko w osobowości Maksa. A jego przeznaczeniem było posiadać znacznie więcej głównych kluczy.

ROZDZIAŁ 2

Śmiercionośna broń

To jest pokój rekreacyjny!!!!

W tym dużym ciemnym pomieszczeniu nie ma widocznego wyjścia. Ludzie relaksują się na poduszkach naprzeciw wielkiego ekranu. Są tu też wypełniona po brzegi lodówka i bar.

Te słowa witają odwiedzających TinyMUD, wirtualny świat zamknięty w beżowym komputerze wielkości małej lodówki, umieszczonym na podłodze biura studentów ostatniego roku uniwersytetu w Pittsburghu. W 1990 roku setki ludzi z całego globu dostało się do tego świata przez Internet. Max, świe-

żo upieczony student Boise State University (BSU), był jednym z nich.

Internet liczył sobie wtedy siedem lat i około trzech milionów ludzi miało do niego dostęp za pośrednictwem marnych 300 000 hostujących komputerów instytucji związanych z armią i stopniowo rosnącej liczby *college'ów* i uniwersytetów. Sieć była początkowo uznawana za zbyt ważną, aby oddać ją w ręce studentów, co jednak z czasem się zmieniło. MUD-y, „lochy dla wielu użytkowników", stały się ulubionym miejscem odwiedzin.

Jak większość rzeczy, które pojawiły się w Internecie przed WWW, MUD-y oferowały czysto tekstowe doświadczenie - świat definiowany całkowicie 21

przez prozę i sterowany prostymi poleceniami, takimi jak „południe", „pół-

noc". TinyMUD wyróżniał się jako pierwszy świat online, który zrzucił jarzmo reguł wyznaczonych przez Dungeons and Dragons. Zamiast ograniczać władzę tworzenia do kilku wybranych administratorów lub „czarowników", TinyMUD

zapewniał wszystkim jego mieszkańcom prawo do zmiany świata wokół nich.

Każdy mógł stworzyć własną przestrzeń, określić jej cechy, wyznaczyć granice i przyjmować odwiedzających. Mieszkańcy szybko uznali wirtualny pokój rekreacyjny za centrum życia towarzyskiego i stworzyli szereg wejść do takich przestrzeni TinyMUD-a jak Ghondahrls Flat (Siedziba Ghondahrla), Majik's Perversion Palace (Pałac Perwersji Majika) i dwustu innych lokali.

W TinyMUD-zie nie było również systemu nagród w stylu D&D, który kładł nacisk na gromadzenie dóbr, wypełnianie misji i zabijanie potworów.

Teraz zamiast toczyć bitwy z orkami i zdobywać punkty, użytkownicy MUD-a rozmawiali, flirtowali, myśleli i uprawiali wirtualny seks. Okazało się, że uwolnienie gry od ograniczeń tolkienowskich gier fabularnych zbliżyło ją do prawdziwego życia i obdarzyło uzależniającą siłą. Popularny dowcip głosił, że MUD to skrót od „multi-undergraduate destroyer" (masowy niszczyciel studentów). W wypadku Maksa okazało się to czymś więcej niż tylko dowcipem.

Na skutek nalegań jego dziewczyna Amy* dołączyła do niego w jednym z TinyMUD-ów. Oryginał na Carnegie Mellon University został zamknięty w kwietniu, ale do tego czasu dzięki temu samemu darmowemu oprogramowaniu w sieci rozpowszechniło się kilku następców MUD-a. Max stał się Lordem Maksem, a Amy przyjęła imię Cymoril, od tragicznej bohaterki cyklu książek i opowiadań o Elryku z Melniboné autorstwa Michaela Moorcocka, należących do ulubionych opowieści Maksa.

* Imię zostało zmienione.

Cymoril była ukochaną Elryka, wątłego albinosa, który za sprawą magicz-nego miecza zwanego Zwiastunem Burzy zmienił się w przerażającego 22

władcę i czarnoksiężnika. Dla Maksa fikcyjny miecz był metaforą mocy komputera - jeśli właściwie się nim posługiwało, mógł zmienić zwykłego człowieka w króla. Ale dla Elryka Zwiastun Burzy był także przekleństwem, ponieważ był on do niego przywiązany i choć walczył, aby go okiełznać, musiał mu ulec.

Dramatyczny, skazany na niepowodzenie romans Elryka z Cymoril był od-biciem bezkompromisowej wizji romantycznej miłości, którą Max stworzył po rozwodzie swoich rodziców: przeznaczenie dosięgło Cymoril w czasie bitwy między Elrykiem a jego znienawidzonym kuzynem Yyrkoonem. Dziewczyna błagała ukochanego, by schował Zwiastuna Burzy do pochwy i skończył walkę, jednak ten, opętany gniewem, zadał Yyrkoonowi śmiertelny cios. Wydając ostatnie tchnienie, Yyrkoon dokonał łamiącego serca aktu zemsty, popychając Cymoril wprost na czubek ostrza Zwiastuna Burzy.

Upiorna prawda docierała do niego bardzo powoli, wraz z czysto zwierzęcym żalem. Zabił dziewczynę, którą kochał. Splamiony krwią Cymoril miecz wypadł mu z dłoni i zagrzechotał na stopniach. Płacząc, Elryk opadł na kolana obok ciała ukochanej i wziął ją w ramiona. Cymoril - jęczał roztrzęsiony. - Cymoril… zabiłem cię*.

* Michael Moorcock, *Los Białego Wilka,* tłum. Radosław Kot (przyp. tłum.).

Na początku Amy myślała, że Max jest fajny, zbuntowany, ma coś z punka i wyróżnia się z tłumu w Boise. Ale kiedy spędzali z sobą każdą wolną chwilę, zaczęła zauważać ciemniejszą, obsesyjną stronę jego osobowości, zwłaszcza gdy zapoznał ją z Internetem i TinyMUD-em.

Max był podniecony tym, że jego dziewczyna podziela internetową pasję.

Ale kiedy sama zaczęła poznawać przyjaciół w MUD-zie, w tym także facetów, stał się zazdrosny i agresywny. Dla Maksa nie było żadnej różnicy, czy Amy zdradza go w prawdziwym czy w wirtualnym świecie. Tak czy inaczej, była to zdrada. Próbował

powstrzymać ją przed logowaniem się, ale odmawiała i zaczęli się kłócić zarówno online, jak i offline.

23

W końcu Amy miała już tego dość: mają się sprzeczać o głupią grę komputerową? W nocy ze środy na czwartek na początku października 1990 roku oboje byli w jednym z pokojów TinyMUD-a, kiedy Cymoril w końcu powiedziała Lordowi Maksowi, że nie jest pewna, czy tak naprawdę są jeszcze razem.

To był pierwszy poważny związek Maksa, więc zareagował ostro. Przysię-

gli sobie, że spędzą razem życie, więc teraz powinni raczej oboje umrzeć, niż się rozejść, napisał w MUD-zie. Potem przeszedł do konkretów i opisał, w jaki sposób ją zabije. Inni użytkownicy śledzili z niepokojem narastanie jego gniewu do poziomu realnej groźby. Co powinni z tym zrobić?

Jeden z „czarowników” z tego świata znalazł adres IP Maksa - unikalny identyfikator, który łatwo zaprowadził go do Boise State University. MUD-er sprawdził numer do biura szeryfa hrabstwa Ada w Boise i zadzwonił z ostrze-

żeniem o potencjalnym morderstwie i samobójstwie, o którym się dowiedział.

Ten rok zaczął się dla Maksa obiecująco. Świetnie sobie radził w pracy na pół

etatu, którą ojciec dał mu w sklepie komputerowym HiTech Systems. Był tam sprzedawcą, dostarczał też towar służbowym vanem i składał pecety na zapleczu. Udało mu się również nie naruszyć warunków nadzoru sądowego, przestał

jednak brać leki na zaburzenia maniakalno-depresyjne - ojciec nie chciał, by w pracy był na prochach, a poza tym Max nie zgadzał się z diagnozą.

Zaczął chodzić z Amy w lutym 1990 roku, cztery miesiące po tym jak spotkał ją w Zoo, klubie tanecznym w Boise, odwiedzanym przez tłumy małolatów. Była rok młodszą od niego niebieskooką blondynką. Max pierwszy raz zobaczył ją u boku swego przyjaciela Luke’a Shenemana, jednego z byłych posiadaczy klucza z Meridian. Kiedy Max kończył ostatnią klasę szkoły średniej, między nim a dziewczyną zaczęło się coś poważnego.

Niczego nie robił na pół gwizdka i jego zaangażowanie w związek z Amy było absolutne. Planowała studia na Boise State University, więc on też tam 24

poszedł, rezygnując z marzeń o CMU czy MIT. Zabrał ją do domu, by pokazać swój komputer, i grali w Tetris. Oboje znaleźli w związku to, czego brakowało w małżeństwach ich rodziców. Myśleli, że to nigdy się nie skończy.

Jego starzy przyjaciele prawie w ogóle nie widywali go podczas wakacji.

Potem zaczął się jesienny semestr w Boise State. Max zdecydował się na informatykę i zapisał na bardzo dużo kursów: rachunki, chemię i zajęcia ze struk-tury danych. Jak każdy student otrzymał konto na uniwersyteckim UNIX-ie i jak kilku z nich od razu zaczął hakować. Szlaki przetarł mu już inny student, David, który wcześniej znalazł drogę do grupy kont ludzi z kierunku. Razem spędzali całe godziny w pokoju z terminalem BSU, wpatrując się w świetlisty zielony tekst i stukając w klawisze. Przetrząsali skrzynki mailowe kierunku, prowadząc długie milczące dyskusje, przerzucając się wiadomościami

przez pokój i przez komputer. David walczył, by nadążyć za podkręconym umysłem Maksa i jego palcami z niezwykłą szybkością stukającymi w klawisze, a Max często tracił cierpliwość - „Na co czekasz? - pisał, gdy David wypadał z kon-wersacji. - Odpowiadaj”.

Administratorzy na ogół tolerowali małe lokalne włamania, ale kiedy Max zaczął węszyć przy zabezpieczeniach innych systemów internetowych, skoń-

czyło się to otrzymaniem krótkiego bana na komputer BSU. Kiedy znowu uzyskał dostęp, powrócił na TinyMUD, by kłócić się z Amy.

Szeryf zadzwonił do administratora uniwersyteckiej sieci o drugiej nad ranem, by poinformować go o groźbie morderstwa i samobójstwa. Policja chciała mieć kopie plików z dysku Maksa, aby poddać je badaniom w poszukiwaniu dowodów - prośba ta wiązała się z trudnym dla *college'u* problemem naruszenia prywatności. Po dyskusji z prawnikiem *college'u* administracja podjęła decyzję, że nie będzie dobrowolnie podejmować żadnych kroków w tym kierunku.

Zamiast tego zabezpieczono pliki Maksa na komputerze i pozbawiono chłopaka dostępu do niego.

25

Amy martwiła się, co będzie z Maksem, nawet jeśli przechodziła przez po-wolny proces zrywania z nim. Wciąż nie był jej obojętny, jak później zeznała, i obawiała się, że naprawdę zrobi sobie krzywdę.

Po tym, co wydarzyło się na TinyMUD-zie, Max nadal do niej dzwonił i rozmowy zmierzały w łatwym do przewidzenia kierunku. Na początku był

miły, pokazywał swą przyjazną stronę, którą jego rodzina i przyjaciele dobrze znali. Potem zaczynał użalać się nad sobą, by przejść do gróźb, a w końcu rozwścieczony, rzucał słuchawką.

30 października powiedział, że chciałby z nią porozmawiać osobiście. Cią-

gle jeszcze mając nadzieję na przyjacielskie zakończenie związku - była pewna, że będzie widywać chłopaka na kampusie, i nie chciała, by jej znienawidził

- Amy zgodziła się przyjść.

Max właśnie przeprowadził się z powrotem do domu matki w Meridian, budynku w stylu rancza, na spokojnej ulicy o kilka kroków od swojego dawnego liceum. Otworzył drzwi i po zapewnieniu, że nie zrobi niczego głupiego, dziewczyna poszła z nim do sypialni położonej z tyłu domu. Matki nie było, a jego czternastoletnia siostra oglądała telewizję.

Łóżko Maksa ciągle nie było zmontowane, usiedli więc na materacu na pod-

łodze i zaczęli rozmawiać o swoich uczuciach. Amy przyznała, że spotkała innego chłopaka na TinyMUD-zie. Miał na imię Chad i mieszkał w Północnej Karolinie. Ich związek przeniósł się poza wirtualny świat - wysyłali sobie zdję-

cia mailem, a ona do niego dzwoniła.

Max starał się zapanować nad uczuciami, z trudem powstrzymując łzy. Powiedział, że czuje się zdradzony. Jednocześnie nie mógł całkiem uwierzyć w to, co słyszał. Poprosił ją

o numer Chada, wyciągnął kartę telefoniczną i zadzwonił do swego wirtualnego rywala.

Nastąpiła trójstronna rozmowa; Max przedstawił się, a potem oddał słuchawkę Amy. Powiedziała Chadowi, jak się czuje. On poprosił ją o numer telefonu. Dała mu go i rozmowa przeszła w jałowe przekomarzanie się, co jeszcze bardziej wkurzyło Maksa. Złapał za słuchawkę i przerwał rozmowę.

26

Amy obserwowała uważnie, jak jego oddech staje się coraz szybszy, a wzrok nerwowo krąży po pokoju.

- Zabiję cię - powiedział w końcu. - Naprawdę chcę to zrobić: teraz umrzesz.

Odparła, że nie poczuwa się do zdrady i nie będzie przepraszać. Max zaczął

drżeć, a za chwilę jego dłonie znalazły się na jej gardle i popychały ją w dół, na materac.

- Dobrze - powiedziała - dlaczego po prostu mnie teraz nie zabijesz?

Kiedy Max odzyskał kontrolę nad sobą, chciał, żeby Amy zniknęła mu z oczu. Podniósł ją z materaca, wypchnął z sypialni i ciągnął za sobą przez cały dom aż do drzwi wyjściowych.

- Idź, teraz. Po prostu spadaj, bo nie chcę cię zabić. Ale mogę jeszcze zmienić zdanie.

Amy wskoczyła do samochodu i szybko odjechała.

W drodze do Boise układała sobie w głowie wydarzenia, które przed chwilą zaszły. Pogrążona w myślach, nie zauważyła nadjeżdżającego samochodu.

Poczuła za to siłę uderzenia i usłyszała zgrzyt metalu.

Obydwa samochody były zmiażdżone, ale nikomu nic poważnego się nie stało. Kiedy rodzice Amy dowiedzieli się o spięciu w domu Maksa, zaczęli się obawiać o jej życie. Tydzień po wypadku Amy poszła na policję i chłopak został aresztowany.

Max powiedział przyjaciołom, że Amy wyolbrzymiła całe zdarzenie. W jej wersji wypadków Max siłą trzyma ją przez godzinę w sypialni, jego dłonie kilkakrotnie lądują na jej gardle, w pewnym momencie niemal pozbawiając ją oddechu. W wersji Maksa trzyma on luźno dłonie na jej szyi przez minutę, ale nie dusi dziewczyny, a już na pewno nie przetrzymuje siłą. Według Amy po całym zajściu chłopak nadal do niej dzwoni, kierując pod jej adresem coraz więcej gróźb. On natomiast twierdził, że dał jej spokój po tym, jak wypchnął ją z domu - Amy jego zdaniem poświęcała go, by uniknąć problemów związanych z wypadkiem.

27

Prokurator okręgowy zaoferował Maksowi, że uzna to za występek. Miesiąc przed rozpoczęciem czterdziestopięciodniowej odsiadki wyznaczonej przez sędziego - Max, wolny, ale zobowiązany do stawiennictwa przed sądem - zauważył Amy spacerującą po University Avenue za rękę z nowym chłopakiem.

Kolejny raz pozwolił, by emocje wzięły górę nad zdrowym rozsądkiem. Pod wpływem impulsu skierował dostawczego vana swego ojca na trawnik i dopadł

spacerującą parę. Był spięty.

- Cześć - powiedział.

- Nie powinieneś pojawiać się w pobliżu mnie - zaprotestowała Amy.

- Nie pamiętasz, co się stało?

Towarzysz Amy odezwał się i Max ostrzegł go: „Lepiej uważaj na siebie, przyjacielu”. Po czym odmaszerował. Po chwili zawarczał silnik. Max był z powrotem w vanie, kierując się prosto ku parze na chodniku. Przejechał wystarczająco blisko, by dziewczyna poczuła pęd powietrza.

Umowa została anulowana. Prokurator okręgowy naciągnął prawo, by oskarżyć Maksa o przestępstwo - atak z użyciem śmiercionośnej broni: własnych rąk. Było to wątpliwe oskarżenie: dłonie Maksa nie były bardziej śmiercionośne niż dłonie kogokolwiek innego.

Prokurator zaoferował mu nowy układ: dziewięć miesięcy więzienia, jeśli Max przyzna się do duszenia Amy. Odrzucił propozycję. Po trzydniowym procesie i półtoragodzinnych roztrząsaniach ława przysięgłych uznała go za winnego. 13 maja 1991 roku Tim Spencer i kilku innych geeków z liceum w Meridian zasiadło na sali sądowej, obserwując, jak sędzina Deborah Bail skazuje ich przyjaciela na pięć lat więzienia.

ROZDZIAŁ 3

Głodni Programiści

Max znalazł dom Tima Spencera położony na szczycie wśród pagórków od-dzielających luźną podmiejską zabudowę półwyspu San Francisco od spokoj-nych, niezbyt rozbudowanych miasteczek na wybrzeżu Pacyfiku. Ale powiedzieć „dom” to mało. To była willa o powierzchni 557 metrów kwadratowych, rozciągająca się na dwudziestohektarowej działce z widokiem na senne nadbrzeżne miasto Half Moon Bay. Max przemaszerował przez podparty kolum-nami przedsionek do podwójnych frontowych drzwi i wszedł do przypominają-

cego jaskinię salonu, gdzie zaokrąglona ściana okien rozciągała się od podłogi aż po sufit. Minął rok od warunkowego zwolnienia Maksa, który przeniósł się do San Francisco, by zacząć wszystko od nowa. Tim i kilku innych przyjaciół z Idaho wynajmowało dom zwany Głodnym Dworkiem, co było odwołaniem do ich pierwszego przedsięwzięcia po przeniesieniu się do Bay Area rok temu.

Planowali stać się częścią gospodarki Doliny Krzemowej, tworząc komputerową firmę konsultingową pod nazwą Głodni Programiści - byli gotowi programować za kromkę chleba. Szybko znaleźli jednak pracę na pełny etat i Głodni Programi-

ści zmienili się w nieoficjalny klub przyjaciół Tima z liceum w Meridian 29

i University of Idaho, liczący ponad dwadzieścia osób. Głodny Dworek stał się miejscem imprez dla całej grupy i domem dla pięciu z nich. Max miał być szó-

sty.

Wprowadził się z ledwie garścią osobistych rzeczy, ale za to z wielkim ba-gażem, którego sporą częścią było głębokie rozgoryczenie z powodu potrakto-wania go przez wymiar sprawiedliwości. W1993 roku, kiedy Max odsiadywał

drugi rok, Sąd Najwyższy Stanu Idaho zdecydował w podobnym przypadku, że

„ręce lub inne części czy wyrostki ciała” nie mogą być uznawane za śmiercionośną broń. Oznaczało to, że Max nigdy nie powinien był zostać skazany za czynną napaść z użyciem broni. Mimo tego werdyktu jego prośba została odrzucona ze względów formalnych: sędzia przyznał, że Max technicznie nie był

winien przestępstwa, za które odsiadywał wyrok, ale jego dawny prawnik po-pełnił błąd i nie podniósł sprawy we wcześniejszej prośbie, a teraz było już na to za późno.

Kiedy Max został w końcu zwolniony 26 kwietnia 1995 roku, wychodził ze świadomością, że odsiedział ponad cztery lata w więzieniu stanowym Idaho za coś, co w świetle prawa powinno zostać uznane za występek godny spędzenia sześćdziesięciu dni w więzieniu okręgowym. Odsiadywał niesprawiedliwy wyrok, podczas gdy jego koledzy ukończyli studia, zrobili dyplomy i wyjechali z Idaho, aby rozpocząć obiecującą karierę.

Zamieszkał razem z ojcem niedaleko Seattle, gdzie odwiedzili go - w drodze na zjazd starych geeków z liceum w Meridian - Tim, Seth i Luke. Podziwiali jego muskulaturę wypracowaną w więziennej siłowni i najwidoczniej nieograniczony optymizm, którym tryskał mimo poważnego wyroku na koncie i braku dyplomu. Max wiedział, że był to czas wielu możliwości - brytyjski naukowiec stworzył World Wide Web trzy miesiące po tym, jak Max został

skazany. Teraz istniało blisko 19 000 stron internetowych, jedna z nich należa-

ła do Białego Domu. Telefoniczni dostawcy Internetu pojawili się niemal w każdym większym mieście, a America Online i CompuServe dodawały do swojej oferty możliwość korzystania z sieci.

Wszyscy zaczynali żyć online; Max nie był już dziwolągiem uzależnionym od sieci, o której nikt nie słyszał. Jak się okazało, teraz był w czołówce grupy, która rozrastała się, włączając miliony ludzi. Jednak ze względu na przeszłość walczył o zdobycie posady w Seattle, pracując dorywczo jako pomocnik techniczny.

W sieci Max kręcił się po nieprzyjemnych okolicach, szukając technicznych wyzwań, których nie dostarczała mu codzienna praca. Powrócił do sieci czat roomów zwanych IRC (Internet Relay Chat), które znał jeszcze jako nastolatek.

Kiedy znalazł się więzieniu, IRC był tłumnie odwiedzanym miejscem. Jednak wraz z rozwojem Internetu większość jego mieszkańców przeniosła się do lep-szej dzielnicy - łatwych w użyciu komunikatorów i czatów opartych na sieci WWW. Ci, którzy pozostali przy IRC-u, byli raczej zatwardziałymi geekami o złej reputacji - hakerami i piratami, knującymi coś w zapomnianych tunelach i zaułkach pod wyczyszczonym skomercjalizowanym Internetem, który rozrastał

się nad nimi.

Max wyobrażał sobie siebie jako widmową obecność w cyberświecie. W

IRC-u wybrał sobie nick Ghost23 - 23 było jego szczęśliwym numerem, poza tym był to także heksagram I Ching reprezentujący chaos. Płynął ku światu

„warez” IRC, gdzie ludzie lekceważący prawo budowali swą reputację, piratu-jąc muzykę, komercyjne oprogramowanie i gry. Wreszcie komputerowe zdolności Maksa znalazły odbiorców, którzy potrafili je docenić. Znalazł niezabezpieczony serwer plików FTP u dostawcy Internetu w Littleton w stanie Kolorado i zamienił go w kryjówkę na kradziony software dla siebie i swoich przyjaciół, zaopatrzony w nielegalne kopie programów, takich jak NetXray, Laplink i Symantec’s pcAnywhere.

To był błąd. Dostawca Internetu zauważył wyciek w swoim paśmie i wyśledził uploady Maksa do korporacyjnego biura CompuServe w Bellevue, gdzie chłopak właśnie podjął dorywczą pracę. W rezultacie zwolniono go. Nie minął

rok od wyjścia z więzienia, a Max znów zszargał sobie reputację.

To właśnie wtedy zdecydował, by zacząć na nowo w Dolinie Krzemowej, gdzie dotcomowa gospodarka osiągała dojrzałość i komputerowy geniusz 31

mógł dostać pracę bez odpowiadania na zbyt wiele pytań dotyczących jego przeszłości.

Potrzebował nowego imienia, wolnego od dawnych wygłupów. Za kratami Max miał ksywkę będącą skrótem tytułu zinu poświęconego tematyce cyber-punkowej, który tworzył na więziennej maszynie do pisania: „Maximum Vision”. Było to przyzwoite, optymistyczne imię, uosabiające wszystko, czego pragnął, i krystalizujące jego pełną nadziei postawę.

Kiedy opuszczał Seattle, patrząc w boczne lusterko, pożegnał się z Maksem Butlerem. Od teraz będzie się nazywał Max Ray Vision.

Max Vision przekonał się, że w Głodnym Dworku żyło się dobrze. Otoczony ze wszystkich stron przez łąki dom miał dwa skrzydła, cztery sypialnie, po-mieszczenie dla pokojówki, przestronną jadalnię, zagrodę dla zwierząt, opalany drewnem piec na pizzę i wewnętrzny grill w pokoju, będącym dodatkiem do obszernej nasłonecznionej kuchni. Mieszkańcy Głodnego Dworku zmienili bibliotekę w salę komputerową i serwerownię, zapełniając ją zwykłymi pece-tami przeznaczonymi do gier. Doprowadzili kable sieciowe do wszystkich pomieszczeń i zainstalowali szybki Internet, co wymagało częściowego zamknię-

cia autostrady 92, kiedy firma telefoniczna kładła nowy kabel wzdłuż drogi.

Stary system telefoniczny połączył zachodnie skrzydło domu ze wschodnim.

Na zakończenie jeden z Głodnych Programistów przyniósł wielką wannę i umieścił ją na ziemi, pod gwiazdami.

Max nie mógł sobie wymarzyć lepszego miejsca do rozpoczęcia nowego życia. Jeden z mieszkańców załatwił mu pracę administratora systemu w MPath Interactive, początkującej firmie z Doliny Krzemowej z dużym kapitałem inwestycyjnym, zajmującej się grami komputerowymi. Max rzucił się w wir pracy. Przeciwstawiając się stereotypowi komputerowego nerda, największą satysfakcję czerpał z obowiązków związanych ze wspieraniem innych. Lubił

pomagać ludziom.

Jednak dość szybko okazało się, że jego wyczyny z Seattle dopadły go aż tu. Pewnego poranka goniec wręczył mu opiewający na 300 000 dolarów pozew Software Publishers Association - przemysłowej grupy, która postanowiła wykorzystać przyłapanie go na piractwie. „To działanie jest ostrzeżeniem dla użytkowników Internetu, którzy są przekonani, że mogą naruszać prawa autor-skie do oprogramowania bez obawy, iż narażają się na karę" - ogłosiło stowa-rzyszenie w oświadczeniu dla prasy.

Jako pierwszy tego rodzaju pozew przypadek Maksa został opisany w magazynie „Wired" i wspomniany w Kongresie podczas przesłuchania na temat internetowego piractwa. Max Vision pozostał jednak niemal nietknięty - nie-wielu w jego nowym życiu łączyło go z człowiekiem wymienionym w pozwie.

Kiedy zainteresowanie prasy spadło, SPA chciało spokojnie zamknąć sprawę za 3500 dolarów i doradztwo komputerowe. Cała afera miała nawet pozytywną stronę. Dzięki niej Max trafił do FBI.

Chris Beeson, młody agent z biura grupy do zwalczania przestępstw komputerowych w San Francisco, dał Maksowi posadę. FBI mogło skorzystać z jego pomocy przy sterowaniu komputerowym podziemiem. Rozrywkowi hakerzy nie stanowili już celu dla biura, oznajmił. Teraz pojawił się nowy, groźniejszy gatunek komputerowych przestępców: „prawdziwych" przestępców. Byli wśród nich cyberzłodzieje, pedofile, a nawet terroryści. FBI nie zajmowało się już tropieniem ludzi takich jak Max i jemu podobni. „Nie jesteśmy wrogami" -

powiedział Beeson. Max nie miał nic przeciwko i w marcu 1997 roku został

formalnie włączony do programu przestępczych informatorów FBI. Jego pierwszym pisemnym raportem dla biura był kurs dla początkujących na temat tworzenia wirusów, warez i sceny hakerów komputerowych. Kolejny raport napisany dziesięć dni później dotyczył skompromitowanych stron służących transferowaniu plików - takich jak ta, którą wykorzystywał w Seattle, i gangu piratów muzycznych znanych jako Rabid Neurosis, który zadebiutował

zeszłego października nielegalnym wypuszczeniem płyty *Ride the Lightning* Metalliki.

Kiedy Max dorwał się do pirackiej wersji AutoCada, rozprowadzanej przez załogę znaną jako SWAT, FBI wynagrodziło go sumą 200 dolarów. Beeson dał

mu do podpisania rachunek z biurowym tajnym imieniem nowego nabytku: Equalizer.

Max lubił agenta FBI, a ten zdawał się odwzajemniać to uczucie. Żaden z nich nie wiedział, że Beeson pewnego dnia wsadzi Equalizera ponownie za kraty, przyczyniając się do przemiany Maksa w jednego z „prawdziwych" przestępców, na których polował.

ROZDZIAŁ 4

Biały kapelusz

Max zaczął nowe życie w czasie, kiedy w świecie hakerów zachodziły głębokie zmiany.

Pierwszymi ludźmi, którzy uznawali siebie za hakerów, byli studenci oprogramowania i elektroniki z MIT-u w latach sześćdziesiątych. Bystre, wyluzo-wane dzieciaki, mające

lekceważący i antyautorytarny stosunek do technologii, której pionierami się stały, stanowiły przeciwwagę dla pozbawionej radości kultury garniturów i laboratoryjnych fartuchów, której ucieleśnieniem było IBM. Nieodłączną część kultury hakerów stanowiło poczucie humoru i darmowe dzwonienie - zazwyczaj nielegalne eksplorowanie zakazanych zaułków sieci telefonicznych. Hakowanie było jednak przede wszystkim twórczym wy-siłkiem, który doprowadził do niezliczonych momentów przełomowych w historii komputerów.

Słowo „haker" nabrało bardziej negatywnych konotacji we wczesnych latach osiemdziesiątych, kiedy pierwsze komputery Commodore 64, TRS-80 i Apple trafiły do pokojów nastolatków na przedmieściach i w miastach w ca-

łych Stanach. Maszyny były produktem kultury hakerów: apple II, a wraz z nim idea domowego komputera narodziły się za sprawą dwóch phreakerów z 35

Berkeley: Steve'a Wozniaka i Steve'a Jobsa. Nie wszyscy nastolatkowie byli usatysfakcjonowani tymi maszynami, a właściwa młodości niecierpliwość sprawiała, że nie mieli zamiaru czekać, aż dostaną się na studia, aby poznać prawdziwą władzę, jaką daje komputer, lub eksplorować globalne sieci za pomocą telefonu i brzęczącego modemu. Zaczęli więc nielegalne wypady na korporacyjne, rządowe i akademickie systemy, stawiali też pierwsze kroki w AR-PANE-cie, poprzedniku Internetu.

Kiedy złapano pierwszych młodych włamywaczy w 1983 roku, prasa w ca-

łym kraju szukała słowa, którym można by ich nazwać, i skorzystała z tego, którego używały same dzieciaki: „hakerzy". Podobnie jak poprzednie pokole-nia hakerów, pokonywali oni ograniczenia technologii, przechytrzając esta-blishment i robiąc rzeczy, które wydawały się niemożliwe. Teraz wiązało się to także z włamywaniem się do korporacyjnych komputerów, przejmowaniem central telefonicznych, wślizgiwaniem się do systemów rządowych, uniwersyteckich i sieci pracowników obrony. Starsze pokolenie krzywiło się na to po-równanie, ale od tego momentu słowo „haker" miało dwa znaczenia: utalento-wanego programisty, który osiągnął coś własnymi siłami, i kogoś, kto dla zabawy włamuje się do cudzych komputerów. Na dodatek wielu hakerów można było zaliczyć zarówno do pierwszej, jak i do drugiej kategorii.

W połowie lat dziewięćdziesiątych społeczność hakerów znowu się dzieliła.

FBI i Secret Service aresztowały najgroźniejszych włamywaczy, takich jak Kevin Mitnick czy Mark „Phiber Optik" Abene, nowojorski phreaker. Perspek-tywa więzienia zmieniła charakter rozrywkowych włamań, sprawiając równocześnie, że nie warto było ryzykować dla osobistej satysfakcji czy przygody.

Rozmach we włamywaniu się do komputerów również osłabł: wszyscy mieli teraz dostęp do Internetu i pecety stały się dostatecznie mocne, by działać w oparciu o te same systemy operacyjne co języki programowania, które napę-

dzały wielkie maszyny niedostępne dla amatorów. Przede wszystkim można było zarobić duże pieniądze, broniąc komputerów, zamiast je atakować.

Włamania do systemów stawały się obciachowe i stopniowo rezygnowano z nich na rzecz

legalnej pracy w ochronie komputerów. I tak hakerzy zaczęli wieszać swoje czarne kapelusze na kołku, stając się „hakerami w białych kape-luszach” (było to nawiązanie do obdarzonych kwadratowymi szczękami bohaterów starych czarno-białych westernów), używającymi swych komputerowych umiejętności w służbie sprawiedliwości i prawdy.

Max uważał się za jednego z białych kapeluszy. Do jego oficjalnych obowiązków należało obecnie śledzenie nowych rodzajów ataków i wyłapywanie słabych miejsc. Jako Max Vision zaczął się właśnie udzielać na listach mailin-gowych poświęconych bezpieczeństwu komputerowemu, na których dyskutowano o ostatnich postępach w tej dziedzinie. Nie potrafił jednak całkiem wyeg-zorcyzmować Ghosta23 ze swej osobowości. Przyjaciele wiedzieli, że nadal włamuje się do systemów. Wystarczyło, że zobaczył coś nowego lub interesującego, i po prostu sam musiał spróbować.

Pewnego dnia kiedy Tim był w pracy, dostał telefon od zakłopotanego administratora systemu z innej firmy, który śledząc kierunek ataku, dotarł do Hungry.com - wirtualnej siedziby Głodnych Programistów. Przechowywali tu swoje projekty, zamieszczali CV i utrzymywali skrzynki mailowe z prywatnymi adresami, które pozostawały niezmienne mimo zmian pracy i różnych wstrząsów. W tym wspólnym systemie było dwunastu geeków, ale Tim od razu wiedział, kto za to odpowiada. Wstrzymał rozmowę z adminem i zadzwonił do Maksa.

- Przestań hakować. Natychmiast - powiedział.

Max wyjąkał przeprosiny - znów ten płonący trawnik. Tim przełączył się na drugą linię, gdzie administrator systemu z nieukrywaną radością w głosie oznajmił mu, że atak został przerwany.

Skarga zaskoczyła Maksa i wprawiła go w zakłopotanie - gdyby ludzie, któ-

rych brał na celownik, wiedzieli, jakim jest dobrym facetem, nie robiliby problemu z nieszkodliwego włamania. „Max, musisz mieć pozwolenie - wyjaśnił

Tim. Dał mu również życiową radę. - Wyobraź sobie, że wszyscy na ciebie 37

patrzą. To dobry sposób, by sprawdzić, czy to, co robisz, jest słuszne. Gdybym tam stał ja albo twój ojciec, czy nadal myślałbyś o tym tak samo? Co byśmy powiedzieli?”

Jeśli było coś, za czym Max tęsknił w nowym życiu, to bliska osoba, z którą mógłby je dzielić. Dwudziestoletnią Kimi Winters spotkał na imprezie rave zwanej Ciepło, odbywającej się w opuszczonym magazynie w mieście - Max stał się znany na scenie rave, tańcząc z zaskakującą płynnością i gracją, wirując ramionami jak brazylijski tancerz z ogniem. Kimi uczyła się w studium pomaturalnym i pracowała na pół etatu jako barista. Była o trzydzieści centymetrów niższa od Maksa i lubiła nosić rozciągniętą czarną bluzę z kapturem, w której wyglądała trochę bezpłciowo. Przy bliższym spojrzeniu można było dostrzec jej niewątpliwą urodę - zaokrąglone policzki i skórę o miedzianym odcieniu, odziedziczoną po koreańskiej matce. Max zaprosił Kimi do siebie na imprezę.

O balangach w Głodnym Dworku krążyły legendy i kiedy Kimi przyszła, w salonie pod szklanym żyrandolem roiło się już od gości z komputerowego światka Doliny Krzemowej - programistów, administratorów systemów i projektantów stron internetowych. Max rozjaśnił się, kiedy ją zauważył. Oprowadził ją po domu, pokazując różne zmyślne urządzenia, którymi Głodni Programiści wzbogacili jego wystrój.

Wycieczka skończyła się w sypialni Maksa w lewym skrzydle Głodnego Dworku. Ze względu na wielkość domu ten pokój miał urok mnisiej celi - nie było w nim żadnych mebli, tylko materac na podłodze i komputer. Na imprezie Max przyglądał się niebieskim i czerwonym plamom światła na butelce miętowego sznapsa - jego jedynej słabości. Kiedy Kimi wróciła następnej nocy na kolację, w jego wegetariańskim menu była tylko jedna pozycja: surowe ciasto.

Max pociął cukrową maź na cienkie plastry i podał swej wybrance ze sznap-sem. Dlaczego niby ktoś nie miałby zjeść na kolację surowego ciasta, jeśli mu to zaproponowano?

Kimi była zaintrygowana. Max tak niewiele potrzebował do szczęścia. Był

jak dziecko. Kiedy wkrótce po imprezie nadszedł dzień jego urodzin, wysłała 38

ozdobny karton baloników do jego biura w MPath, co wzruszyło go niemal do łez.

Była dziewczyną jego marzeń, jak jej później powiedział. Zaczęli rozmawiać o wspólnym życiu.

We wrześniu właściciel Głodnego Dworku, niezadowolony z tego, co programiści zrobili z jego posiadłością, rozwiązał z nimi umowę. Po ostatniej po-

żegnalnej balandze we wspólnym domu Głodni rozproszyli się po różnych wynajmowanych mieszkaniach wokół Zatoki. Max i Kimi wylądowali sami w Mountain View, w ciasnej kawalerce w kompleksie mieszkaniowym przypominającym baraki, położonym wzdłuż autostrady 101, zatłoczonej głównej arterii Doliny Krzemowej.

Max wznowił współpracę z FBI i polowanie w IRC-u dało mu szansę na wybicie się jako haker w białym kapeluszu. Zaprzyjaźnił się z ludźmi z czat roomów, którzy zakładali prawdziwą firmę konsultingową w San Francisco i byli zainteresowani zatrudnieniem Maksa. Pojechał do miasta, żeby odwiedzić Matta Harrigana, znanego też jako „Cyfrowy Jezus”.

Harrigan, mając zaledwie 22 lata, był jednym z czterech białych kapeluszy, którzy zostali opisani w dużym artykule w „Forbesie” z zeszłego roku, i sprytnie korzystał ze swoich piętnastu minut sławy, aby zdobyć pieniądze na rozkręcenie biznesu: profesjonalnej firmy hakerskiej w dzielnicy finansowej San Francisco.

Pomysł był prosty: korporacje będą płacić jego firmie Microcosm Computer Resources za poddawanie ich sieci prawdziwym hakerskim atakom, kończą-

cym się szczegółowym raportem na temat mocnych i słabych stron zabezpieczenia klienta. Biznes „testów penetracyjnych” - jak to nazywano - był zdominowany przez wielką piątkę firm konsultingowych, ale Harrigan już zdobył

klientów, przyznając się do tego, czego żadna z tych firma nie mogła otwarcie powiedzieć: mianowicie, że jego doświadczenie pochodzi z prawdziwego hakowania i że zatrudniał bez problemu innych byłych hakerów.

39

MCR będzie sobie liczyć od 300 do 400 dolarów za godzinę, wyjaśniał Harrigan. Max będzie pracował jako podwykonawca, biorąc od 100 do 150 dolarów. Wszystko za

robienie dwóch rzeczy, które lubił najbardziej na świecie: hakowanie i pisanie raportów.

Znalazł swoją niszę. Okazało się, że jednostronność jego umysłu czyniła go idealnym kandydatem do przeprowadzania testów penetracyjnych: był odporny na frustrację, dobijał się do sieci klienta całymi godzinami, nieustannie zmieniając kierunek natarcia, dopóki nie znalazł właściwej drogi.

Kiedy Max zaczął dobrze zarabiać w MCR, Kimi porzuciła pracę baristy i znalazła bardziej satysfakcjonujące zajęcie, ucząc autystyczne dzieci. Para przeprowadziła się z ciasnego mieszkania w Mountain View do dwupoziomo-wego mieszkania w San Jose. W marcu pobrali się w kościele na kampusie w Lakewood w stanie Waszyngton, gdzie mieszkała rodzina Kimi.

Tim Spencer i większość spośród Głodnych Programistów przyjechali do Waszyngtonu, by zobaczyć ślub swego trudnego dziecka. Na uroczystość przybyli rodzice Maksa, jego siostra, rodzina Kimi, grupa przyjaciół i dalsi krewni. Max był we fraku i miał szeroki uśmiech, Kimi rozpromieniona w białej ślubnej sukni i welonie. Otoczeni rodziną i ukochanymi przyjaciółmi, stanowili idealną jak z obrazka parę rozpoczynającą wspólne życie.

Pozowali do zdjęcia na zewnątrz: ojciec Kimi, żołnierz, stał dumnie w swym galowym mundurze, a jej matka w tradycyjnym koreańskim stroju *han-bok.* U boku swoich rodziców Max promieniał przed obiektywem, kiedy nad północno-zachodnim Pacyfikiem burzowe chmury zbierały się na niebie.

Minęły zaledwie trzy lata od chwili, gdy wyszedł na wolność, i teraz miał

wszystko - oddaną żonę, obiecującą karierę hakera w białym kapeluszu, ładny dom. W ciągu kilku tygodni to wszystko straci.

ROZDZIAŁ 5

Cyberwojna!

Po powrocie do domu w San Francisco czekała na Maksa pokusa zapisana w komputerowym kodzie.

```
bcopy(fname, anbuf, alen = (char *)*cpp - fname);
```

Była to jedna z 9000 linii tworzących Berkeley Internet Name Domain (BIND), stara belka stropowa w architekturze Internetu, równie ważna jak ruter czy kabel światłowodowy. Rozwinięty we wczesnych latach osiemdziesiątych dzięki grantowi z Pentagons Defense Advanced Research Projects Agency (DARPA) BIND wprowadził do użytku skalowalny Domain Name System, rodzaj rozproszonej książki telefonicznej, która przekłada sekwencje takie jak Yahoo.com - zrozumiałe dla ludzi, na numeryczne adresy - zrozumiałe dla sieci. Bez BIND lub jednego z konkurencyjnych programów, które powstały później, dostawalibyśmy nasze informacje online z 157.166.226.25 zamiast z CNN.com i odwiedzali 74.125.67.100, żeby używać wyszukiwarki Google’a.

BIND był jedną z innowacji, które sprawiły, że gwałtowny rozwój Internetu stał się możliwy. Zastąpiła ona prymitywny mechanizm, który nie mógł się 41

rozwijać wraz z siecią, niemniej w latach dziewięćdziesiątych był to także jeden z

odziedziczonych programów powodujących największe problemy, jeśli chodzi o bezpieczeństwo Internetu. Ten kod był produktem mniej skompliko-wanej epoki, kiedy dostęp do sieci był ograniczony i nie istniało zbyt wiele zagrożeń. Teraz hakerzy sondowali jego głębiny, odkrywając najwidoczniej nieskończoną liczbę dziur w zabezpieczeniach.

Najwyżsi kapłani wśród specjalistów od sieci powołali Internet Software Consortium, mianowali siebie strażnikami kodu i zaczęli z furią go zmieniać.

Ale w międzyczasie najbardziej nowoczesne, wyrafinowane sieci na świecie z błyskotliwymi nowymi serwerami i superkomputerami działały na bazie pełne-go błędów programu z innej epoki.

W 1998 roku eksperci od bezpieczeństwa odkryli najnowszy błąd w kodzie.

Skurczył się do tej jednej linii. Przyjmował zapytania z Internetu, tak jak powinien, i kopiował je bajt po bajcie do czasowego bufora „anbuf" w pamięci serwera. Nie sprawdzał jednak właściwie rozmiaru przyjmowanych danych. W

rezultacie haker mógł z premedytacją przesłać wydłużone zapytanie do serwera BIND, zalać bufor i rozlać dane po całej pamięci komputera jak ropę z tankow-ca Exxon Valdez.

Atak przeprowadzony przypadkowo mógł sprawić, że program przestanie działać, ale haker mógł świadomie spowodować coś znacznie gorszego. Mógł

wypełnić bufor swym małym fragmentem wykonywalnego kodu komputerowego, a następnie kontynuować podróż, przez cały czas drepcąc ostrożnie na szczyt pamięci programu, gdzie znajduje się specjalna przestrzeń do krótko-terminowego przechowywania, zwana „stosem".

Procesor przechowuje w nim zapisy wszystkich wykonywanych operacji -

za każdym razem kiedy program kieruje się ku podprogramowi, procesor przesuwa jego obecny adres pamięci do stosu jak zakładkę. Dzięki temu wie, gdzie ma wrócić, gdy zadanie zostanie wykonane.

Kiedy haker pojawi się w stosie, może zmienić ostatni powracający adres na lokację swego własnego złośliwego ładunku. Gdy komputer wykona już 42

bieżące zadania, powraca nie tam, gdzie zaczął, ale do instrukcji hakera - a ponieważ BIND działa pod wszechmogącym administracyjnym „źródłowym" kontem, dzieje się to też w przypadku kodu atakującego. Komputer znajduje się teraz pod kontrolą hakera.

Dwa tygodnie po ślubie Maksa i Kimi założona przez rząd Computer Emergency Response Team (CERT) na Carnegie Mellon University - prowadząca coś w rodzaju Emergency Broadcast System dla luk w systemie bezpieczeń-

stwa - podniosła alarm z powodu błędu BIND, razem z metodą szybkiego na-prawienia go: dwiema dodatkowymi liniami kodu komputerowego, które odrzucały zbyt długie zapytania. Ale CERT zignorował zasadniczy błąd, skupia-jąc się w swym ostrzeżeniu na dwu innych słabych punktach BIND, które nie groziły poważnymi konsekwencjami. W rezultacie nie każdy docenił powagę sytuacji.

Max doskonale ją rozumiał.

Przeczytał radę CERT-u z zaskoczeniem. BIND był standardowo instalowany na Linuksie i funkcjonował na serwerach korporacyjnych, dostawców usług internetowych oraz sieci non profit, edukacyjnych i wojskowych. Był

wszędzie. Podobnie jak wadliwa linia kodu. Jedyne, co powstrzymywało go-rączkę ataków, to to, że nie istniał jeszcze program pozwalający na wykorzy-stywanie luk w systemie bezpieczeństwa. Ale tylko do czasu.

18 maja exploit rzeczywiście pojawił się na Rootshell.com, stronie poświę-

conej informacjom o bezpieczeństwie komputerowym. Max podniósł słuchawkę i zadzwonił do domu swojego opiekuna z FBI Chrisa Beesona. Sytuacja jest poważna, wyjaśnił. Każdy, kto nie zainstalował łatki BIND, mógł być teraz zhakowany przez pierwszego lepszego skryptowego dzieciaka zdolnego do ściągnięcia programu i wpisania komendy.

Doświadczenie pokazywało, że szczególnie narażone na ataki były komputery rządowe. Zaledwie miesiąc wcześniej mniej groźny robak w systemie ope-racyjnym Sun Solaris doprowadził do hakera włamującego się do komputerów w dziesiątkach baz wojskowych USA, co zastępca sekretarza do spraw 43

obrony nazwał „najbardziej jak dotąd systematycznym i zorganizowanym atakiem" na amerykański system obrony. Atak ten wywołał pełny cybernetyczny fałszywy alarm: Pentagon nazwał go „Solar Sunrise" i uznał, że głównym po-dejrzanym jest Saddam Husajn, dopóki śledczy nie znaleźli prawdziwego wi-nowajcy - młodego izraelskiego hakera, który zrobił to dla zabawy.

Tego dnia Max zadzwonił do Beesona jeszcze raz, kiedy grupa hakerów znanych jako ADM wypuściła uzbrojoną wersję exploita BIND przeznaczoną do losowego skanowania Internetu w poszukiwaniu niezabezpieczonych serwerów, aby włamywać się do nich, instalować swoje oprogramowanie i używać świeżo zainfekowanych komputerów jako platformy dla kolejnych skanów i włamań. Teraz było już pewne, że ktoś chciał opanować cały Internet. Pytanie tylko kto.

Max odłożył słuchawkę i zamyślił się. *Ktoś* to zrobi…

O swoim planie opowiedział żonie chłopięcym, podekscytowanym tonem.

Napisze swój własny program atakujący BIND. Jego wersja wypełni luki wszędzie, gdzie tylko je znajdzie; to będzie jak wysłanie sterylnych muszek owocówek, aby powstrzymać zarazę. Ograniczy swój atak do celów najbardziej potrzebujących unowocześnienia: systemu bezpieczeństwa armii amerykań-

skiej i cywilnych stron rządowych.

- Nie daj się złapać - rzuciła Kimi, która wiedziała już, że nie należy spierać się z Maksem, kiedy jest całkowicie opętany jakimś pomysłem.

Max walczył z dwoistą naturą swej osobowości: żonaty profesjonalista za-korzeniony w otaczającym go świecie i impulsywne dziecko kuszone zachętą do psoty. Dziecko zwyciężyło. Usiadł przed klawiaturą i wpadł w szał programowania.

Jego kod będzie operował w trzech bardzo krótkich stadiach. Rozpocznie się od

zarzucenia wirtualnego haka abordażowego przez lukę w BIND, wykonującego komendy, które zmuszą maszynę do sięgnięcia do Internetu i ścią-

gnięcia dwustutrzydziestobajtowego skryptu. Ten skrypt z kolei połączy go 44

z innym hostem, zinfiltrowanym przez Maksa, z którego ściągnie on wielki pakiet zła zwany rootkitem.

Rootkit to paczka standardowych systemowych programów, które zostały uszkodzone, by w sekrecie służyć hakerowi. Nowy program logowania działa jak prawdziwy, ale teraz posiada tylne wejście, przez które intruz może ponownie dostać się do komputera. Program nadal pozwala użytkownikom zmienić hasło, ale również dyskretnie zapisuje i przechowuje nowe hasło w miejscu, z którego można je później wyciągnąć. Nowa lista programów zawiera treść katalogu, tak jak powinna, ale stara się ukryć wszystkie pliki będące częścią rootkitu.

Kiedy już rootkit będzie na miejscu, kod Maksa uzyska to, czego nie udało się zrobić rządowi: zapgrejduje znakowany komputer do ostatniej wersji BIND, zamykając lukę w systemie bezpieczeństwa, przez którą wszedł. Komputer będzie teraz zabezpieczony przed przyszłymi atakami, ale Max intruz w dobrej wierze nadal będzie mógł wchodzić do systemu, kiedy zechce. W ten sposób jednocześnie naprawiał błąd i wykorzystywał go, był równocześnie czarnym i białym kapeluszem.

Za każdym razem atak będzie trwał zaledwie kilka minut. Wystarczy zarzu-cenie haka, ściągnięcie skryptu, rootkitu i komputer jeszcze przed chwilą kontrolowany przez administratorów systemu należy do Maksa.

Max nadal był zajęty programowaniem, kiedy odezwało się od niego FBI, prosząc o pełny raport na temat luk w BIND. Federalni dostali szansę; kod Maksa będzie teraz mówił za niego. Wystarczyła mu chwila na włamanie się do kilku uniwersyteckich komputerów i użycie ich jako bazy, następnie 21

maja we wtorek wszedł do Internetu przez skradzione konto Verio… i wystartował.

Efekty były natychmiastowe i bardzo zadowalające. Kod haka abordażowego został zaprojektowany tak, by Max na swoim komputerze poza połączeniem przez Verio mógł obserwować, jak atak się rozszerza. Okienko Xterm wyska-kiwało na jego ekranie za każdym razem, kiedy zhakowane maszyny z całego 45

kraju wysyłały sygnał. Baza Sił Powietrznych w Brooks teraz należała do Maksa Visiona. Podobnie jak McChord, Tinker, Offutt, Scott, Maxwell, Kirtland, Keesler, Robins. Jego kod wdarł się na serwery sił powietrznych, komputery wojska, maszyny w biurze sekretarza stanu. Każdy z komputerów miał teraz tylne wejście, z którego Max mógł korzystać, kiedy tylko chciał.

Zapisywał wojenne podboje jak punkty w grze wideo. Kiedy jego kod wsunął się do przestrzeni internetowej marynarki, znalazł tam tak wiele niezabezpieczonych serwerów BIND, że strumień wyskakujących okienek zmienił się w rzekę. Jego własny komputer zmagał się z napięciem, aż w końcu padł.

Po lekkim podrasowaniu wystartował ponownie. Przez pięć dni Max był za-absorbowany swym rozrastającym się w cyberprzestrzeni imperium. Zignorował mail z FBI, które nadal

chciało dostać raport. „Gdzie to jest? - pytał agent Beeson - zadzwoń”.

Teraz, kiedy już mógł wejść do niemal każdej sieci, musiał przekonać się, co jeszcze może zrobić. Max testował swój exploit BIND na serwerach Id Software z Mesquite w Teksasie, firmy produkującej gry, która pracowała właśnie nad trzecią edycją niezwykle popularnej pierwszoosobowej strzelanki *Quake*.

Max kochał tego rodzaju gry. Był w sieci we flashu i po pewnym czasie wynurzył się ze swą zdobyczą. Oznajmił Kimi, że właśnie uzyskał kod źródłowy -

wirtualną kopię - *Quake III*, najbardziej oczekiwanej gry roku.

Na Kimi nie zrobiło to większego wrażenia: „Czy możesz to zwrócić?”.

Max wkrótce uświadomił sobie, że jego ataki nie pozostały niezauważone.

Naukowiec Vern Paxson z Lawrence Berkeley National Laboratory dostrzegł

skanowanie Maksa podczas korzystania z systemu, który sam stworzył, zwanego BRO od Big Brother. BRO stanowiło eksperyment w stosunkowo nowym rodzaju środków bezpieczeństwa zwanym systemem wykrywania włamań -

cybernetyczny alarm antywłamaniowy, którego jedyną funkcją było spokojne siedzenie w sieci i dokładne analizowanie całego ruchu, by znaleźć podejrzaną aktywność i zaalarmować administratorów, kiedy dostrzeże coś niepokojącego.

Paxson sporządził wyczerpujący raport o atakach na CERT. Max przechwycił go i był pod wrażeniem. Badacz nie tylko wykrył jego atak, ale stworzył

listę serwerów, które kod zaatakował przez sieć Lawrence Berkeley - Max używał tej sieci jako jednego z drugorzędnych punktów wypadowych. Wysłał

Paxsonowi anonimową notę z konta laboratorium.

Vern,

przykro mi, że sprawiłem Ci kłopot, ale ja na własną rękę załatałem NAJWIĘKSZE DZIURY W SYSTEMIE BEZPIECZEŃSTWA w wielu Twoich systemach. Przyznaję, że były nowe luki, ale zabezpieczone hasłem, a ja nigdy nie wyrządziłbym szkody cudzemu systemowi komputerowemu. Gdybym nie przeprowadził tego ataku, zrobiłby to ktoś in-ny i źle by się to skończyło. Te dzieciaki wszędzie zostawiają warezy i IRC BS, kiedy mają humory. Porażka.

Możesz nie doceniać tego, co zrobiłem, ale dla mnie było to najwyż-

szym dobrem. Opuszczam wszystkie hosty na liście, którą sporządzi-

łeś… Nie dotykam tych systemów, odkąd wiem, że odwróciłeś je do CERT-u. CERT powinien zatrudnić ludzi posiadających moje umiejęt-ności. Oczywiście gdybym był opłacany, nigdy nie zostawiałbym rootkitów ani czegoś podobnego.

Bardzo sprytnie, nie? Tak. To było uderzenie. Opanowywanie setek, nie, tysięcy systemów, ze świadomością, że przy okazji NAPRAWIASZ

je.

Nie mam zamiaru nigdy więcej robić podobnych rzeczy. Teraz masz moje narzędzia. To mnie wkurza…

Hm. Tak czy inaczej, po prostu nie chcę, by się to wydarzyło ponownie, więc daję sobie z tym spokój…

„Cracker”

47

Tym listem Max zakończył swój pięciodniowy atak na instytucje rządowe, zostawiając za sobą więcej spenetrowanych systemów, niż mógł policzyć. Był

zadowolony, że uczynił Internet bezpieczniejszym miejscem, a tysiące komputerów, które były narażone na atak każdego hakera na świecie, teraz mogły ulec tylko jednemu: Maksowi Visionowi.

Max natychmiast dołączył do nowego, bardziej społecznie akceptowanego projektu: będzie pisał aplikacje sieciowe, które pozwolą każdemu w Internecie zażądać automatycznego skanowania ich sieci w czasie rzeczywistym, żeby sprawdzić, czy są narażone na atak na BIND. Stworzył również przyjazną wersję programu, którego używał do zakończonych właśnie ataków. Podobnie jak wcześniej, będzie skanował rządowe i wojskowe sieci, ale zamiast włamywać się do podatnych komputerów, automatycznie wyśle mail z ostrzeżeniem do administratorów. Tym razem nie będzie potrzeby ukrywania się pod znakowa-nym kontem internetowym. Obydwa serwisy będą funkcjonowały na całkiem nowej publicznej stronie: Whitehats.com.

Po dwóch dobach pracy Max tkwił po uszy w nowym, legalnym projekcie hakerskim, kiedy dostał ponownie maila od Beesona. „Co się stało? Miałeś wysłać maila”.

Max nie mógł wyjaśnić przyjacielowi z FBI, że był zajęty organizowaniem jednego z największych w historii włamań do rządowych komputerów. Ograniczył się więc do przedstawienia nowego projektu. „Prawie skończyłem tworzenie ogólnodostępnego skanera zagrożeń i strony, z której można pobrać łatkę -

ale pewne części nie są jeszcze gotowe do wypuszczenia” - odpisał.

„A, i tu jest program robaka ADM - dodał. - Nie sadzę, by się bardzo roz-przestrzenił”.

ROZDZIAŁ 6

Tęsknię za przestępstwem

Po południu 2 czerwca Max otworzył drzwi swego mieszkania w San Jose i ujrzał Chrisa Beesona. Od razu zorientował się, że ma kłopoty: oprócz Beesona przyszło jeszcze trzech innych facetów w garniturach, w tym Pete Trahon, z pewnością przełożony Beesona, szef grupy do spraw przestępczości komputerowej.

Miesiąc po ataku na BIND był dla Maksa czasem wypełnionym pracą. Wystartował z Whitehats.com i był to natychmiastowy sukces w świecie bezpieczeństwa komputerowego. Oprócz tego, że strona służyła za bazę jego narzę-

dzia do skanowania, można było na niej znaleźć także najnowsze porady CERT-u i linki do łatek software’owych BIND, jak również teksty, które Max napisał, analizując robaka ADM przejrzyście i ze spostrzegawczością zdradza-jącą oko prawdziwego znawcy. Nikt

w całej społeczności nie podejrzewał, że Max Vision, wschodząca gwiazda Whitahats.com, osobiście dostarczy najlepszego przykładu tego, jak poważny charakter ma luka w bezpieczeństwie BIND.

Kontynuował także pisanie raportów dla FBI. Po ostatnim Beeson zaczął

wysyłać do niego maile, żeby zorganizować zwykłe spotkanie poświęcone 49

ostatnim odkryciom Maksa. „Co powiesz na spotkanie u ciebie? - napisał Beeson. - Wiem, że mam tu gdzieś twój adres".

Teraz, kiedy już był na schodach do mieszkania, wyjaśnił, po co naprawdę przyszli. Wiedział wszystko o ataku Maksa na Pentagon. Jeden z ludzi, którzy z nim byli, młody śledczy sił powietrznych z Waszyngtonu nazwiskiem Eric Smith, odkrył, że ślady włamania BIND prowadzą do domu Maksa. Beeson miał nakaz rewizji.

Max wpuścił ich, już na dzień dobry przepraszając. Wyjaśnił, że chciał tylko pomóc.

Rozmawiali w przyjacielskim tonie. Max, szczęśliwy z powodu publiczno-

ści, stał się ekspansywny, wyjaśniając meandry swego ataku i słuchając z zainteresowaniem Smitha opowiadającego o tym, jak wyśledził go za sprawą okienek sygnalizujących opanowanie atakowanego systemu. Informacje szły do konta Verio i dostawca Internetu, otrzymawszy wezwanie sądowe, ujawnił

numer telefoniczny Maksa. To nie było trudne. Max był przekonany, że robił

coś dobrego dla Internetu, więc nie troszczył się o zacieranie śladów.

Na pytanie, czy ktokolwiek wiedział o jego zamiarach, Max odpowiedział, że włączony był w to jego szef Mart Harrigan - Cyfrowy Jezus. Sam nie zrezygnował całkowicie z hakowania, powiedział Max, dodając, że firma Harrigana właśnie dostała kontrakt z Agencji Bezpieczeństwa Narodowego*.

* Zaangażowanie Harrigana jest przedmiotem sporu. Max twierdził, że planował atak na BIND z Harriganem w biurze MCR i że Harrigan napisał program, który stworzył listę docelo-wych komputerów rządowych. Harrigan twierdzi, że nie był w to zaangażowany, ale wiedział, co Max chce zrobić.

Na żądania agentów Max napisał zeznanie. „Moim motywem było wyłącznie sprawdzenie, czy to się da zrobić. Wiem, że to mnie nie usprawiedliwia, i wierzcie mi, przykro mi z tego powodu, ale to prawda".

Kimi wróciła ze szkoły i zastała federalnych ciągle jeszcze przetrząsających mieszkanie. Agenci jak pasące się łanie równocześnie podnieśli głowy w kierunku dziewczyny, szybko ocenili ją jako niegroźną i bez słowa powrócili 50

do pracy. W końcu wyszli, zabierając z sobą cały sprzęt komputerowy.

Drzwi się zamknęły, zostawiając nowożeńców z tym, co pozostało z ich domu. Max zaczął przepraszać. Kimi przerwała mu ze złością.

- Powiedziałam ci, żebyś nie dał się złapać!

Agenci FBI dostrzegli szansę w przestępstwie Maksa. Trahon i Beeson wrócili do jego domu i przedstawili byłemu sprzymierzeńcowi sytuację. Jeśli liczy na pobłażliwość, musi

pracować dla nich - pisanie raportów nie miało już na to wpływu.

Chętny do zadośćuczynienia i zdeterminowany, by ratować życie i karierę, Max nie poprosił o żadne pisemne potwierdzenie tej umowy. Przyjął na wiarę, że jeśli on pomoże agentom FBI, oni pomogą jemu.

Dwa tygodnie później dostał swoje pierwsze zadanie. Gang phreakerów właśnie opanował system telefoniczny sieciowej firmy 3Com i używał go do prywatnych telekonferencji. Beeson i Trahon byli w stanie dostać się do nielegalnej linii czatowej, ale nie mieli szans wmieszać się w tłum hakerów i uzyskać jakichkolwiek wartościowych informacji. Max przestudiował najnowsze metody phone phreakingu, a następnie połączył się z systemem z terenowego biura FBI, podczas gdy biuro nagrywało rozmowę.

Rzucając kilka imion hakerów, których znał, i wykorzystując własną fachową wiedzę, Max z łatwością przekonał telefonicznych hakerów, że jest jednym z nich. Otworzyli się i ujawnili, że są międzynarodowym gangiem zło-

żonym z około 35 telefonicznych hakerów, zwanym DarkCYDE, mieszkają-

cych głównie w Wielkiej Brytanii i Irlandii. DarkCYDE mieli ambicję „zjednoczyć phreakerów i hakerów z całego świata w jedną wielką cyfrową armię", jak głosił chełpliwy manifest grupy. Ale w gruncie rzeczy byli po prostu dzie-ciakami bawiącymi się telefonem, jak robił to Max w liceum. Po tym telefonie Beeson poprosił go, by trzymał się blisko gangu. Max czatował z jego członkami na IRC-u i przekazywał raporty swoim opiekunom.

51

Tydzień później zadowoleni z jego pracy agenci wezwali go do siedziby federalnych w San Francisco, żeby przedstawić mu nowe zadanie. Tym razem miał jechać do Vegas.

Max wodził wzrokiem ponad kompletem przybranych lnianymi obrusami kar-cianych stolików w krzykliwym holu Plaza Hotel and Casino. Dziesiątki młodych mężczyzn w T-shirtach i szortach lub dżinsach - hakerskich mundurach -

przycupniętych nad rzędem komputerów lub stojących z boku od czasu do czasu wskazywało coś na ekranie.

Czy może być coś dziwniejszego od spędzania weekendu w mieście grze-chu, tłukąc w klawiaturę niczym jakiś robot, z daleka od basenu, drinków i imprez? Hakerzy uczestniczyli w zażartej drużynowej rywalizacji, mającej na celu spenetrowanie kilku komputerów pospiesznie połączonych w sieć. Pierwsza drużyna, która umieści wirtualny znacznik w jednym z celów, będzie miała prawo do 250 dolarów nagrody i przechwalania się - z dodatkowymi punktami za hakowanie innych graczy. Pod palcami hakerów powstawały nowe fortele, z wirtualnych arsenałów wyciągano trzymane dotąd w ukryciu chwyty.

Na Def Conie, największej światowej konwencji hakerów, gra w „zdobądź

flagę" co roku budziła takie same emocje jak partia szachów Fischera ze Spas-skim.

Na Kimi to wszystko nie zrobiło wrażenia, ale Max był w siódmym niebie.

Na podłodze rozstawiono mnóstwo stolików ze starym oprzyrządowaniem

komputerowym, dziwną elektroniką, wytrychami, T-shirtami, książkami i eg-zemplarzami „2600: The Hacker Quarterly”. Max zauważył Eliasa Levy’ego, sławnego „białego kapelusza”, i wskazał go Kimi. Levy, znany też jako Aleph One, był moderatorem listy mailingowej Bugtraq - „New York Timesa” w świecie komputerowego bezpieczeństwa - i autorem podstawowego artykułu na temat przepełnienia bufora, zwanego „Miażdżenie stosu dla zabawy i zarobku”, 52

który pojawił się we „Phracku”. Max nie miał śmiałości, by zbliżyć się do tej osobistości. Cóż mógłby Levy’emu powiedzieć?

Max nie był oczywiście jedynym agentem sprawiedliwości na Def Conie.

Od skromnych początków tej imprezy w 1992 roku jako jednorazowej konferencji zwołanej przez dawnych phone phreaków Def Con rozwinął się w legendarny zjazd, który ściągał prawie 2000 hakerów, profesjonalistów zajmują-

cych się bezpieczeństwem komputerowym i włóczęgów z całego świata. Przy-bywali na imprezę osobiście, z przyjaciółmi, których poznali online, wygłaszali wykłady i słuchali innych, kupowali, sprzedawali i upijali się na całonocnych balangach w pokojach hotelowych.

Def Con był tak oczywistym celem dla policji, że organizator Jeff „Dark Tangent” Moss wymyślił nową grę zwaną „Znajdź federalnego”. Haker, który uznał, że rozpoznał tajniaka w tłumie, mógł go wskazać, udowodnić, że ma rację, i zabrać do domu T-shirt z napisem „Znalazłem federalnego na Def Conie”. Często podejrzany agent po prostu poddawał się i grzecznie pokazywał

odznakę, dając hakerowi łatwe zwycięstwo.

Misja Maksa miała szeroki zakres. Trahon i Beeson chcieli, by zaprzyjaźnił

się z hakerami i spróbował poznać ich prawdziwe nazwiska, a potem zwabił

ich do wymiany publicznego PGP - klucza od szyfrów, którego dbający o własne bezpieczeństwo geekowie używają niczym wosku do pieczętowania, by zaszyfrować i podpisywać maile. Max w duchu buntował się przeciw temu, co miał robić. Pisanie raportów dla FBI to jedno, nie miał żadnych rozterek, ro-biąc porządek z phreakerami z DarkCYDE, którzy byli zbyt młodzi, by wpaść w poważne problemy. Ale to jego zadanie śmierdziało kablowaniem. Osobista lojalność była zapisana głęboko w oprogramowaniu Maksa i wystarczyło jedno spojrzenie na tłum uczestników Def Conu, by dostrzec, że jest wśród swoich.

Wielu hakerów niechętnie rezygnowało z dziecinnych zabaw na rzecz legalnej pracy w dotcomach lub zakładało firmy zajmujące się bezpieczeństwem komputerowym. Stawali się białymi kapeluszami, jak Max. Popularny na 53

konwencji T-shirt z napisem „Tęsknię za przestępstwem” oddawał powszechny nastrój.

Max zbagatelizował rozporządzenie FBI i zaczął brać udział w imprezach i dyskusjach. Na liście była w tym roku najbardziej oczekiwana premiera oprogramowania stworzonego przez Cult of the Dead Cow. The cDc byli gwiazdami rocka hakerskiego świata - dosłownie: grali muzykę i nasycali swoje wystą-

pienia na konferencjach przesadną teatralnością, która uczyniła z nich ulubień-

ców mediów. Na tym Def Conie grupa wypuszczała Back Orifice, wyrafinowany zdalny program na komputery pracujące na Windowsie. Jeśli byłeś w stanie kogoś skłonić do uruchomienia Back Orifice, mogłeś uzyskać dostęp do jego plików, zobaczyć, co ma na monitorze, a nawet patrzeć przez jego kamerę internetową. Wszystko po to, by wprawić w zakłopotanie Microsoft ze względu na słabe zabezpieczenia Windows 98.

W czasie prezentacji Back Orifice tłum niemal wpadł w ekstazę i Max stwierdził, że ta atmosfera jest zaraźliwa. Ale bardziej interesujący ze względ-

dów praktycznych był dla niego wykład na temat prawnych aspektów hakingu, który prowadziła adwokat z San Francisco Jennifer Granick. Zaczęła swą prezentację od opisu ostatnich przełomowych dochodzeń w sprawie hakera z Bay Area Carlosa Salgado juniora, trzydziestoszścioletniego fachowca od naprawiania komputerów, który w większym stopniu niż ktokolwiek inny uosabiał

przyszłość przestępczości komputerowej.

Ze swego pokoju w domu rodziców w Daly City, jakieś dziesięć kilometrów na południe od San Francisco, Salgado włamał się do dużej firmy technologicznej i ukradł bazę danych z 80 000 numerów kart kredytowych z nazwiskami, kodami pocztowymi i datami wygaśnięcia. Numery kart kredytowych wy-kradano już wcześniej, ale to, co Salgado zrobił potem, zapewniło mu miejsce w podręcznikach historii cyfrowej przestępczości. Używając nicka „Smak”, pojawił się w czat roomie #carding na IRC-u i wystawił całą listę na sprzedaż.

To było jak sprzedawanie boeinga 747 na pchlim targu. W tym czasie oszustwa online związane z kartami kredytowymi stanowiły margines zajmowany przez dzieciaki i drobnych przestępców, którzy ledwie wyszli poza osiągnięcia poprzednich pokoleń oszustów, łowiących rachunki ze śmietników za centrami handlowymi. Ich typowe transakcje były jednocyfrowe, a porady, których sobie udzielali, pełne mitów i idiotyzmów. Większość rozmów prowadzono w otwartym kanale, gdzie każdy przedstawiciel prawa mógł się zalogować i obserwować ich przebieg - jedynym zabezpieczeniem carderów było to, że nikomu nie chciało się tego robić.

Co ciekawe, Salgado znalazł przyszłego kupca na #cardingu. Był nim student informatyki z San Diego, który utrzymywał się na uczelni, fałszując karty kredytowe z wykorzystaniem numerów kont podkradanych z wyciągów rachunków wysyłanych pocztą. Ten student miał kontakty z mafią, która, jak uważał, kupiłaby całą skradzioną bazę danych Smaka za sześciocyfrową sumę.

Transakcja nie doszła do skutku, ponieważ Salgado, chcąc trochę dokładniej sprawdzić kontrahenta, zhakował jego ISP i pobuszował w jego plikach. Kiedy student się o tym dowiedział, wkurzył się i w tajemnicy zaczął współpracować z FBI. Rankiem 21 maja 1997 roku Salgado pojawił się na spotkaniu w palarni na międzynarodowym lotnisku w San Francisco, gdzie miał wymienić CD-ROM z bazą danych na walizkę wypakowaną 260 000 dolarów w gotówce.

Zamiast tego został aresztowany przez policjantów z wydziału przestępstw

komputerowych.

Nieudana intryga otworzyła FBI oczy: Salgado był pierwszym z nowego gatunku zorientowanych na zysk hakerów i stwarzał zagrożenie dla przyszłego e-handlu. Badania pokazały, że użytkownicy sieci obawiali się przesyłania numerów kart kredytowych przez elektroniczny eter - to była rzecz, która w pierwszym rzędzie powstrzymywała ich przed zakupami w Internecie. Teraz po latach starań o zdobycie zaufania konsumentów i nagrodzeniu wiary inwestorów firmy zajmujące się sprzedażą w Internecie ruszały na podbój Wall Street.

55

Niecałe dwa tygodnie przed aresztowaniem Salgado Amazon.com wystartował

z długo oczekiwaną pierwszą ofertą publiczną i zakończył dzień z 54 milionami dolarów zysku.

Pierwsza oferta publiczna Salgado była znacznie wyższa; firmy oferujące karty kredytowe określiły całkowity limit wydawanych pieniędzy na jego 80

000 kart na ponad miliard dolarów - 931568 535, jeśli odliczyć nieuregulowane należności prawowitych właścicieli. Jedyną rzeczą, której mu brakowało, był

NASDAQ, żeby móc sprzedawać akcje. Od kiedy przestępcze podziemie poznało ten sekret, stał on się osobnym przemysłem.

Kiedy tylko Salgado został aresztowany, przyznał się FBI do wszystkiego.

Było to, jak powiedziała Granick hakerom na Def Conie, wielkim błędem.

Mimo współpracy Salgado w tym samym roku został skazany na trzydzieści miesięcy więzienia.

- Teraz FBI chciało, żebym wam powiedziała, że pan Salgado postąpił

słusznie, składając zeznania - tu zrobiła przerwę - ale to bzdura.

- Po prostu powiedz nie! - wyrzuciła z siebie, a w reakcji na jej słowa ze strony publiczności wezbrała fala radosnych okrzyków i gwizdów. - Nie ma sensu rozmawiać z gliniarzem… Jeśli macie zamiar współpracować, róbcie to po konsultacji z adwokatem i ustaleniu warunków. Po co dawać im informacje za darmo?

Z tyłu sali Kimi dała Maksowi kuksańca w żebro. Zrobił wszystko, czego Granick radziła komputerowym włamywaczom unikać. Wszystko.

Po raz kolejny zastanawiał się na swym układem z federalnymi.

„Musimy zmienić parę rzeczy w naszej umowie”.

Max mógł wyczuć frustrację promieniującą z jego monitora, kiedy czytał

ostatnią wiadomość od Chrisa Beesona. Wrócił z Def Conu z pustymi rękami, a następnie opuścił spotkanie w budynku federalnych, na którym miał otrzymać 56

nowe zadanie. Wkurzyło to Pete’a Trahona, szefa Beesona. W dalszej części maila Beeson ostrzegł Maksa przed ponurymi konsekwencjami kontynuowania bumelki. „Każde następne niepojawienie się na spotkaniu bez wyjątkowych przyczyn będzie uznane za brak

współpracy z twojej strony. Jeśli nie będziesz chciał współpracować, będziemy MUSIELI podjąć odpowiednie działania.

Pete spotyka się z prokuratorem w TWOJEJ sprawie w poniedziałek. Chce cię widzieć w naszym biurze niezwłocznie, punktualnie o 10.00 rano w PONIEDZIAŁEK 17.08.98. W przyszłym tygodniu nie mam czasu (dlatego chcę się z tobą zobaczyć wcześniej), tak więc będziesz się musiał spotykać bezpośrednio z Pete'em".

Tym razem Max się pojawił. Trahon wyjaśnił, że zaczął się interesować szefem Maksa w MCR Mattem Harriganem. Agent był poważnie zaniepokojony pomysłem prowadzenia przez hakera firmy zajmującej się bezpieczeństwem komputerowym, w której pracowali inni hakerzy, tacy jak Max, i współzawod-niczącej o kontrakt z NSA. Jeśli Max chciał usatysfakcjonować FBI, powinien skłonić Harrigana do przyznania, że nadal jest hakerem i odgrywał swoją rolę w ataku BIND przeprowadzonym przez Maksa.

Agent dał mu nowy formularz do podpisania. Była to pisemna zgoda na noszenie przy sobie podsłuchu. Trahon wręczył mu policyjne urządzenie do na-grywania wyglądające dla niepoznaki jak pager.

W drodze do domu Max zastanawiał się nad sytuacją. Harrigan był przyjacielem i kolegą po fachu. Teraz FBI domagało się od Maksa, żeby dokonał

ostatecznej zdrady - by stał się prawdziwym Judaszem dla Cyfrowego Jezusa.

Następnego dnia bez pluskwy FBI spotkał się z Harriganem w małej restauracji u Denny'ego w San Jose. Jego oczy skanowały innych jedzących i parking za oknem. Federalni mogli być wszędzie.

Wyciągnął kawałek papieru i przesunął go wzdłuż stolika. „Tu jest wszystko, co się dzieje…"

Po tym spotkaniu zadzwonił do Jennifer Granick, która zgodziła się go reprezentować - dostał jej wizytówkę po imprezie na Def Conie.

57

Kiedy Beeson i Trahon dowiedzieli się, że znalazł sobie adwokata, bez chwili wahania zerwali z nim współpracę. Granick zaczęła wydzwaniać do FBI i do biura prokuratora, żeby dowiedzieć się, co władza chce zrobić z jej nowym klientem. Trzy miesiące później dostała wreszcie odpowiedź od najlepszego rządowego prokuratora w Dolinie Krzemowej. Stany Zjednoczone nie były już zainteresowane współpracą z Maksem. Mógł się spodziewać, że wkrótce wróci do więzienia.

ROZDZIAŁ 7

Max Vision

Kiedy Max przestał być informatorem FBI, powrócił do pracy, budując reputację „białego kapelusza”, mimo że wisiał nad nim miecz Damoklesa w postaci federalnego aktu oskarżenia.

Słabość BIND i wynikający z niej sukces Whitehats.com pozwoliły mu na szybki start. Teraz zawiesił swój własny szyld jako konsultant do spraw bezpieczeństwa komputerowego, tworząc nową stronę, na której reklamował się jako haker do wynajęcia za 100 dolarów na godzinę lub za darmo dla grup non profit. Jego najlepszą rekomendacją było 100 procent sukcesu w testach penetracyjnych. Nigdy nie natrafił na sieć, do której nie mógłby się włamać.

To były piękne dni dla białych kapeluszy. Buntowniczy duch, jaki zrodził

ruch open source software, udzielił się ruchowi bezpieczeństwa komputerowego i nowy narybek absolwentów uniwersytetów i tych, którzy ich nie ukończyli, byłych i obecnych czarnych kapeluszy, wywracał konserwatywne przekonania, które zdominowały myślenie o bezpieczeństwie na całe dekady.

Najpierw do lamusa odeszła zasada, że luki w systemie bezpieczeństwa i metody ataku powinny być trzymane w tajemnicy przez kadrę zaufanych 59

i odpowiedzialnych dorosłych. Białe kapelusze nazywały te przekonania „bezpieczeństwem dzięki tajemnicy”. Nowe pokolenie wolało określenie „pełne otwarcie”. Dyskutowanie o problemach bezpieczeństwa w szerokim gronie nie tylko pomaga w ich naprawieniu, ale także rozwija wiedzę o bezpieczeństwie i hakowaniu jako całości. Trzymanie robaków w tajemnicy przynosiło korzyść tylko dwóm grupom: złym facetom, którzy je wykorzystywali, i sprzedawcom takim jak Microsoft, którzy woleli usunąć luki w bezpieczeństwie, nie przyznając się do własnych błędów.

Ruch pełnego otwarcia stworzył listę mailingową Bugtraq, na której hakerzy o dowolnym kolorze kapelusza byli zachęcani do wysyłania szczegółowych raportów o błędach w bezpieczeństwie, które znaleźli w oprogramowaniu. Jeśli mogli dostarczyć kod exploita - kod, który pokazywał błąd - tym lepiej. Preferowaną ścieżką pełnego otwarcia było wskazanie błędów producentowi oprogramowania i danie mu czasu na stworzenie łatki, zanim ujawniono błąd lub exploit na Bugtraqu. Ale nikt tu nie cenzurował postów i ludzie, którzy znaleźli bugi, bardzo często wrzucali nieznany wcześniej exploit na listę, co oznaczało, że trafiał on w ciągu kilku minut do tysięcy analityków bezpieczeństwa i hakerów. Ten manewr dawał niemal stuprocentową gwarancję, że firmy tworzące oprogramowanie zareagują błyskawicznie.

Bugtraq stwarzał hakerom możliwość popisania się swymi umiejętnościami eksperckimi bez łamania prawa. Ci, którzy ciągle jeszcze włamywali się do systemów, mieli przeciwko sobie pełną energii społeczność białych kapeluszy, uzbrojoną w rosnący arsenał obronnych narzędzi.

Pod koniec 1998 roku były pracownik cyberbezpieczeństwa w NSA Marty Roesch

stworzył jedno z najlepszych tego typu narzędzi. Pomyślał, że byłoby zabawnie zobaczyć, jakie przypadkowe ataki przepływały przez jego domowy modem w czasie, gdy był w pracy, i uruchomił sniffer znany jako Snort, a potem wypuścił go jako projekt open source.

60

Na pierwszy rzut oka Snort nie był niczym specjalnym - sniffer jest powszechnym narzędziem bezpieczeństwa, które obserwuje ruch w sieci i wrzuca go do pliku, by poddać analizie. Jednak miesiąc później Roesch zmienił swój program w pełny system wykrywania włamań (IDS - Intrusion Detection System), który zaalarmuje operatora, kiedy tylko spostrzeże w sieci ruch odpowiadający charakterystyce znanego ataku. Na rynku była pewna ilość IDS-ów, ale wszechstronność Snorta i jego licencja open source od razu spodobała się bia-

łym kapeluszom, którzy niczego tak nie kochali jak majsterkowania nowym narzędziem bezpieczeństwa. Programiści wolontariusze zajęli się dodatkowymi funkcjami programu.

Max był zafascynowany Snortem. To oprogramowanie było podobne do BRO, projektu laboratorium Lawrence Berkeley, który pomógł wywęszyć atak na BIND, i Max wiedział, że to może zmienić zasady gry w świecie bezpieczeństwa online. Teraz białe kapelusze mogły obserwować w czasie rzeczywistym każdego, kto próbował wykorzystać słabości dyskutowane na Bugtraqu czy gdzieś indziej. Snort był jak system wczesnego ostrzegania dla sieci, komputerowym odpowiednikiem sieci radarowej NORAD, która monitoruje amerykańską przestrzeń powietrzną. Brakowało mu tylko spójnej i aktualnej listy sygnatur ataków, tak by oprogramowanie wiedziało, czego ma szukać.

W ciągu kilku pierwszych miesięcy po wypuszczeniu Snorta niezorganizo-wany wyciek sygnatur stworzonych przez użytkowników osiągnął całkowitą liczbę około 200. W jedną bezsenną noc Max zwiększył tę liczbę o ponad drugie tyle, podbijając ją do 490 sygnatur. Część z nich była oryginalna, inne stanowiły poprawione wersje istniejących reguł bądź portów z popularnego ko-mercyjnego systemu Dragon IDS. Pisanie reguł oznaczało zidentyfikowanie unikalnych cech w ruchu w sieci, stworzonym przez konkretny atak, jak numer portu lub sekwencja bajtów. Na przykład wezwanie: alert udp any any - > $INTERNAL 31337 (msg: „BackOrificel-scan”; content:”|ce63 dld2 16e7 13cf38a5

a586|”;) - wykryło czarne kapelusze próbujące użyć złośliwego oprogramowania 61

Back Orifice stworzonego przez Cult of the Dead Cow, który zafascynował

tłum na Def Conie 6.0. Poinformowało ono Snorta, że nadchodzące połączenie to port 31337 z określoną sekwencją, a więc w sieciowym ruchu był ktoś, kto chciał wykorzystać tylne wejście.

Max postawił sygnaturę online jako pojedynczy plik na Whitehats.com, wymieniając garść innych geeków, którzy przyczynili się do jej powstania, i uwzględniając też Ghosta23 - własne *alter ego.* Później zmienił plik w rozwiniętą bazę danych i zaprosił innych ekspertów do stworzenia własnych reguł.

Nadał projektowi chwytliwą nazwę arachNIDS jako skrót od Advanced Reference Archive of Current Heuristics for Network Intrusion Detection Systems.

ArachNIDS stał się hitem i pomógł Snortowi wznieść się na nowy poziom popularności

wśród ludzi zajmujących się bezpieczeństwem komputerowym, dla których Max Vision stawał się gwiazdą. Gdy coraz więcej białych kapeluszy uczestniczyło w projekcie, stał się on odpowiednikiem bazy odcisków palców FBI w świecie komputerowego bezpieczeństwa, zdolnym do zidentyfikowania potencjalnie każdej znanej techniki ataku lub jej wariantów. Max, bazując na własnym sukcesie, pisał teksty analizujące internetowe robaki z tą samą wnikliwością spojrzenia, jaką wykazał przy robaku ADM. Zaczęły się również pojawiać propozycje z prasy branżowej, aby Max komentował ostatnie ataki hakerów.

W 1999 roku Max wszedł w inne obiecujące przedsięwzięcie wymierzone wyraźnie przeciw czarnym kapeluszom. Projekt Miodowej Sieci, jak je później nazwano, był dziełem byłego oficera amerykańskiej armii, który wykorzystał

swoje zainteresowanie taktykami bojowymi do stworzenia sieci „miodowych punktów" - komputerów-pułapek, których jedynym celem było dać się zhakować. Projekt Miodowej Sieci podłączy w tajemnicy sniffer do systemu i umie-

ści go bez zabezpieczenia w Internecie, niczym tajną agentkę wystrojoną w czółenka i minispódniczkę na rogu ulicy.

Kiedy haker namierzy miodowy punkt, każdy jego ruch będzie nagrywany i potem analizowany przez ekspertów zajmujących się bezpieczeństwem, a rezultaty ich badań zostaną udostępnione publicznie w myśl zasady całkowitego otwarcia. Max oddał się detektywistycznej pracy, rekonstruując przestępstwa na podstawie pakietu źródłowych danych i dokonując spójnej analizy, która ujawniła część sekretnych technik stosowanych przez podziemie.

Wiedział jednak, że rosnąca reputacja białego hakera nie uratuje go przed federalną ławą przysięgłych. W wolnych chwilach snuł razem z Kimi fantazje o ucieczce przed przeznaczeniem. Wyjadą razem do Włoch. Albo na jakąś odległą wyspę. Zaczną od nowa. On znajdzie sponsora, kogoś z pieniędzmi, kto pozna się na jego talencie i będzie mu płacił za hakowanie.

Życie z wymiarem sprawiedliwości w tle źle wpływało na ich relacje. Przed najazdem policji nie mieli zbyt wielu planów na przyszłość. Teraz nie mogli o niej myśleć. Zostali pozbawieni kontroli nad nią, zadręczała ich niepewność jutra. Każde z nich martwiło się w samotności, irytując się przy próbie rozmowy. „Podpisałem zeznania, ponieważ właśnie wzięliśmy ślub i nie chciałem cię zranić" - powiedział Max. Uważał to za swój błąd. Żeniąc się, dał swym wro-gom broń przeciwko sobie, fatalne posunięcie.

Kimi przeniosła się z pomaturalnego studium De Anza na Uniwersytet Kalifornijski do Berkeley i oboje przeprowadzili się na drugą stronę Zatoki, by zamieszkać tuż obok kampusu. Ta zmiana okazała się dla Maksa szczęśliwa.

Wiosną 2000 roku firma Hiverworld z Berkeley zaoferowała mu pracę. Dostał

szansę na dołączenie do innych Głodnych Programistów, którzy odnosili sukcesy, wykorzystując dotcomowy boom. Firma planowała stworzenie nowego systemu zabezpieczającego przed hakowaniem, który podobnie jak Snort wykrywałby włamania, ale również aktywnie skanował sieć użytkownika, wyszu-kując słabe punkty i pozwalając

mu ignorować złośliwe ataki niemające szans powodzenia. Twórca Snorta Marty Roesch został pracownikiem numer 11.

Teraz firma chciała Maksa jako numer 21.

63

Miał rozpocząć pracę 21 marca. Było to niskie stanowisko w obiecującej początkującej firmie komputerowej. Amerykańskie marzenie 2000 roku.

Rankiem 21 marca 2000 roku do drzwi Maksa zapukało FBI.

Z początku pomyślał, że to dowcip Hiverworld, inicjacja nowego pracownika. Jednak nie. „Nie otwieraj" - powiedział do Kimi. Złapał za telefon i ukrył

się, w razie gdyby agent zaglądał przez okno. Zadzwonił do Granick i powiedział jej, co się dzieje. Wyrok musiał w końcu zostać wykonany. FBI przyszło tu, by zabrać go do więzienia. Co powinien zrobić?

Agenci odeszli - nakaz aresztowania nie upoważniał ich do wejścia siłą.

Max chwilowo udaremnił więc ich plany, po prostu nie otwierając drzwi. Granick zadzwoniła do prokuratora, próbując przygotować kulturalne zgłoszenie się oskarżonego w terenowym biurze FBI w Oakland. Max skontaktował się z CTO w Hiverworld, swoim nowym szefem, by powiedzieć, że nie pojawi się w pracy pierwszego dnia. Odezwie się za dzień lub dwa i wszystko wyjaśni.

Tego dnia wieczorne wiadomości totalnie go rozwaliły: domniemany haker komputerowy Max Butler został oskarżony o piętnaście przestępstw, w tym nielegalne przechwytywanie komunikacji, włamania do komputerów i posiadanie skradzionych haseł.

Po dwóch nocach, jakie spędził w areszcie, zabrano go do federalnego ma-gistratu w San Jose, by postawić w stan oskarżenia. Kimi, Tim Spencer i dwunastu Głodnych Programistów wypełnili salę. Max został zwolniony za kaucją 100 000 dolarów - Tim wystawił czek na połowę, a pozostali Głodni, którzy dorobili się na dotcomach, dali resztę w gotówce.

To aresztowanie wywołało szok w świecie komputerowego bezpieczeństwa.

Hiverworld z miejsca wycofała ofertę pracy - żadna początkująca firma zajmująca się bezpieczeństwem nie mogła zatrudnić człowieka oskarżonego właśnie o włamania do komputerów. Społeczność zamartwiała się, co się stanie z bazą 64

danych arachNIDS bez opieki Maksa. „To jego sprawa - zadecydował Roesch w poście zamieszczonym na liście mailingowej poświęconej bezpieczeństwu -

więc jeśli otwarcie nie przekaże tego komuś innemu, nadal powinien się nią zajmować".

Max odpowiedział osobiście w długim liście, w którym zaczął od opisywa-nia swego dziecięcego zamiłowania do komputerów, kończąc na przewidywa-niach dotyczących wykrywania włamań w przyszłości. Jego zdaniem Whitehats.com i arachNIDS będą działać dalej, niezależnie od tego, co się wydarzy.

„Moja rodzina udzieliła mi wielkiego wsparcia i mam oferty utrzymywania stron, które w jakiś sposób są zagrożone".

Przedstawiając siebie jako ofiarę, atakował „gorączkę polowań na czarow-nice”, która ogarnęła łowców hakerów, potępiał Hiverworld za nielojalność.

„Kiedy sprawa się wyjaśniła i napisano o mnie w prasie, Hiverworld postanowiła zerwać naszą umowę. Firma wykazała się godnym pożałowania tchórzo-stwem. Nie potrafię wyrazić, jak bardzo byłem rozczarowany, spotykając się z całkowitym brakiem wsparcia ze strony Hive.

Dopóki nie udowodnią mi, że złamałem prawo, jestem niewinny, i byłbym wdzięczny, gdyby nasza społeczność przyjęła to do wiadomości”.

Sześć miesięcy później Max przyznał się do winy. Informacja ta przeszła niemal niezauważona pod lawiną federalnych postępowań przeciw hakerom. W

tym samym miesiącu Patrick „MostHateD” Gregory, przywódca gangu znanego jako globalHell, został skazany na 26 miesięcy więzienia i zobowiązany do zapłacenia 154 529 dolarów i 86 centów jako zadośćuczynienia za całą masę zniszczonych stron internetowych. W tym samym czasie prokurator oskarżył

dwudziestoletniego Jasona „Shadow Knight” Diekmana z Kalifornii o rozrywkowe włamania do systemów uniwersyteckich i NASA, a szesnastolatek Jonathan James, znany jako „C0mrade” otrzymał sześciomiesięczny wyrok za włamania dla zabawy do komputerów Pentagonu i NASA - był to pierwszy wyrok więzienia za hakowanie, jaki kiedykolwiek wydano na osobę nieletnią.

65

Wszystko wskazywało na to, że policja federalna sprawowała teraz silną kontrolę nad włamaniami do komputerów, które tak długo budziły strach wśród amerykańskich przedsiębiorców i przedstawicieli rządu. W rzeczywistości wszystkie te zwycięstwa były bitwami we wczorajszej cyberwojnie przeciw hakerom włamującym się dla rozrywki, którzy byli wymierającym gatunkiem.

I chociaż Max wyznał swe winy na sali sądowej w San Jose, FBI odkrywało zagrożenie XXI wieku, które zbierało się kilka tysięcy kilometrów dalej. W

przyszłości zwiąże się ono ściśle z losem Maksa Visiona.

ROZDZIAŁ 8

Witamy w Ameryce

Dwaj Rosjanie rozgościli się w małym biurze w Seattle. Aleksiej Iwanow, lat dwadzieścia, pisał na komputerze, podczas gdy jego towarzysz, dziewiętnastoletni Wasilij Gorszkow, stał obok i przyglądał się. Właśnie przylecieli z Rosji i już byli w trakcie najważniejszej w ich życiu rozmowy o pracę. Negocjowali lukratywne międzynarodowe partnerstwo z amerykańską początkującą firmą Invita, zajmującą się bezpieczeństwem komputerowym.

Pracownicy biura kręcili się wokół nich, a cicha popowa muzyka sączyła się z komputerowych głośników. Po kilku minutach Gorszkow przeszedł przez pokój i usiadł przy innym komputerze. Michael Patterson, dyrektor generalny Invity, zaczął z nim rozmawiać.

To właśnie on zaprosił Rosjan do Seattle. Invita, jak im napisał w mailu, jest młodą firmą, ale zdobywa klientów dzięki kontaktom, które właściciele wyro-bili sobie, pracując w Microsofcie i Sun. Teraz firma potrzebuje pomocy w zdobywaniu rynku wschodnioeuropejskiego. Iwanow, który twierdził, że ma dwudziestu współpracujących z nim utalentowanych programistów, wydawał się idealnym kandydatem. Gorszkow był „cieniem" zaproszonym przez Iwanowa, 67

by służyć jako rzecznik. W domu zostawił narzeczoną, z którą spodziewali się pierwszego dziecka.

Patterson zaczął zwyczajowo, pytając Gorszkowa o ostatnią falę włamań komputerowych w amerykańskich firmach, z których część płaciła hakerom za ich zaprzestanie. „Wiem, że jesteście w tym tak dobrzy, jak mi się wydaje -

powiedział Patterson - czy któryś z was za tym stoi?"

Gorszkow - okutany w grubą kurtkę, którą nosił w swym rodzinnym Czelabińsku, ponurym, zanieczyszczonym, przemysłowym mieście na Uralu - wy-kręcał się przez chwilę, by w końcu odpowiedzieć: „Kilka miesięcy temu pró-

bowaliśmy, ale okazało się to nieopłacalne".

Rosjanin był skromny. Od blisko roku małe i średnie firmy internetowe w Stanach Zjednoczonych były dręczone cyberatakami mającymi na celu wyłu-dzenie pieniędzy przez gang określający się jako Grupa Ekspertów od Zabezpieczeń przeciw Hakerom - nazwa ta prawdopodobnie lepiej brzmi po rosyjsku. Przestępstwa zawsze przebiegały w ten sam sposób: atakujący z Rosji lub Ukrainy włamywali się do sieci ofiary, kradli numery kart kredytowych lub inne dane, a następnie wysyłali mail bądź faks do firmy, domagając się pienię-

dzy w zamian za milczenie na temat włamania i za załatanie dziur, które wykorzystywali hakerzy. Jeśli firma nie zapłaciła, Grupa Ekspertów groziła zniszczeniem systemu ofiary.

Gang wydobył dziesiątki tysięcy numerów kart kredytowych z Online Information Bureau, izby rozrachunkowej transakcji finansowych w Vernon, Connecticut. Uderzył w ISP Speakeasy z Seattle. Sterling Microsystem w Anaheim w Kalifornii został zaatakowany razem z ISP Cincinnati, koreańskim bankiem w Los Angeles, firmą

zajmującą się usługami finansowymi z New Jersey, firmą zajmującą się płatnościami elektronicznymi E-Money z Nowego Jorku, a nawet czcigodną Western Union, która straciła blisko 16 000 numerów kart kredytowych swoich klientów za sprawą ataku, którego sprawcy domagali się 50 000 dolarów. Kiedy sprzedawca muzyki CD Universe nie zapłacił 100

000 dolarów okupu, tysiące numerów kart kredytowych klientów pojawiło się na publicznych stronach internetowych.

68

Część firm zapłaciła Grupie Ekspertów niewielkie sumy, by zostawili je w spokoju, podczas gdy FBI ze wszystkich sił starało się wytropić włamywaczy.

Ostatecznie namierzyło jednego z przywódców, „subbsta", który naprawdę nazywał się Aleksiej Iwanow. Nie było to zbyt trudne - haker, przekonany o tym, że jest poza zasięgiem amerykańskiego wymiaru sprawiedliwości, wysłał

swoje CV do Speakeasy podczas negocjacji okupu.

Rosyjska milicja zignorowała dyplomatyczną prośbę o zatrzymanie i przesłuchanie Iwanowa. To właśnie wtedy federalni stworzyli Invite, tajną firmę stworzoną po to, by zwabić hakerów w pułapkę. Teraz Iwanow i Gorszkow byli otoczeni przez tajniaków z FBI udających pracowników firmy wraz z bia-

łym kapeluszem z pobliskiego University of Washington, który grał rolę komputerowego geeka imieniem Ray. Ukryte kamery i mikrofony nagrywały wszystko w biurze, a zainstalowane przez FBI oprogramowanie szpiegowskie zapisywało każde uderzenie w klawiaturę komputerów. Na parkingu około dwudziestu agentów było gotowych do pomocy w aresztowaniu podejrzanych.

Agent udający dyrektora generalnego Pattersona próbował wyciągnąć z Gorszkowa jak najwięcej.

- A karty kredytowe? Numery kart kredytowych? Te rzeczy?

- Tutaj nigdy nie powiemy, że mieliśmy dostęp do numerów kart kredytowych - odpowiedział haker.

Tajniak i Gorszkow zaśmiali się porozumiewawczo.

- Rozumiem cię, wiem, co chcesz powiedzieć - stwierdził Patterson.

Kiedy dwugodzinne spotkanie się zakończyło, Patterson zaprowadził męż-

czyzn do samochodu pod pretekstem zawiezienia ich do tymczasowego mieszkania, przygotowanego na ich pierwszą wizytę. Po krótkiej przejażdżce samochód zatrzymał się, agenci błyskawicznie otoczyli go i aresztowali Rosjan.

Po powrocie do biura agent FBI uświadomił sobie, że keylogger, program do zapisywania uderzeń w klawisze, zainstalowany w komputerach w biurze Invity stwarzał rzadką okazję. To, co zrobił później, sprawiło, że stał się pierwszym agentem FBI oskarżonym przez rosyjską milicję o popełnienie 69

przestępstwa komputerowego. Wszedł do pliku keyloggera i znalazł hasło, którym dwaj

Rosjanie posługiwali się, by wejść do swojego komputera w Czelabińsku. Następnie, po konsultacji z szefem i prokuratorem federalnym, zalogował się na rosyjskim serwerze hakerów i zaczął przeglądać spis nazwisk, szukając plików należących do Iwanowa i Gorszkowa.

Kiedy je znalazł, ściągnął 2,3 gigabajta skompresowanych danych i nagrał

je na CD-ROM-ach, by później otrzymać nakaz przeszukania informacji, które zebrał. Było to pierwsze międzynarodowe zdobycie dowodów poprzez hakowanie.

Kiedy federalni przekopywali dane, zapierający dech w piersiach zakres działalności Iwanowa stał się jasny. Oprócz wymuszeń rozwinął on bardzo skuteczną metodę wyciągania gotówki dzięki kartom, które ukradł, używając specjalnego oprogramowania, by automatycznie otwierać konta na PayPalu i eBayu i licytować dobra wystawione na aukcjach, mając pół miliona skradzionych kart kredytowych w swojej kolekcji. Kiedy program wygrywał aukcję, towary był wysyłane do Europy Wschodniej, gdzie odbierali je znajomi Iwanowa. Następnie software powtarzał to kolejny raz i tak w kółko. PayPal sprawdził listę skradzionych kart kredytowych, porównując ją ze swymi we-wnętrznymi bazami danych, i okazało się, że oszukańcze transakcje pochłonęły zaskakującą sumę 800 000 dolarów.

Był to pierwszy wstrząs zapowiadający wielkie tektoniczne zmiany, które zasadniczo ukształtują Internet na następną dekadę. Być może na zawsze. Ma-jąc bardzo dobre uczelnie techniczne, ale bardzo mało możliwości legalnego zatrudnienia dla ich absolwentów, Rosja i kraje byłego Związku Radzieckiego stały się wylęgarnią nowego gatunku hakerów.

Tacy jak Iwanow gromadzili fortuny, łupiąc indywidualnych konsumentów i firmy. Byli bezkarni dzięki skorumpowanej bądź leniwej milicji w swoich rodzinnych krajach i słabej współpracy międzynarodowej. Inni, jak Gorszkow, zeszli na przestępczą drogę ze względu na kiepską sytuację ekonomiczną. Ten haker skończył Państwowy Uniwersytet Techniczny w Czelabińsku ze 70

specjalizacją inżyniera mechanika i utopił niewielki spadek po ojcu w firmie zajmującej się projektowaniem stron i hostingiem. Mimo pozowania w Invicie na twardego hakera Gorszkow był nowym członkiem gangu Iwanowa i zapłacił

za swą podróż do Ameryki w nadziei na poprawę swego losu. W pewien sposób udało mu się to: po aresztowaniu w Seattle zarabiał więcej, zajmując się sprzątaniem w kuchni za jedenaście centów na godzinę, niż jego narzeczona wyciągała z opieki społecznej w rodzinnym kraju.

Po aresztowaniu Iwanow zaczął współpracować z FBI, ujawnił całą listę przyjaciół i znajomych, którzy ciągle jeszcze zajmowali się hakowaniem w Rosji. Pracownicy Biura uświadomili sobie, że macki setek nastawionych na zysk włamywaczy i mistrzów oszukiwania z Europy Wschodniej dosięgnęły już zachodnich komputerów.

W następnych latach ich liczba wzrosła do tysięcy. Iwanow i Gorszkow byli Magellanem i Kolumbem: ich pojawienie się w Ameryce błyskawicznie zmieniło mapę światowej cyberprzestępczości będącą w posiadaniu FBI i bezdysku-syjnie umieściło Europę Wschodnią w jej centrum.

ROZDZIAŁ 9

Okazje

Na ogłoszenie wyroku Max włożył blezer i wymięte bojówki i patrzył w milczeniu, jak prawnicy zmagają się o jego los.

Jennifer Granick, adwokat, powiedziała sędziemu Jamesowi Ware'owi, że Max zasługuje na zmniejszenie kary z uwagi na swą służbę jako Equalizer.

Oskarżyciel zajął przeciwne stanowisko. Max, twierdził, *udawał*, że jest informatorem FBI, podczas gdy w tajemnicy popełniał przestępstwa przeciw rzą-

dowi USA. To było gorsze, niż gdyby nigdy nie podjął współpracy.

Ogłaszanie wyroku za przestępstwo komputerowe było czymś dziwnym.

Dziesiątki kolegów Maksa w świecie bezpieczeństwa - ludzie oddani przeciw-stawianiu się hakerom, napisali do sędziego Ware'a, wstawiając się za Maksem. Dragos Ruiu, liczący się specjalista od bezpieczeństwa z Kanady, nazwał

Maksa „błyskotliwym innowatorem na tym polu". Francuski programista Renaud Déraison podkreślał zasługi Maksa w stworzeniu Nessusa, swojego skanera słabych punktów i jednego z najważniejszych darmowych narzędzi bezpieczeństwa, które były wówczas dostępne. „Biorąc pod uwagę potencjał

Maksa i jego wyraźną wizję internetowego bezpieczeństwa[…] byłoby bardziej 72

pożyteczne dla społeczeństwa jako całości, gdyby pozostał on wśród nas jako specjalista od bezpieczeństwa komputerowego […] zamiast spędzać czas w więziennej celi i patrzeć, jak jego komputerowy talent zmierza ku powolnemu, lecz nieuchronnemu upadkowi".

Od pracownika z branży technologicznej z Nowej Zelandii: „Bez pracy, którą wykonał Max […] byłoby o wiele trudniej mojej firmie i niezliczonym innym przedsiębiorstwom zabezpieczyć się przed hakerami". Od fana z Doliny Krzemowej: „Odejście Maksa ze społeczności zajmującej się bezpieczeństwem komputerowym bardzo osłabi naszą zdolność do obrony". Były pracownik Departamentu Obrony napisał: „Uwięzienie tej osoby byłoby parodią".

Kilku spośród Głodnych Programistów również napisało listy, podobnie jak matka i siostra Maksa. W swoim piśmie Kimi z elokwencją prosiła o uwolnienie Maksa. „Uratował mi życie, pomagając mi wydostać się z toksycznego związku, i nauczył mnie szacunku do samej siebie. Dał mi schronienie, kiedy nie miałam gdzie mieszkać. Bardzo się o mnie troszczył, kiedy byłam poważ-

nie chora, ponownie ratując moje życie, zabierając mnie na pogotowie, gdy nie chciałam tam iść, twierdząc, że czuję się »dobrze«, mimo że umierałam".

Kiedy prawnicy skończyli debatę, Max przemówił we własnym imieniu ze szczerą uprzejmością, jaką okazywał zawsze - poza swoim komputerem. Wyja-

śnił, że jego ataki zrodziły się z dobrych intencji. Chciał tylko załatać dziurę w BIND i stracił głowę.

„Porwało mnie to - powiedział delikatnie. - Trudno jest wyjaśnić uczucia kogoś, kto był pochłonięty dziedziną bezpieczeństwa komputerowego […].

Czułem się wówczas, jakbym brał udział w wyścigu. Myślałem, że jeśli szybciej dotrę do dziur w systemie, będę mógł zapobiec wykorzystaniu ich przez ludzi o złych zamiarach.

To, co zrobiłem, było karygodne. Zepsułem sobie reputację w świecie bezpieczeństwa komputerowego. Zraniłem rodzinę i przyjaciół".

Sędzia Ware słuchał uważnie, ale już podjął decyzję. Zwolnienie Maksa z odbywania kary więzienia byłoby wysłaniem niewłaściwego przekazu do 73

innych hakerów. Jak stwierdził, „należy pokazać tym, którzy chcieliby pójść w twoje ślady, że mogą trafić za kraty".

Wyrok: osiemnaście miesięcy w więzieniu, a następnie trzyletni dozór policyjny, w czasie którego Max nie będzie mógł korzystać z Internetu bez zezwo-lenia swego kuratora sądowego.

Prokurator poprosił sędziego, by Max natychmiast został aresztowany, ale Ware odrzucił tę prośbę i zostawił hakerowi miesiąc na uporządkowanie swoich spraw i zgłoszenie się do funkcjonariuszy policji stanowej.

Po tym jak przyznał się do winy, razem z Kimi przenieśli się do Vancouver, blisko jej rodziny. Kiedy wrócili do domu, Max, nie tracąc czasu, odpowiednio przygotował Whitehats.com i arachNIDS, aby przetrwały okres, kiedy będzie w więzieniu. Ustawił automatyczne płacenie rachunków za Internet i napisał

dla Kimi listę rzeczy, którymi miała się zająć pod jego nieobecność. Teraz jest odpowiedzialna za arachNIDS, powiedział, wskazując serwer stojący na pod-

łodze.

Wzięli dwa koty, aby Kimi miała towarzystwo, kiedy Maksa nie będzie.

Dostały imiona mieczy z *Elryka z Melniboné.* Rudy kocur został Żałobnym Ostrzem, a kotka Zwiastunem Burzy.

Max spędził swój ostatni weekend na wolności, siedząc nad klawiaturą i przygotowując arachNIDS do opieki Kimi. Kiedy nadszedł poniedziałek, po-stąpił zgodnie z planem. 25 czerwca 2001 roku został zamknięty w więzieniu okręgowym, a potem trafił do swego nowego domu, Taft Federal Prison, prowadzonego przez korporację należącą do Wackenhut, znajdującego się w pobliżu małego miasteczka w środkowej Kalifornii.

Był rozdrażniony, spotkała go kolejna niesprawiedliwość, tak jak wcześniej w Idaho. Wysłano go z powrotem do więzienia nie za hakowanie, ale za to, że odmówił wrobienia Matta Harrigana. Został ukarany za lojalność, raz jeszcze padając ofiarą kapryśnego wymiaru sprawiedliwości. Wątpił, by sędzia Ware kiedykolwiek szczegółowo zapoznał się z jego sprawą.

74

Kimi była zagubiona, po raz pierwszy, odkąd spotkała Maksa, została sama.

Mimo całej gadki o tym, że na zawsze zostaną razem, postępował w taki sposób, że zostali

rozdzieleni.

Dwa miesiące później, kiedy Kimi rozmawiała z nim przez telefon, nagle usłyszała *trzask!* i zapach gryzącego dymu wypełnił jej nozdrza. Płyta główna serwera stanęła w płomieniach. Max starał się uspokoić żonę - wystarczy tylko wymienić płytę. On mógł to zrobić przez sen. Instruował Kimi przez telefon, jak postępować, ale do niej docierało właśnie, że nie jest stworzona do bycia żoną uwięzionego hakera.

W sierpniu pojechała na festiwal Burning Man w Nevadzie, by zapomnieć o swych problemach. Kiedy przyjechała do domu, zadzwoniła do Maksa, przekazując mu złe wieści. Spotkała kogoś.

To była kolejna zdrada. Max przyjął nowinę z niesamowitym spokojem, wypytując ją o każdy szczegół: co wzięła, kiedy go zdradziła? W jakiej pozycji uprawiali seks? Chciał usłyszeć jej prośbę o wybaczenie - udzieliłby go błyskawicznie. Ale ona nie o to prosiła. Chciała rozwodu. „Nie wiem, czy w ogóle jeszcze myślisz o przyszłości” - powiedziała.

Chcąc zamknąć sprawę, Kimi złapała samolot do Kalifornii i pojechała do Taft. Usiadła w poczekalni, nerwowo wodząc wzrokiem po ścianie zapełnionej plakatami ukazującymi sieć Wackenhut z więzieniami przypominającymi mrowiska rozsianymi po całym kraju. Kiedy przyprowadzono Maksa, usiadł

przy piknikowym stoliku z nierdzewnej stali w pokoju odwiedzin i uderzył w błagalny ton. Zapewnił ją, że w więzieniu myśli o przyszłości i snuje plany.

„Rozmawiałem z kilkoma ludźmi - powiedział, zniżając słój głos do szeptu.

- Ludźmi, z którymi mógłbym pracować”.

Jeffrey James Norminton kończył dwudziestosiedmiomiesięczną odsiadkę, kiedy Max spotkał go w Taft. Miał 34 lata, tępy wygląd zabijaki, mocny kark, wysokie czoło i bruzdy na policzkach niczym Kirk Douglas. Alkoholik i utalentowany oszust, był finansowym czarodziejem, który swoje najlepsze numery wykonywał na lekkim rauszu.

Zaczynał pić coors lighty, gdy tylko stoczył się z łóżka, i pod koniec dnia nie nadawał się do niczego, ale w słodkim momencie między trzeźwością poranka a popołudniowym zamroczeniem Norminton był mistrzem wielkich oszustw - kryminalnym cudotwórcą, który potrafi stworzyć siedmiocyfrowe sumy z niczego.

Ostatnie przestępstwo wymagało niewiele więcej niż telefonu i faksu. Jego ofiarą padła Entrust Group, inwestycyjny dom brokerski z Pensylwanii. Letniego dnia 1997 roku Norminton zadzwonił do wiceprezesa Entrust, podając się za menedżera inwestycyjnego z Highland Federal Bank, prawdziwego banku w Santa Monica w Kalifornii.

Wzbudzając sympatię i zaufanie, oszust przekonał Entrust do kupienia w tym banku certyfikatów depozytowych o wysokim stopniu zwrotu, obiecując wiceprezesowi gwarantowane 6,20 procent zysku w jednorocznej inwestycji.

Kiedy Entrust ochoczo przelał 297 000 dolarów do Highland, pieniądze wylą-

dowały na koncie fikcyjnej firmy, którą wspólnik Normintona założył pod na-zwą Entrust. Dla banku transakcja wyglądała na przerzucanie pieniędzy przez dom inwestycyjny z

jednej filii do drugiej.

Oszuści szybko wyjęli pieniądze, zostawiając na koncie 10 000 dolarów, i jeszcze raz zrobili ten sam numer, tym razem jednak to wspólnik Normintona zadzwonił do tego samego wiceprezesa i udając przedstawiciela innego banku, City National, zaoferował jeszcze wyższy zysk. Entrust z chęcią zrobił jeszcze dwa przelewy na łączną sumę 800 000 dolarów.

Nie zaspokoiło to jednak ambicji Normintona. Wysłał swojego wspólnika do City National, aby podjął 700 000 na jeden czek gotówkowy. Śledczy z banku nabrał podejrzeń i sprawdził, że źródłem przelewu internetowego jest prawdziwy Entrust. Przy następnej wypłacie przy okienku czekali agenci FBI.

Finansowy mistrz grzał teraz wyrko w Taft. Jedyną jasną stroną uwięzienia było to, że spotkał zdolnego hakera, który chciał wrócić do gry.

Norminton nie krył, że dostrzegł prawdziwy potencjał Maksa, i obaj zaczęli się spotykać codziennie na spacerniaku, opowiadając sobie wojenne opowieści 76

i fantazjując o tym, co mogliby razem zrobić, kiedy już wyjdą na wolność. Z

Normintonem jako przewodnikiem Max mógł bez trudu nauczyć się włamywać do komputerów domów maklerskich, gdzie wpadłyby w ich ręce pieniądze z przepełnionych kont handlowych, które przelaliby do innych banków. Jeden wielki łup i byliby ustawieni do końca życia.

Po pięciu miesiącach Normintona wraz z jego planami odesłano do domu, do słonecznego Orange County w Kalifornii, podczas gdy Max pozostał w Taft na cały rok odsiadki - długie, monotonne dni, kiepskie jedzenie, wstawanie na zbiórkę, dźwięk kajdan i kluczy.

W sierpniu 2002 roku uzyskał wcześniejsze zwolnienie do sześćdziesięcio-jednoosobowego domu przejściowego w Oakland, gdzie dzielił pokój z pię-

cioma innymi skazanymi. Kimi spotkała się z Maksem, aby przedstawić mu pozew rozwodowy. Jej związek z facetem poznanym na Burning Manie zaczynał być poważny, nadeszła już pora, powiedziała, żeby Max pozwolił jej odejść. On nie chciał jednak podpisać dokumentu.

Względna wolność w domu przejściowym była wątła - instytucja wymaga-

ła, by znalazł dobrze płatną pracę lub wrócił do więzienia, a praca zdalna była niedozwolona. Sięgnął po swoje stare kontakty w Dolinie Krzemowej i przekonał się, że jego możliwości zatrudnienia zostały przekreślone przez wyrok za poważne przestępstwo hakerskie i ponad rok w więzieniu.

Zdesperowany, pożyczył laptopa od jednego z Głodnych Programistów i wysłał wiadomość na listy zatrudnienia przeglądane przez ekspertów od bezpieczeństwa komputerowego, którzy go kiedyś podziwiali. „Pokazywałem się w miejscach, gdzie oferują fizyczną pracę o 5.30 rano, i ciągle nic nie znalazłem - napisał. - Moja sytuacja jest po prostu śmieszna”. Zaoferował swoje usługi za najniższą stawkę. „Jestem chętny do pracy za minimalne wynagro-dzenie przez następnych kilka miesięcy. Na pewno w jakiejś firmie zajmującej się bezpieczeństwem gdzieś w okolicy jest wolne stanowisko. […] Kilku ostatnich pracodawców płaciło mi po 100 dolarów na godzinę, teraz proszę tylko o

6,75”.

77

Konsultant odpowiedział na prośbę, pozwalając Maksowi pracować w swym biurze we Fremont, gdzie mógł dojechać z domu przejściowego kolejką BART. Zaoferował 10 dolarów na godzinę za pomoc w budowaniu serwerów.

Dla Maksa był to powrót do pierwszej pracy, którą wykonywał w sklepie ojca, kiedy był nastolatkiem. Tim Spencer pożyczył Maksowi rower, którym codziennie dojeżdżał do stacji kolejki. Max został zwolniony z domu przejściowego po dwóch miesiącach i Głodni Programiści raz jeszcze wyciągnęli pomocną dłoń, dając mu dach nad głową. Przeniósł się do mieszkania w San Francisco, które dzielił z Chrisem Toshokiem, Sethem Alvsem - weteranem przygód z głównym kluczem w Meridian - i byłą dziewczyną Toshoka Charity Majors.

Mimo więziennych fantazji, które pielęgnowali razem z Normintonem, Max był zdeterminowany, by postępować zgodnie z prawem. Wrócił do szukania pracy. Ale oferty nie były przeznaczone dla byłego więźnia. Nawet Projekt Miodowej Sieci, któremu udzielił swej ekspertyzy zaledwie kilka lat temu, odrzucił go.

W jego życiu coś się jednak zmieniło na lepsze - zaczął chodzić z Charity Majors, uciekinierką z Idaho, która stylizowała się na awatara z wirtualnego świata, malując swoje paznokcie jak skittles - każdy w innym kolorze - i nosiła szkła kontaktowe, które nadawały jej oczom niemożliwie szmaragdowy kolor.

Pieniądze były problemem dla obydwojga. Charity pracowała jako administrator systemu dla strony pornograficznej w Nevadzie, zarabiając według stawek Srebrnego Stanu, które były za niskie jak na San Francisco. Max był prawie kompletnie spłukany.

Jeden z dawnych klientów Maksa z Doliny Krzemowej próbował mu po-móc, dając kontrakt na 5000 dolarów na przeprowadzenie testu penetracyjnego swej sieci. Firma lubiła Maksa i nie dbała zbytnio o to, czy napisze on raport, ale haker potraktował to zlecenie bardzo poważnie. Atakował firmowy firewall całymi miesiącami, oczekując jednego z tych łatwych zwycięstw, do których się przyzwyczaił jako biały kapelusz. Ale spotkała go niespodzianka. Stan 78

bezpieczeństwa komputerowego w firmach poprawił się w czasie jego odsiadki. Nie mógł zrobić żadnej wyrwy w sieci swego jedynego klienta. Jego historia jako hakera, składająca się w 100 procentach z sukcesów skończyła się.

- Nigdy wcześniej nie odniosłem porażki, włamując się do systemu - powiedział Charity z niedowierzaniem.

- Kochanie, nie dotykałeś komputera przez wieki - odparła - To zabierze ci chwilę. Nie myśl, że musisz to zrobić dzisiaj.

Max nie dawał za wygraną, ale w rezultacie czuł się jeszcze bardziej sfru-strowany z powodu swej bezsilności. W końcu spróbował czegoś nowego.

Zamiast szukać słabych punktów na wzmocnionych serwerach firmowych, wziął na celownik kilku pojedynczych pracowników.

Te ataki od „strony klienta” są czymś, czego większość ludzi doświadczyła ze strony hakerów - spam pojawiający się w twojej skrzynce, maile z linkami do czegoś, co wygląda jak elektroniczna kartka z życzeniami lub zabawne zdjęcie. To, co ściągasz, jest w rzeczywistości programem wykonywalnym -

jeśli zlekceważysz ostrzeżenie, zainstaluje się on na twoim Windowsie i stra-cisz kontrolę nad własnym komputerem.

W 2003 roku brudną tajemnicą tych ataków było to, że nawet doświadczeni użytkownicy, którzy wiedzieli więcej niż tylko to, że nie należy instalować nieznanego oprogramowania, mogli zostać przechytrzeni. Najczęściej winę ponosiło „rozdęcie przeglądarki”. W latach dziewięćdziesiątych ostra walka z Netscape’em o kontrolę na rynku przeglądarek doprowadziła Microsoft do na-pakowania Internet Explorera zbędnymi elementami i funkcjami. Każda dodat-kowa funkcja w przeglądarce oznaczała nową możliwość ataku. Im więcej kodu, tym więcej robaków.

Dziury w Internet Explorerze zaczęły pojawiać się nieustannie. Zazwyczaj były najpierw odkrywane przez programistów Microsoftu lub białego kapelusza, który często, ale nie zawsze, ostrzegał firmę, zanim opublikował szczegóły na Bugtraqu.

Kiedy już wszyscy wiedzieli o dziurze, zaczynał się wyścig. Czarne kapelusze pracowały nad wykorzystaniem robaka, tworząc strony internetowe 79

dokonujące ataków i wabiąc ofiary do ich odwiedzenia. Wystarczyło na nie zajrzeć, by utracić kontrolę nad własnym komputerem, bez żadnych zewnętrznych oznak infekcji. Nawet jeśli informacje o robakach nie zostały publicznie ujawnione, źli ludzie mogli je odkryć, analizując łatki dodane przez Microsoft.

Specjaliści od bezpieczeństwa patrzyli z niepokojem, jak czas pomiędzy ujawnieniem błędów i ich wykorzystaniem przez hakerów kurczył się z dnia na dzień. W najgorszym razie czarne kapelusze pierwsze odkrywały robaka: był to tak zwany zero-day exploit, który zostawiał dobrym ludziom sporo do nadro-bienia.

Kiedy Microsoft zaczął wypuszczać nowe łatki co tydzień, nawet czujne firmy miały problemy z instalowaniem ich na bieżąco, a przeciętni użytkownicy często w ogóle o to nie dbali. Światowe badania obejmujące 100 000 użytkowników Internet Explorera, prowadzone mniej więcej w tym samym czasie, kiedy Max walczył z firewallem, wykazały, że 45 procent z nich ucierpiało z powodu niezabezpieczonych słabych punktów związanych ze zdalnym dostę-

pem. Ograniczenie wyników jedynie do użytkowników z USA obniżyło ten wynik tylko trochę, do 36 procent.

Atak Maksa był skuteczny. Po uzyskaniu dostępu do komputera z Windowsem należącego do pracownika wdarł się do firmowej sieci od wewnątrz, zgarnął trochę łupów i wyskoczył jak rozrywający ciało potwór w *Obcym.*

„To właśnie wtedy zdecydowałem się na porzucenie starej metody przeprowadzania testów penetracyjnych i włączenie ataku przeciw klientowi do obowiązkowej części testu - napisał później do kolegi białego kapelusza. - Od tamtej pory byłem pewien stuprocentowej skuteczności”.

Zamiast z wdzięcznością ostateczny raport Maksa został przyjęty z oburze-niem. Posługiwanie się atakiem od strony klienta w teście penetracyjnym było niemal niestosowne. Gdyby cię zatrudniono do sprawdzenia fizycznego bezpieczeństwa w głównej siedzibie firmy, niekoniecznie czułbyś się upoważniony do włamywania się do domu pracownika i kradzieży kluczy. Klient zrugał

go - zapłacili przecież Maksowi za atakowanie swoich serwerów, a nie pracowników.

Max zaczął się zastanawiać, czy w ogóle ma przyszłość w branży komputerowego bezpieczeństwa. Wszystkim jego dawnym przyjaciołom należącym do społeczności zaczęło się powodzić. Hiverworld, gdzie Max niemal został za-trudniony jako pracownik numer 21, zreorganizował zarząd i zdobył 11 milionów dolarów kapitału inwestycyjnego, zmieniając nazwę na nCircle Network Security. Marty Roesch opuścił firmę i wykorzystał sukces Snorta - do którego przyczynił się Max - otwierając w Maryland własny biznes pod nazwą Source-fire. Jego firma miała wkrótce zadebiutować na NASDAQ-u.

W jakimś alternatywnym wszechświecie, w którym Max nigdy nie zhakował Pentagonu ani nie używał konta Verio, albo po prostu trzymał język za zębami i założył podsłuch na spotkanie z Maksem Harriganem, prowadziłby jedną z tych firm do finansowego sukcesu, czerpiąc satysfakcję z pełnej wyzwań pracy. Zamiast tego mógł tylko przyglądać się z boku.

Błąkał się bez celu spragniony gotówki, miotając się w poszukiwaniu czegoś, co mógłby zrobić z wolnością. Wtedy właśnie sprawdził swoją skrzynkę mailową na Whitehats.com i znalazł anonimowy list od „starego przyjaciela z Shaft”. To było hasło, które Max wymyślił z Jeffem Normintonem.

Max spotkał się z Normintonem w pokoju Saint Francis Hotel i szybko doszli do porozumienia. Norminton źle znosił nadzór po zwolnieniu; sędzia, który wydał wyrok w jego sprawie, wymagał od niego comiesięcznego oddawania moczu do analizy, aby nadzorujący go oficer miał pewność, że znowu nie za-czął pić. A to był problem, ponieważ znowu pił. Kiedy odmówił oddania prób-ki, sąd nakazał mu zrobić test w Impact House, centrum leczenia alkoholizmu i narkomanii w Pasadenie. Wyszedł stamtąd po trzech tygodniach i teraz szukał

okazji, by zgarnąć jak najwięcej kasy i uciec do Meksyku.

Nadszedł moment na wprowadzenie w życie planów, które snuli w więzieniu, powiedział Norminton. Zaoferował Maksowi finansową pomoc w nowej karierze profesjonalnego hakera.

Max był gotowy. Walczył dostatecznie długo, próbując uczciwie zarabiać na życie, i był zmęczony porażkami. Wiedział, że przestał już być mile widziany w domu Głodnych Programistów, nawet jeśli nigdy się nie skarżyli. Jego dieta ograniczała się do makaronu i warzyw, nie miał ubezpieczenia zdrowotnego, a samo leczenie zębów kosztowałoby go tysiące dolarów.

Obsługa hotelu przerwała rozmowę, by dostarczyć koszyk gościnny. Norminton zrobił

przedstawienie, zanosząc go do łazienki, włączając prysznic i zamykając drzwi. To w razie gdyby w koszyku był podsłuch, wyjaśnił Maksowi. Kiedy śmiejąc się, skończyli rozmowę, Max dał Normintonowi krótką listę zakupów ze sprzętem, którego potrzebował, żeby zacząć: wysokiej klasy laptop Alienware i antenę. Dużą.

Był tylko jeden szkopuł. Norminton był spłukany. Musieli przyjąć do spółki kogoś, kto miał pieniądze na start. Tak się szczęśliwie składało, że Jeff znał

właściwego człowieka.

ROZDZIAŁ 10

Chris Aragon

Max spotkał swego przyszłego przyjaciela i wspólnika w przestępczym procederze w North Beach, małej Italii San Francisco, gdzie obskurne kluby ze striptizem i salony wróżek sąsiadowały z rzędem sympatycznie pstrokatych restauracji, w których podawano ciepły chleb i gorący makaron klientom z ulicy.

Spotkanie zostało umówione w kawiarni niedaleko księgarni City Lights, w latach pięćdziesiątych kolebki Beat Generation, po przekątnej od Vesuvio Café, lokalu reklamowanego przez wielki kolorowy mural przedstawiający butelki wina i pacyfki. W dole Transamerica Pyramid dźgała niebo, stojąc na straży dzielnicy finansowej.

Norminton przedstawił Chrisa Maksowi ponad ściszonym brzękiem filiżanek do kawy i talerzy. Obydwaj natychmiast się dogadali. Czterdziestojednoletni Chris był adeptem wschodniej duchowości, wegetarianinem, który prak-tykował medytację, by skupić swój umysł. Max, ze swymi hipisowskimi wartościami, wydawał się bratnią duszą na życiowej drodze. Czytali nawet te same książki.

I - tak jak Max - Chris trafi za kratki więcej niż jeden raz.

Wszystko zaczęło się w Kolorado, kiedy Chris miał 21 lat. Pracował jako 83

masażysta w kurorcie z gorącymi źródłami, zarabiając dostatecznie dużo, aby płacić za wynajem mieszkania i finansować skromny kokainowy nałóg, kiedy spotkał pokręconego weterana imieniem Albert See, którego poznał w więzieniu, kiedy odbywał wyrok jako nieletni. See właśnie uciekł z więzienia o zła-godzonym rygorze i potrzebował pieniędzy, by opuścić kraj.

Chris pochodził z uprzywilejowanej klasy - jego matka Marlene Aragon pracowała w Hollywood, podkładając głos w filmach, i ostatnio cieszyła się występem w nadawanej w sobotnie poranki kreskówce *Challenge of the Super-friends,* podkładając głos Cheetah, kociej prześladowczym Wonder Woman.

Chris również miał romantyczne spojrzenie na przestępstwo i przestępców. Na ścianie w swoim mieszkaniu powiesił plakat przedstawiający okładkę albumu Waylona Jenningsa *Ladies Love Outlaws.* Wciągnął w to Alberta i obaj wzięli udział w serii śmiałych i przeważnie spartaczonych napadów na bank w kuror-tach rozsianych po Kolorado.

Pierwszy napad na Aspen Savings and Loan w Aspen zaczął się całkiem nieźle: Chris, z niebiesko-białą chustą na twarzy, by ukryć swój młody wiek, wycelował automatyczną wojskową czterdziestkę piątkę w menedżera banku, kiedy ten rano otwierał drzwi. Wraz z Albertem zmusili go, żeby wszedł do środka, gdzie znaleźli ukrytą pod biurkiem sprzątaczkę, która dzwoniła na policję. Uciekli w popłochu.

Drugi napad - tym razem na Pitkin County Bank and Trust - skończył się, zanim się zaczął. Wspólnik Chrisa ukrył się w kontenerze na śmieci obok tyl-nego wejścia, planując wyskoczyć z shotgunem, kiedy pierwsi pracownicy przyjdą rano do pracy Ich zamiary zostały pokrzyżowane, kiedy Chris, obserwujący wszystko z drugiej strony ulicy, zobaczył śmieciarkę podjeżdżającą, by opróżnić kontener.

Trzeci napad był lepiej zaplanowany. 22 lipca 1981 roku Chris i Albert odwiedzili Voit Chevrolet w Rifle i zgłosili chęć jazdy próbnej nowym camaro.

Pechowy sprzedawca uparł się, że pojedzie z nimi, i kiedy opuścili granice miasta, Chris zjechał na pobocze, a Albert, grożąc pistoletem, wyciągnął sprzedawcę z samochodu. Związali go sznurem, zakneblowali i zostawili w polu, by 84

zniknąć w srebrnym sportowym samochodzie.

Następnego dnia o 4.50 po południu Chris pojechał skradzionym cámaro do Valley Bank and Trust w Glenwood Springs, gdzie mieszkańcy miasteczka oddawali na przechowanie swoje pieniądze zarobione na kwitnącej turystyce.

Sam Chris również był klientem tego banku. Czekał na zewnątrz za kierownicą, podczas gdy Albert w ciemnych okularach i ze skórzaną dyplomatką wszedł

do środka. Po kilku minutach wybiegł z 10 000 w gotówce i wskoczył do cámaro, a Chris ruszył ostro z kopyta.

Skierowali się na południe od miasta, nieubitą drogą, która wiła się poprzez skaliste czerwone wzniesienia otaczające Glenwood Springs. Potem zjechali na polną drogę, gdzie czekała jego dziewczyna z samochodem na zmianę. Trium-fujący i podekscytowany Chris jechał za nią, kręcąc camaro zwycięskie ósemki i podnosząc kłęby pyłu na sześć metrów do góry.

Podskakiwał i krzyczał: „Udało się!”, kiedy policyjny samochód, otoczony chmurą pyłu, wjechał prosto na nich. Chris i Albert rzucili się pieszo do sza-leńczej ucieczki przez skalisty teren usiany drzewami. Chris spadł z krawędzi skały i wylądował na kaktusie. Dwaj gliniarze dopadli ich. Chris rzucił broń i poddał się.

Wiele się z tej sytuacji nauczył: nie tego, że zbrodnia nie popłaca, ale tego, że pistolety i kradzione samochody są głupim sposobem na rabowanie banku.

Kiedy w 1986 roku, po spędzeniu pięciu lat w federalnym więzieniu, wyszedł

na zwolnienie warunkowe, zajął się oszustwami z użyciem kart kredytowych, osiągając nawet skromne sukcesy. Potem zaczął pracować z meksykańskim przemytnikiem narkotyków, którego poznał w więzieniu. Pomógł mu dostarczyć 2000 funtów marihuany na ośmiohektarowe ranczo w pobliżu Riverside w Kalifornii - tylko po to by wpaść w zakrojonej na skalę całego kraju tajnej operacji DEA*. We wrześniu 1991 roku znowu był w więzieniu.

* DEA - Drug Enforcement Administration - amerykańska agencja rządowa zajmująca się kontrolą rynku leków, a także zwalczaniem handlu narkotykami.

85

Kiedy wyszedł w 1996 roku, miał 35 lat, a połowę dorosłego życia i część dzieciństwa spędził za kratami. Postanowił żyć w zgodzie z prawem. Z pomocą matki założył legalne przedsiębiorstwo leasingowe pod nazwą Mission Pacific Capital, dostarczające komputery i wyposażenie dla początkujących firm, które chciały dołączyć do wyścigu dot-comów.

Schludny i przystojny, z pełnym empatii spojrzeniem, Chris łatwo wszedł w rolę biznesmena z południowej Kalifornii. Po latach wypełnionych przestępstwami i

niepewnością życie normalnego przedstawiciela klasy średniej miało egzotyczny urok i dawało poczucie spełnienia. Uwielbiał jeździć na spotkania służbowe, przeprowadzać rozmowy o pracę i zatrudniać ludzi, gawędzić z ko-legami. Na konferencji poświęconej marketingowi w Nowym Orleanie spotkał

Clarę Shao Yen Lee, elegancką kobietę chińskiego pochodzenia, która wyemi-growała z Brazylii. Ujęty jej urodą i inteligencją, wkrótce się z nią ożenił.

Pod przywództwem Chrisa Mission Pacific wyrobiła sobie reputację inno-wacyjnego brokera leasingowego, jednego z pierwszych, którzy oferowali szybkie umowy przez Internet, co pomogło firmom zdobyć dziesiątki tysięcy klientów z całego kraju. Były przestępca, który napadał na banki i przemycał

narkotyki, miał za wspólników dwóch prominentnych biznesmenów z Orange County i zatrudniał 21 ludzi pracujących w przestronnym biurze o krok od Pacific Coast Highway. Clara wpadała co jakiś czas, aby zadbać o wizerunek firmy i pomóc w tworzeniu materiałów marketingowych. Do 2000 roku mał-

żonkowie dorobili się ekskluzywnego mieszkania w Newport Beach i syna oraz pokazali, że biznes, którego potencjał wydawał się równie nieograniczony jak sam Internet, jest ich.

Tamtej wiosny czar prysł. Bańka dot-comów pękła i strumień nowych firm, które były dla Mission Pacific niczym dopływ świeżej krwi, zaczął wysychać.

Potem większe korporacje, takie jak American Express, opanowały branże leasingowa, wypierając mniejsze firmy. Firma Chrisa była jedną z wielu, które musiały upaść. Zaczął zwalniać pracowników i w końcu musiał powiedzieć maruderom, że Mission Pacific nie będzie w stanie dać im następnej wypłaty.

Chris podjął pracę w innej firmie leasingowej, ale został zwolniony, gdy została przejęta przez duży bank. Tymczasem jego żona urodziła drugiego syna.

Tak więc kiedy pojawił się Jeff Norminton, opowiadając o superhakerze, któ-

rego spotkał w Taft, Chris był gotów go wysłuchać.

Chris zaczął finansować plan Normintona, jeszcze zanim spotkali się z Maksem w restauracji North Beach, kupując część wyspecjalizowanego sprzę-

tu, którego potrzebował haker. Teraz, kiedy Chris poznał Maksa osobiście, chciał sprawdzić jego umiejętności. Po wielogodzinnej rozmowie wyszli z kawiarni, by znaleźć miejsce, z którego można przeprowadzić hakerski atak.

Wylądowali w dwudziestosiedmiopiętrowym Holiday Inn w Chinatown kilka przecznic dalej. Zgodnie ze wskazówkami Maksa poprosili o pokój wysoko nad ulicą. Max usadowił się przy oknie, odpalił laptopa, podłączył antenę i zaczął skanować w poszukiwaniu sieci WiFi.

W 2003 roku świat masowo przechodził na bezprzewodowy Internet, tworząc przy okazji wielką dziurę w systemie bezpieczeństwa. Rewolucję rozpoczął bezprzewodowy punkt dostępu Apple Airport, a następnie dołączyli producenci hardware’u, tacy jak Linksys i Netgear. Wraz ze spadkiem cen sprzętu coraz więcej firm i domowych użytkowników

zaczęło uwalniać się z pęt nie-bieskich kabli Ethernetu.

Ale bezprzewodowy sprzęt, wprowadzany do domów i biur w całym kraju, był marzeniem hakera. W przeważającej części opierał się on na bezprzewo-dowym standardzie zwanym 802.11b, obejmującym schemat szyfrowania, który w teorii utrudniłby wskoczenie do czyjejś bezprzewodowej sieci bez uwierzytelnienia lub śledzenie komputerowego ruchu. Ale w 2001 roku badacze z Uniwersytetu Kalifornijskiego w Berkeley odkryli dużą liczbę poważ-

nych słabości w schemacie szyfrowania, które sprawiały, że był on łatwy do złamania przy użyciu łatwo dostępnego sprzętu i właściwego oprogramowania.

I co liczyło się w praktyce - techniczna czarna magia zazwyczaj nie była nawet do tego potrzebna. Aby ułatwić użytkowanie, producenci wypuszczali bezprzewodowe punkty dostępu ze standardowo wyłączonym szyfrowaniem. W

małych i dużych firmach po prostu podpinano pudełka i zapominano o nich 87

- czasem mylnie zakładając, że ściany biura zatrzymają sieć przed wyjściem na ulicę.

Kilka miesięcy przed pójściem Maksa do więzienia haker w białym kapeluszu wynalazł sport zwany „wardrivingiem", aby zwrócić uwagę na niezabezpieczone sieci w San Francisco. Po przyczepieniu magnetycznie montowanej anteny na dachu swego saturna jeździł po ulicach w centrum miasta, podczas gdy jego laptop wyszukiwał sygnały punktów dostępu WiFi. Po godzinie krą-

żenia po dzielnicy finansowej jego zestaw znalazł blisko osiemdziesiąt sieci.

Od tamtej chwili minęło półtora roku i San Francisco, podobnie jak inne duże miasta, było pokryte niewidzialnym morzem WiFi, w którym każdy mógł się zanurzyć.

Hakowanie z domu było dobre dla nastolatków i idiotów - Max przekonał

się o tym w bolesny sposób. Dzięki WiFi mógł teraz pracować niemal z każde-go miejsca, zachowując całkowitą anonimowość. Tym razem jeśli policja wpadnie na trop jednego z jego hakerskich ataków, skończy na progu jakiegoś biednego frajera, którego Max wykorzystał, by wejść do sieci.

Antena, której używał, była monstrualną paraboliczną kratką o szerokości ponad 60 centymetrów, która szybko wykryła dziesiątki sieci wokół Holiday Inn. Wskoczył do jednej z nich i pokazał Chrisowi, jak to wszystko działa.

Posługując się skanerem słabych punktów - narzędziem, którego używał w swoich testach penetracyjnych - był w stanie szybko przeszukać wielki kawał

internetowej przestrzeni adresowej. Przypominało to zarzucanie pływających sieci do morza WiFi. Dziury w systemie bezpieczeństwa były wszędzie. Miał

pewność, że dotrze do sieci instytucji finansowych i internetowych sprzedawców błyskawicznie. To Norminton i Chris mieli zdecydować, jakiego rodzaju danych potrzebowali i w jaki sposób je wykorzystają.

Chris był pod wielkim wrażeniem. Ten blisko dwumetrowy półwegetarianin znał swój hakerski fach, nawet jeśli nieco nadwątlony przez więzienie.

Przedstawił Maksa jednemu ze swoich więziennych kumpli, poznanemu w 1992 roku w Terminal Island, Wernerowi Janerowi, który zajmował się 88

oszustwami w branży nieruchomości. Zaoferował on Maksowi 5000 dolarów za wejście do komputera osobistego wroga. Wypisał czek na Charity, by Max nie musiał się tłumaczyć z zarobku swemu kuratorowi sądowemu.

Pieniądze te pozwoliły Maksowi złapać oddech. Zaczął latać do Orange County, błędnie zapisując swe imię na biletach, aby nie pozostawiać śladów stanowiącego naruszenie zwolnienia warunkowego opuszczania Bay Area. On i Norminton wpadali do Chrisa zazwyczaj raz w tygodniu, hakując z jego gara-

żu.

Ściągnął listę małych instytucji finansowych ze strony FDIC-u, stwierdzając, że mają one najwięcej słabych punktów, i stworzył skrypt pozwalający na skanowanie każdego banku w poszukiwaniu znanych luk w bezpieczeństwie.

Elektroniczny dzwonek rozbrzmiewał w garażu, kiedy tylko trafił na którąś z nich. Max wślizgiwał się do banku i wydobywał nazwiska klientów, dane operacji finansowych i numery kont.

To chaotyczne podejście oznaczało, że Max zaoszczędzi sobie frustracji, którą odczuwał w swych ostatnich legalnych testach penetracyjnych. Hakowanie jakiegokolwiek poszczególnego celu może być trudne, a czasem po prostu niemożliwe. Ale jeśli zeskanujesz setki tysięcy systemów, możesz być pewien, że znajdziesz jakieś podatne na atak. To była gra w numery, jak sprawdzanie drzwi od samochodów, kiedy idziesz przez parking.

Charity miała tylko ogólne wyobrażenie o tym, czym zajmował się Max, ale nie podobało jej się to. Starając się zdobyć jej przychylność, Chris i Norminton zaprosili parę na małe wakacje w Orange County, opłacając im przejazd i tygo-dniowy pobyt w Disneylandzie. Charity widziała, że Max i Chris świetnie się dogadują, ale coś jej w nim nie pasowało. Był zbyt śliski, zbyt wygładzony.

Max przerzucił się na małe strony sklepów internetowych, skąd wydobywał

historie transakcji, niektóre z numerami kart kredytowych. Jego wysiłki nie były ukierunkowane, a Chris i Norminton nie wiedzieli, co z tymi wszystkimi danymi zrobić.

89

Na szczęście Chris spodziewał się pieniędzy. Werner Janer był mu winien 50 000 i był gotów je przelać na konto we wskazanym przez Chrisa banku.

Chcąc jak najszybciej położyć ręce na żywej i nieopodatkowanej gotówce, Chris poprosił Normintona, by ten zrobił to, co potrafi najlepiej. Jeff zgodził

się, by jeden z jego przyjaciół przyjął przelew i wybrał pieniądze w ciągu kilku dni.

Pierwsza wypłata poszła zgodnie z planem i Norminton wraz z przyjacielem pojawił się u Chrisa, wręczając mu ponad 30 000 dolarów w studolarowych banknotach. Jednak następnego dnia Norminton zgłosił, że jego kumpel się rozchorował i weźmie dzień wolnego.

W rzeczywistości Norminton odkrył źródło nieoczekiwanego dopływu go-tówki: to była działka Chrisa z oszustwa na nieruchomościach, w którym po-mógł Janerowi. Pieniądze były brudne, a Norminton był teraz zamieszany w aferę. Następnego ranka Chris znalazł hondę, którą pożyczył przyjacielowi, zaparkowaną poza jego biurem, z przedziurawioną oponą i wgięciem na błot-niku. W samochodzie była informacja od Normintona: FBI depcze mi po pię-

tach. Uciekam z miasta.

Chris zadzwonił do faceta, który przechowywał pieniądze, wiedząc już, jak to wygląda: wspólnik Normintona cieszył się doskonałym zdrowiem i zgodnie z planem wybrał pozostałe 20 000 poprzedniego dnia. Dał je Normintonowi.

Czy Chris tego nie rozumie?

Chris dotarł do Maksa przez Charity i zażądał wyjaśnień: co Max wie o miejscu pobytu Normintona? Gdzie są pieniądze? Max był równie zaskoczony zniknięciem wspólnika i ostatecznie obaj zgodzili się kontynuować współpracę bez Normintona.

Max i Chris wpadli w rutynę. Raz na miesiąc Chris przylatywał lub przyjeżdżał

na północ i spotykał się z Maksem w centrum San Francisco, gdzie wynajmowali pokój w hotelu. Nieśli z sobą wielką antenę po schodach przeciwpożarowych i montowali ją na trójnogu w pobliżu okna. Potem Max guzdrał się przez chwilę, żeby znaleźć najszybsze WiFi z mocnym sygnałem.

Nauczyli się, że wysokość nie jest tak istotna w hakowaniu WiFi jak bez-

ładne skupisko budynków widocznych za oknem. Kiedy nic im się nie udawało złapać, Chris schodził do recepcji i prosił o inny pokój, wyjaśniając poważnie, że jego komórka nie może złapać zasięgu albo że jest zbyt przestraszony wysokością, aby pozostać na dwudziestym piętrze.

Max traktował to jak pracę, mówił Charity „do zobaczenia” i znikał, często nawet na tydzień, w jednym z najlepszych w hoteli mieście, takich jak Hilton, Westin, W czy Hyatt. Trąbienie samochodowych klaksonów dobiegało z dołu, a Max zarzucał swoją sieć w cyberprzestrzeń, zgarniając wszelkie dane, jakie mógł znaleźć, tak naprawdę nie wiedząc, czego szuka.

Przy okazji włamał się do komputera Kimi oraz komputera jej nowego chłopaka, do którego się wprowadziła. Zastanawiał się nad splądrowaniem jej książki adresowej i rozesłaniem zbiorowego maila z jej adresu, w którym byłby szczegółowy opis tego, jak go zdradziła. Pomyślał, że każdy powinien wiedzieć, iż nowe życie Kimi zostało zbudowane na fundamencie niewierności.

Nie zrobił tego jednak. Teraz miał Charity. Kimi odeszła i uświadomił sobie, że nic by nie osiągnął, zawstydzając ją. Wkrótce podpisał pozew rozwodowy.

Wracając do swej pracy, zaczął używać wyszukiwarki Google’a, chcąc znaleźć wskazówki na temat swych celów: co robią inni oszuści? Jak czerpią pieniądze ze skradzionych danych? Właśnie wtedy odkrył, że prawdziwe przestępstwa miały miejsce w

sieci na dwu stronach: CarderPlanet i Shadowcrew.

ROZDZIAŁ 11

Dwudziestodolarowe zrzuty Scripta

Wiosną 2001 roku około 150 rosyjskojęzycznych przestępców komputerowych zwołało spotkanie w restauracji w Odessie, ukraińskim mieście portowym, aby stworzyć rewolucyjną stronę internetową. Był tam Roman Vega, trzydziesto-siedmioletni mężczyzna, który sprzedawał podrobione karty kredytowe przestępczemu podziemiu przez swą internetową witrynę BOA Factory; cyberoszust znany jako „King Arthur” oraz człowiek, który stanie się ich przywódcą -

ukraiński sprzedawca kart kredytowych znany jako „Script”.

Zarzewiem dyskusji był sukces założonej w 2000 roku na brytyjskim serwerze strony internetowej zwanej Counterfeit Library, której twórcy rozwiązali jeden z podstawowych problemów w prowadzeniu nielegalnych interesów w czat roomach IRC-a, gdzie wiedza i doświadczenie zebrane w ciągu lat przestępczej działalności znikały wraz z zakończeniem czatu. Stworzona przez garść zachodnich cyberoszustów Counterfeit Library była stroną, na której zebrano praktyczne informacje i rady dla przestępców, dołączając forum umoż-

liwiające dyskusje online. Złodzieje tożsamości mogli się tu spotykać i wymieniać wskazówkami oraz sprzedawać i kupować „nowe”

karty identyfikacyjne - ten eufemizm powstał w takim samym duchu, w jakim mówi się, że prostytutki chodzą na „randki”.

Counterfeit Library miała więcej wspólnego z elektronicznym systemem bulletinem board z epoki przed WWW niż z IRC-em. Członkowie mogli tworzyć posty w stałych wątkach dyskusyjnych i budować osobistą reputację i marki. Kiedy przestępcy z całego świata odkryli ten skrawek suchego lądu w mętnym i burzliwym morzu podziemnego handlu, strona zgromadziła setki, a potem tysiące członków w Ameryce Północnej i w Europie. Byli wśród nich złodzieje tożsamości, hakerzy, phisherzy, spamerzy, fałszerze pieniędzy i kard kredytowych, wszyscy, którzy tyrali w swoich mieszkaniach i magazynach aż do teraz nieświadomi wielkości ich sekretnego bractwa.

Carderzy z Europy Wschodniej z zazdrością patrzyli na Counterfeit Library.

Teraz mieli zamiar zastosować tę samą alchemię w swoim podziemnym światku.

W czerwcu 2001 roku pojawił się owoc spotkania w Odessie: The International Carders Alliance lub po prostu Carderplanet.com, bardziej zorganizowa-na wersja Counterfeit Library dostosowana do podziemnego światka byłego imperium sowieckiego. Podczas gdy Counterfeit Library stanowiła swobodną płaszczyznę dyskusji, a BOA Factory otwartą witrynę przedsiębiorstwa, CarderPlanet była zdyscyplinowanym internetowym bazarem, pełnym gorączko-wej wymiany towarów.

Otwarcie przedstawiając swe cele, strona naśladowała sztywną hierarchię włoskiej mafii, posługując się także jej nazewnictwem. Zarejestrowany użytkownik był określany jako „sgarrista”, czyli żołnierz pozbawiony specjalnych przywilejów. Szczebel wyżej znajdował się „giovane d’honoré”, który pomagał

w moderowaniu dyskusji pod nadzorem „capo”. Na szczycie łańcucha pokar-mowego był don CarderPlanet - Script.

Rosyjskojęzyczni sprzedawcy tłumnie rzucili się na nową stronę, aby zaoferować mnóstwo produktów i usług. Numery kart kredytowych były, naturalnie, podstawowym towarem, ale tylko na początku. Niektórzy sprzedawcy wyspe-cjalizowali się w wartościowszych „pełnych informacjach” - numerach kart 93

kredytowych wraz z nazwiskami, adresami, numerem ubezpieczenia i nazwiskiem panieńskim matki właściciela, wszystko razem za około 30 dolarów.

Znakowane konta na eBayu były warte 20 dolarów. Ambitni kupcy mogli wy-dać 100 dolarów na „zmianę rachunku” albo COB - skradzione konto karty kredytowej, gdzie adres billingowy mógł zostać zmieniony na inny kontrolowany przez kupca. Inni sprzedawcy podrabiali czeki lub polecenia wypłaty albo wynajmowali w USA bezpieczne miejsca, gdzie towary zamówione na amerykańskie karty kredytowe mogły być dostarczane bez wzbudzania podejrzeń i przesłane do oszusta.

W ofercie były także takie produkty jak czyste plastikowe karty z paskiem magnetycznym oraz „nowe” kompletne dokumenty tożsamości z hologramami, które sprzedawano gdziekolwiek za 75-150 dolarów, zależnie od jakości. Moż-

na było kupić zestaw dziesięciu dokumentów tożsamości z tym samym zdję-

ciem, ale różnymi nazwiskami, za 500 dolarów.

Każdy mógł się zarejestrować na CarderPlanet, ale żeby móc sprzedawać na stronie, należało najpierw dać swoje produkty do sprawdzenia uznanemu re-cenzentowi. Od nowych sprzedawców czasem wymagano, aby przeprowadzali swoje transakcje za pośrednictwem Scripta albo wysyłali składkę na fundusz ratunkowy, który płacił kupującym, w razie gdy uznany sprzedawca wypadł z biznesu i nie zrealizował zamówień. Oczekiwano, że sprzedawcy będą utrzymywali zarząd powiadamiany o wszelkich planach wakacyjnych, chroniący informacje kupujących przed atakami hakerów i natychmiast odpowiadający na skargi kupujących. „Rabusie”, którzy nie dostarczyli towaru, byli blokowani, podobnie jak każdy sprzedawca, który zebrał pięć skarg klientów. Wkrótce w ślady CarderPlanet poszło anglojęzyczne podziemie, tworząc stronę Shadowcrew. We wrześniu 2002, zainspirowany zaskakującym sukcesem zdyscypli-nowanej hierarchii CarderPlanet, carder znany jako „Kidd” ściągnął najlepszych strzelców z Counterfeit Library, by prowadzić biznes w rosyjskim stylu.

Informacja na temat strony rozeszła się przez czat roomy IRC-a i więzienne 94

spacerniaki. Do kwietnia 2003 roku na Shadowcrew zarejestrowało się 4000

użytkowników.

Z dewizą: „Dla tych, którzy lubią grać w cieniu”, Shadowcrew była jednocześnie zdalnym uniwersytetem i supermarketem online, w którym można było kupić wszystko, co nielegalne. Podręczniki oferowały lekcje na temat wykorzystania skradzionych numerów kart kredytowych, fałszowania prawa jazdy, unieszkodliwiania alarmu przeciwwłamaniowego czy wytłumienia pistoletu.

Użytkownicy szczycili się wiedzą o tym, w którym stanie obowiązywało łatwe do

podrobienia prawo jazdy. Uznani sprzedawcy na całym świecie mogli dostarczyć oszałamiającej ilości nielegalnych produktów i usług: historii kredytowych, zhakowanych kont bankowych, nazwisk, dat urodzenia, numerów ubezpieczenia społecznego i potencjalnych celów złodziei tożsamości.

Podobnie jak w przypadku CarderPlanet, każdy produkt miał swoich specjalistów i każdy sprzedawca musiał być oceniony przez zaufanego członka forum, zanim pozwolono na sprzedaż. Spory były załatwiane sprawiedliwie, a administratorzy i moderatorzy pracowali po godzinach, by ujawnić i i zablokować rabusiów sprzedających lipne produkty.

Handel wykroczył poza dane ku bardziej namacalnym towarom, takim jak nielegalne czytniki kart bankomatowych, leki dostępne tylko na receptę i koka-ina, oraz ofertom takim jak zablokowanie systemu lub sieci polegające na zaję-

ciu wszystkich wolnych zasobów (DDoS) - skasuj dowolną stronę za 200 dolarów - i dostosowywanie malware'u, by mógł przechytrzyć programy antywirusowe. Jeden dobrze oceniany sprzedawca oferował usługę testową, obiecując klientowi otrzymanie technicznej legalizacji w ciągu kilku dni. Sprzedawca występujący pod nickiem UBuyWeRush zalał podziemie urządzeniami do zapisu pasków magnetycznych i innymi niezbędnymi rzeczami, takimi jak specjalny papier i magnetyczne kartridże z atramentem do podrabiania czeków.

Dziecięca pornografia była zabroniona, a facet, który chciał sprzedawać eg-zotyczne zwierzęta, został wyśmiany. Ale poza tym prawie wszystko na Shadowcrew było dozwolone.

95

Do tego czasu na CarderPlanet powstały mniejsze fora dla przestępców z Azji, Europy i USA, ale to Shadowcrew stworzyła prawdziwy międzynarodowy rynek, krzyżówkę Chicago Mercantile Exchange i kantyny Mosa Eisleya z *Gwiezdnych wojen*, gdzie przestępcy reprezentujący różne specjalności mogli się spotykać i nawiązywać współpracę. Złodzieje tożsamości z Denver mogli kupować numery kart kredytowych od hakera z Moskwy i wysyłać je do Szan-ghaju, gdzie wykorzystywano je do podrobienia kart kredytowych, by przed wizytą w centrum handlowym dokupić jeszcze fałszywe prawo jazdy od oszusta z Ukrainy.

Max podzielił się swym odkryciem z Chrisem. Chris był tym zafascynowany, logował się na fora i studiował posty jak podręcznik. Wiele rzeczy wyglądało podobnie jak w latach osiemdziesiątych, kiedy zajmował się oszukiwaniem na kartach kredytowych. Inne zmieniły się diametralnie.

Był czas, kiedy oszuści mogli dosłownie wyciągnąć numery kart kredytowych ze śmieci, nurkując w koszach za rachunkami lub odbitkami z drukarki kasjera. Teraz mechaniczne drukowanie odeszło do historii, a Visa i MasterCard wymogły, by rachunki nie zawierały pełnych numerów kont kart kredytowych. Nawet jeśli zdobyłeś numer, nie wystarczyło to już do zrobienia fał-

szywej karty. Firmy oferujące karty kredytowe dodawały teraz specjalny kod do każdego paska magnetycznego - coś w rodzaju PIN-u, ale nieznanego nawet właścicielowi karty.

Nazywany Card Verification Value albo CVV, stanowi on połączenie innych danych z

paska - w pierwszym rzędzie numeru konta i daty wygaśnięcia -

zaszyfrowanych według klucza znanego tylko bankowi, który wydał kartę.

Kiedy pasek magnetyczny zostaje wsunięty do czytnika terminalu, CVV razem z numerem konta i innymi danymi trafia do właściwego banku w celu weryfikacji. Jeżeli numer nie jest właściwy, transakcja zostaje odrzucona.

Kiedy CVV został wprowadzony przez Visę w 1992 roku, natychmiast wpłynął na zmniejszenie strat spowodowanych oszustwami z blisko 18

96

procent transakcji Visy do około 15 procent rok później. W 2000 roku innowacja ta potwierdziła swą skuteczność jako mocne zabezpieczenie przeciw atakom phishingowym, w których spamer wysyła tysiące fałszywych maili, mają-

cych skłonić klientów do wpisania numeru karty kredytowej na fikcyjnej stronie banku. Bez CVV na pasku magnetycznym - którego klient nie znał, więc nie mógł ujawnić - te skradzione numery były bezużyteczne przy kasach. Nikt nie mógł wejść do kasyna w Vegas, by wczytać kartę zrobioną dzięki phishin-gowi, dostać górę czarnych żetonów i zanieść je do stolika z ruletką.

MasterCard poszedł w ślady Visy, tworząc własny Card Security Code -

CSC. Następnie w 1998 roku Visa wprowadziła CVV2, inny sekretny kod wydrukowany na odwrocie, przeznaczony wyłącznie do użytku telefonicznego i internetowego. Innowacje te zmniejszyły straty spowodowane przestępstwami i dokończyły budowę chińskiego muru między oszustwami w Internecie i realnym życiu. Konta skradzione ze stron e-handlowych lub za sprawą ataków phishingowych mogły być używane wyłącznie w Internecie lub przez telefon, podczas gdy dane z paska magnetycznego tylko w sklepie, ale nie w sieci, ponieważ nie zawierały wydrukowanego CVV2.

Do 2002 roku zastosowane środki bezpieczeństwa sprawiły, że źródłowe dane z paska magnetycznego stały się jednym z najbardziej wartościowych towarów w podziemiu, czyniąc celem ataków samych klientów.

Hakerzy zaczęli włamywać się do systemów przeprowadzania transakcji, aby uzyskać dane, ale najprostszym sposobem ich kradzieży było werbowanie spragnionych gotówki pracowników restauracji i wyposażenie ich w kieszon-kowy „skimmer”, czytnik pasków magnetycznych z wbudowaną pamięcią.

Urządzenie wielkości zapalniczki, łatwe do ukrycia w kieszeni fartucha pracownika fast foodów czy marynarce eleganckiego *maître d’*, mieściło w swej pamięci setki kart. Dostęp do tych danych można było później uzyskać przez port USB. Kelnerowi wystarczyła zaledwie sekunda na osobności, by przecią-

gnąć kartę klienta przez skimmer.

97

W późnych latach dziewięćdziesiątych złodzieje w dużych amerykańskich miastach zaczęli szukać kelnerów, kelnerek i pracowników drive-through, któ-

rzy chcieliby sobie dorobić. Zazwyczaj dostawali 10 dolarów za dane jednej karty. Mimo

że wiązało się to z większym ryzykiem, również pracownicy stacji benzynowych i sklepów mogli to robić, instalując małe skimmery w czytnikach przy dystrybutorach paliwa lub w czytnikach terminali. Część danych była wykorzystywana na miejscu, ale większość z nich wysyłano do Europy Wschodniej, gdzie sprzedawano je w Internecie po dziesięć, dwadzieścia, sto lub nawet kilka tysięcy naraz.

Carderzy nazywali je „zrzutami", każdy z nich zawierał tylko dwie linijki tekstu - po jednej na każdą ze ścieżek wydrukowanych na ośmiocentymetro-wym pasku magnetycznym na karcie kredytowej.

Track 1: B4267841463924615ASMITH/

DEFFREYA041010127352005210000000

Track 2: 4267841463924615=041010127352521

Zrzut był wart około 20 dolarów w wypadku standardowej karty, 50 w wypadku złotej karty i od 80 do 100 dolarów w przypadku firmowej karty z wysokim limitem.

Chris zdecydował, że sam spróbuje cardingu. Stwierdził, że Script, ojciec chrzestny CarderPlanet, jest najrzetelniejszym źródłem zrzutów w świecie.

Zapłacił Ukraińcowi 800 dolarów za dwadzieścia numerów kart Visa Classic, inwestując też blisko 500 dolarów w MSR206, ulubiony podziemny koder pa-sków magnetycznych.

Kiedy już z Maksem podłączyli mający wielkość pudełka po butach MSR206 do jego komputera i zainstalowali właściwe oprogramowanie, Chris mógł wziąć anonimową kartę Visa, którą dostał, lub jedną z własnych kart kredytowych i zakodować ją dwoma szybkimi posunięciami, używając jednego ze zrzutów kupionych od Scripta.

Z przeprogramowaną kartą w kieszeni Chris niecierpliwie rozglądał się po miejscowym Blockbusterze i kilku innych sklepach, by ocenić możliwości.

98

Proste oszustwo przy użyciu paska magnetycznego może być tanie i łatwe, ale ma poważne ograniczenia. Szybko stwierdził, że kupowanie sprzętu elektronicznego lub drogich ubrań będzie trudne. Aby zapobiec temu, nad czym Chris właśnie się zastanawiał, wiele ekskluzywnych sklepów wymagało od kasjera wpisania czterech ostatnich cyfr z awersu karty kredytowej. Czytnik terminalu

- w najlepszym razie - odrzuca ją, jeśli cyfry nie pasują do tych, które znajdują się na pasku. Przeprogramowana karta była dobra tylko w miejscach, gdzie pracownicy nigdy nie dotykali plastiku, jak stacje benzynowe czy sklepy spo-

żywcze.

Chris zrobił pierwszy krok w miejscowym supermarkecie. Załadował wó-

zek tym, co mu się nawinęło pod rękę, i przeciągnął swój plastik przez terminal. Po chwili słowo „przyjęte" zamigotało na wyświetlaczu i gdzieś w Ameryce konto przypadkowego klienta zostało obciążone 400 dolarami za artykuły spożywcze.

Aragon dostarczył nielegalnie zdobyte dobra małżeństwu z Orange County, które znajdowało się w gorszej sytuacji finansowej niż on sam, a następnie zabrał męża -

przedsiębiorcę, któremu ostatnio skradziono narzędzia budowla-ne - do lokalnego Walmartu, aby kupić mu nowe. Rozeszła się wieść, że Chris ma karty kredytowe, i wkrótce udostępnił je kilku przyjaciołom, którzy zawsze dbali o to, aby w ramach podziękowań zrobić dla niego małe zakupy.

Widział zarysy biznesplanu w swym krążącym plastiku. Nie zajmuj się już niczym innym, powiedział Maksowi, naprawdę można zarobić na zrzutach.

ROZDZIAŁ 12

Darmowy Amex!

Max podzielił się swym planem z Charity w czasie obiadu złożonego z sushi.

„Które instytucje zasługują twoim zdaniem na największą karę?" - spytał.

Właściwie już miał odpowiedź: te które pożyczają pieniądze. Chciwe banki i firmy wydające karty kredytowe, które każdego roku obciążają klientów 400

miliardami dolarów długu, pobierając lichwiarski procent i łowiąc na plastik dzieciaki, które jeszcze nie skończyły szkoły średniej. Ponieważ klienci nigdy bezpośrednio nie ponosili strat spowodowanych z oszustwami - zgodnie z prawem mogli być obciążeni tylko do 50 dolarów, a większość banków rezygnowała nawet z tego - przestępstwa związane z kartami kredytowymi nie miały ofiar, obciążając kosztami jedynie bezduszne instytucje.

Kredyt nie był czymś prawdziwym, dowodził Max, ale po prostu abstrak-cyjną koncepcją. Będzie kradł numery w systemie, nie dolary z czyjejś kieszeni. Uderzy to w instytucje finansowe, a one właśnie na to zasługują.

Charity nauczyła się akceptować rozgoryczenie, które Max wyniósł z wię-

zienia. Mieszkając z nim, nie mogła oglądać filmów kryminalnych, 100

ponieważ każdy policjant będący pozytywnym bohaterem sprawiał, że Max dostawał białej gorączki. Nie była całkiem pewna, jakie są jego zamiary… i nie chciała o nich nic wiedzieć. Ale jedno było pewne: jej chłopak postanowił zostać Robin Hoodem.

Max dobrze wiedział, skąd wyciągnąć dane z pasków magnetycznych, których chciał Chris. Na CarderPlanet i Shadowcrew jak na dłoni leżały tysiące potencjalnych źródeł. Ofiarą padną sami carderzy.

Większość z nich nie była hakerami, lecz zwykłymi oszustami; wiedzieli trochę o przekrętach, ale niewiele o bezpieczeństwie komputerowym. Z pewnością nie będą trudniejsi do znakowania niż Pentagon. Była to również propozycja do zaakceptowania moralnie: będzie podbierał numery kart kredytowych, które już zostały skradzione - przestępcy mieli zamiar ich użyć, więc równie dobrze mógł to zrobić jego wspólnik Chris Aragon.

Zaczął od wyboru broni, decydując się na krążącego już w sieci sprawdzo-nego Bifrost Trojana. Podrasował go odpowiednio, aby nie został wykryty przez programy antywirusowe. Aby sprawdzić rezultaty, użył VM-ware, oprogramowania do emulacji komputera, by uruchomić na swym komputerze dziesięć różnych wirtualnych Windowsów jednocześnie, na każdym umieszczając nieco inne oprogramowanie zabezpieczające.

Kiedy malware nie został wykryty na żadnym z nich, przeszedł do następnego etapu - zebrania listy numerów ICQ carderów i adresów mailowych z postów na publicznym forum, których tysiące zgromadził w swej bazie danych.

Następnie, podszywając się pod dobrze znanego sprzedawcę o nicku Hum-mer911, wysłał wiadomość na wszystkie adresy z listy. Oznajmiał w niej, że zgromadził więcej zrzutów American Express, niż może użyć lub sprzedać, więc część z nich chce rozdać. Kliknij tutaj, by dostać darmowy Amex.

Kiedy carder kliknął na link, jego oczom ukazywała się stworzona przez Maksa lista fałszywych zrzutów, a w tym czasie ukryty na stronie kod wykorzystywał luki w nowym Internet Explorerze.

101

Exploit bazował na tym, że Internet Explorer może obsługiwać więcej niż tylko strony WWW. W1999 roku Microsoft dodał wsparcie dla nowego typu plików znanych jako aplikacja HTML - plik stworzony przy użyciu tych samych języków znaczników i języków skryptowych używanych przez strony WWW, które mogą robić na komputerze użytkownika coś, na co nigdy nie pozwolono by stronom WWW, na przykład tworzyć i kasować pliki i wykonywać arbitralne polecenia. Pomysł polegał na pozwoleniu projektantom już przyzwyczajonym do programowania na użytek Internetu wykorzystania tych samych umiejętności do stworzenia w pełni funkcjonalnych aplikacji na pecety.

Internet Explorer rozpoznaje, że aplikacje HTML mogą stanowić śmiertelne zagrożenie, i nie obsługuje ich z sieci, lecz jedynie z twardego dysku użytkownika. Teoretycznie.

W praktyce Microsoft zostawił dziurę w sposobie, w jaki przeglądarka wy-

świetla zawartość wbudowaną w stronę WWW. Wiele stron internetowych zawiera tagi OBJECT, będące prostymi instrukcjami nakazującymi przeglądarce ściągnięcie czegoś z innego adresu w sieci - zazwyczaj pliku filmowego lub muzycznego - i włączenie go jako części własnej strony. Okazało się jednak, że można także załadować aplikację HTML przez tag OBJECT i że polecenie to zostanie wykonane. Trzeba się tylko trochę przebrać.

Podczas gdy ofiary Maksa śliniły się nad fałszywymi zrzutami American Express, niewidoczny tag OBJECT nakazał ich przeglądarkom wpuszczenie złośliwego HTML-a. Aplikacji, którą Max stworzył na tę okazję. Co najważ-

niejsze, Max nadał aplikacji nazwę kończącą się „.txt” - pozornie wskazującą, że jest to zwykły plik tekstowy. Internet Explorer widział ten plik i decydował, że jego uruchomienie jest bezpieczne.

Kiedy już jednak przeglądarka zaczęła ściągać plik, serwer Maksa przesyłał

wskaźnik typu zawartości „application/hta” - identyfikujący go teraz jako aplikację HTML. W istocie serwer Maksa zmienił jego historię, przedstawiając ten plik jako nieszkodliwy dokument służący sprawdzeniu bezpieczeństwa 102

przeglądarki, a następnie poprawnie zidentyfikował go jako aplikację HTML, kiedy nadszedł czas, by przeglądarka zdecydowała, jak zinterpretować plik.

Oceniwszy plik jako bezpieczny, opierając się na jego nazwie, Internet Explorer nie

weryfikował tego stwierdzenia, kiedy poznał prawdę. Po prostu uruchomił kod Maksa jako aplikację HTML zamiast strony internetowej.

Aplikacja HTML Maksa była zwartym skryptem Visual Basic, który zapisał

i uruchomił mały program będący hakiem abordażowym na komputerze użytkownika. Max nazwał ten hak „hope.exe". Hope było drugim imieniem Charity.

Hak abordażowy ściągnął i zainstalował zmodyfikowanego Bifrost Trojna. I w ten właśnie sposób Max opanował komputer.

Carderzy rzucili się na zatrutą stronę jak wygłodniałe piranie: setki ich komputerów na rozkaz wysłało raporty do Maksa. Podniecony, zaczął na oślep skakać po twardych dyskach przestępców. Był zaskoczony tym, jak amatorsko to wy-glądało. Większość z jego ofiar kupowała małe ilości zrzutów, 10-20 naraz, czasem nawet mniej. Carderów było wielu i nic nie powstrzymywało Maksa od ciągłego powracania do ich komputerów. W końcu akcja „darmowy Amex" przyniesie mu około 10 000 zrzutów.

Znalezione zrzuty przesłał Chrisowi, a przy okazji wyciągnął od swych ofiar także inne ważne dane - szczegóły ich oszustw, informacje na temat skradzionych tożsamości, hasła, listy mailingowe używane w przekrętach phishingowych, trochę prawdziwych nazwisk, zdjęcia, adresy mailowe i ICQ ich przyjaciół - przydatne do przyszłych ataków na podziemie.

Zastawiwszy dobrze przygotowaną pułapkę, został teraz w niewidzialny sposób włączony w ekosystem carderów. To był początek czegoś wielkiego.

Będzie rabusiem wśród carderów, żyjącym z tego, co uda mu się zebrać z ich nielegalnej działalności. Jego ofiary nie mogą zadzwonić na policję, a mając 103

anonimowe podłączenie do Internetu i inne środki ostrożności, będzie odporny na odwet.

Dość szybko jednak Max przekonał się, że nie każdy carder jest tym, kim się wydaje.

Kolejna ofiara była z Santa Ana. Kiedy Max wszedł do jej komputera przez tylne drzwi i zaczął grzebać dookoła, od razu zobaczył, że coś było nie tak.

Na komputerze działał program Camtasia gromadzący zapisy wideo wszystkiego, co pojawiło się na monitorze - nie były to informacje, które przestępcy zazwyczaj chcą archiwizować. Max przetrząsnął twardy dysk i jego podejrzenia się sprawdziły: było tam pełno raportów FBI.

Chris był wstrząśnięty odkryciem agenta FBI na swoim własnym podwórku, ale Maksa to intrygowało - twardy dysk agenta oferował potencjalnie użytecz-ny wgląd w metody biura. Zastanawiali się, co dalej robić. Pewne pliki wskazywały na to, że tajniak ma współpracownika dostarczającego informacji o Scripcie, przywódcy CarderPlanet, który sprzedał Chrisowi pierwsze zrzuty.

Czy powinni ostrzec Scripta, że w jego kręgu działała policyjna wtyczka?

Zdecydowali, że nic nie zrobią; jeśli kiedykolwiek mnie złapią, myślał Max, mogę wykorzystać to jako atut. Gdyby wyszło na jaw, że przypadkowo zhakował agenta FBI, mogłoby to skompromitować biuro, a może nawet skończyło-by się to dla jego pracowników jakimiś karami.

Powrócił do hakowania carderów. Teraz wiedział, że nie jest jedynym out-siderem penetrującym przestępcze forum.

ROZDZIAŁ 13

Villa Siena

Wejście do Villi Siena, rozległego zamkniętego osiedla położonego niecały kilometr od John Wayne Airport, otaczały palmy. Za frontową bramą inspirowane europejską sztuką fontanny bulgotały pośród starannie wypielęgnowa-nych dziedzińców, obok cztery baseny połyskiwały błękitem pod słonecznym niebem południowej Kalifornii. Mieszkańcy mogli się bawić w klubach, relaksować w spa, ćwiczyć w jednej z trzech sal fitness lub odwiedzić całodobową portiernię, aby ułożyć plan na wieczór.

W przestronnym apartamencie Chris Aragon prowadził swoją fabrykę. W

jednym z gigantycznych okien spuszczono zasłony, aby ukryć stertę maszyn wypełniających stoły z Ikei i granitowe blaty. Chris włączył drukarkę kart, która ruszyła z jęczącym dudnieniem rozpędzających się kółek i silników cią-

gnących taśmy napięte jak struny.

Max ściągał teraz zrzuty regularnie, a gdy coś wpadło mu w ręce, należało to wykorzystać jak najszybciej - dane były własnością podwójnie skradzioną i Chris musiał wypalić je w plastiku, zanim oszuści, którzy kupili lub zhakowali numery, wyczyszczą konta lub popełnią błąd prowadzący do zablokowania 105

kart. Chris naruszył swoje ostatnie rezerwy, by zainwestować w warty około 15

000 dolarów sprzęt do drukowania kart i lokal do jego użytkowania. Teraz inwestycja przynosiła zyski.

Chris włożył prostokątny kawałek PCW do podajnika niezgrabnej, kancia-stej maszyny Fargo HDP600, drukarki kart wartej 5000 dolarów używanej do drukowania firmowych kart identyfikacyjnych. Za sprawą jednego kliknięcia na laptopie maszyna wciągała kartę w swe wnętrzności i brzęczała: raz, drugi, trzeci, czwarty. Każdy dźwięk oznaczał nakładanie kolejnego koloru na powierzchni karty, podczas gdy przesuwał się on po czystym pasku transmisyj-nym i był błyskawicznie odparowywany przez elementy ogrzewające kartę.

Końcowe niskie rzężenie fargo oznaczało, że na plastik nakładana jest przezro-czysta warstwa laminatu.

Od początku do zakończenia procesu upływały 44 sekundy i maszyna wypluwała kartę - pokryte błyszczącymi żywymi kolorami konsumenckie dzieło sztuki. Widniał na niej amerykański orzeł bielik wpatrzony w logo Capital One, ponury centurion American Express lub plama błękitnego nieba na bia-

łym tle, jeśli była to należąca do Sony MasterCard. Proces wyglądał tak samo w wypadku kart o wysokim limicie, z tym wyjątkiem że Chris czasem zaczynał

od pomalowanego na srebrno lub złoto kawałka PCW zakupionego, podobnie jak czyste karty, w pudełkach po sto sztuk.

Kiedy już miał plik świeżo wydrukowanych kart w dłoni, przechodził do następnego etapu produkcji: uruchomienia jednobarwnej drukarki służącej do tworzenia delikatnych

elementów na rewersie karty. Następnie, jeśli potrzebny był hologram, rozrywał opakowanie wyprodukowanych w Chinach podróbek właściwego surowca, delikatnie kładł jedną z płytek na wbijaku i pociągał

dźwignię, by wyciąć owalny lub zaokrąglony kształt rozmiarów znaczka pocz-towego. Kupiona za 2000 dolarów wypalarka Kwikprint Model 55, przypominająca wiertarkę pionową skrzyżowaną ze średniowiecznym narzędziem tortur, pokrywała metalową folią powierzchnię PCW.

Potem przychodziła pora na embosser: gigantyczne napędzane silnikiem ko-

ło karuzeli pokryte literami i cyframi, które wydawało dźwięk jak maszyna 106

do pisania IBM Selectric, kiedy litera po literze wybijało w plastiku nazwisko, numer konta i datę wygaśnięcia, pokrywając każdą z nich srebrną lub złotą folią. Od chińskiego dostawcy Chris otrzymał specjalny kod bezpieczeństwa do Visy: „latające V" i połączone „MC" MasterCard. Dwa charakterystyczne znaki, które można znaleźć tylko na kartach kredytowych, prawdziwych i fałszywych.

System weryfikacji kart kredytowych nie sprawdza nazwiska klienta, co oznaczało, że Chris mógł na awersie swego plastiku umieścić dowolny pseudonim. Na kartach, których sam używał, lubił mieć wydrukowane „Chris Anderson". Na swym komputerze Chris przeredagowywał zrzuty Maksa, by dopasować nazwisko na pasku magnetycznym do widniejącego na awersie - tak dobrze się składało, że nazwisko było jedyną częścią danych na pasku magnetycznym, której nie używano w obliczaniu kodu bezpieczeństwa CW, więc mógł je zmieniać wedle upodobań.

Na końcu trzeba było jeszcze dwa razy przeciągnąć kartę przez niezawodny MSR206, aby zaprogramować zrzuty Maksa na pasku magnetycznym, i po-dróbka, która niemal w każdym szczególe była kopią plastiku znajdującego się w portfelu bądź portmonetce gdzieś w Ameryce, była gotowa.

Ale to jeszcze nie wszystko.

W razie zakupów na dużą kwotę należało mieć przy sobie prawo jazdy.

Dzięki swej linii produkcyjnej i lekcjom pobranym na Shadowcrew Chris radził sobie także z tym. Gdy robił prawo jazdy, przerzucał się z PCW na teslin, cieńszy, bardziej elastyczny materiał, sprzedawany w arkuszach 21,6 na 28

centymetrów. Jeden arkusz na wierzch, drugi na spód - to wystarczyło na dziesięć prawek.

Kalifornijskie prawo jazdy posiadało jeszcze dwa elementy, które wymaga-

ły dodatkowego hakowania. Przezroczysta pieczęć stanu Kalifornia, umiesz-czona jako powtarzający się wzór na czystym laminacie ponad środkową czę-

ścią prawa jazdy. Aby ją skopiować, Chris użył pearl eksu - delikatnego kolo-rowego pudru, który można kupić w sklepach dla plastyków i rzemieślników za 107

mniej niż trzy dolary za słój. Trik polegał na tym, by posypać arkusz laminatu mieszanką srebrnego i złotego pearl eksu, włożyć go do drukarki napełnionej jasnym atramentem i wydrukować zwierciadlane odbicie wzoru Kalifornii przezroczystym atramentem. Nie ma znaczenia, że atrament jest niewidoczny -

istotna była rozgrzana głowica drukarki. Kiedy arkusz wchodził, wysoka tem-peratura odbijała ten wzór na powierzchni, a pearl ex można było łatwo zmyć, spłukując kartę zimną wodą.

Ultrafioletowe drukowanie na przedniej stronie prawa jazdy nie sprawiało problemu. Wystarczała do tego zwykła drukarka atramentowa, pod warunkiem że odciągnęło się atrament z kartridża i wypełniło go ultrafioletowym atramentem sprzedawanym w tubkach.

Po całym sypaniu, drukowaniu i myciu zostały Chrisowi cztery arkusze materiału. Włożył dwa arkusze zadrukowanego teslinu między laminat i przepu-

ścił je przez ciśnieniowy laminator. Po docięciu rezultat był imponujący. Przejedź palcami po prawie jazdy, a poczujesz doskonale jedwabną powierzchnię, potrzymaj ją pod kątem, a zobaczysz przezroczystą pieczęć stanową, połóż je pod ultrafioletową żarówką, a błyśnie flaga stanu: słowa „Republika Kalifornii” na czerwono, a nad nimi brązowy niedźwiedź chodzący na czterech łapach po żółtym wzgórzu.

Kiedy karty i prawa jazdy były gotowe, Chris wykonał kilka telefonów i zebrał swoje dziewczyny. Uważał, że najlepiej nadają się do tej roboty atrakcyjne dwudziestolatki. Do ekipy należały: Nancy, mierząca metr sześćdziesiąt Laty-noska z wytatuowanym na nadgarstku słowem „love”; Lindsay, blada dziewczyna o brązowych włosach i orzechowych oczach; Adrian, młoda Włoszka; i Jamie, która pracowała jako kelnerka w Hooters w Newport Beach.

W Villi Siena spotkał mieszkające tam dwie bliźniaczki, brunetki Liz i Michelle Esquere. Michelle tylko kręciła się razem z grupą, ale Liz okazała się bardzo przydatna. Pracowała w agencji udzielającej kredytów hipotecznych, była inteligentna, dobrze wykształcona i wystarczająco odpowiedzialna, by wziąć na siebie część prac administracyjnych, takich jak prowadzenie list wy-płat, jako dodatkowego zajęcia obok robienia zakupów.

Chris miał talent do dobierania pracownic. Mógł poznać nową kandydatkę w restauracji i zaprosić ją na imprezę z przyjaciółmi. Chodziła z nimi po klubach i na drogie obiady, jeżdżąc wynajętą limuzyną, kiedy jedno z nich świę-

towało urodziny. Widziała pieniądze wszędzie. Następnie, kiedy nadszedł wła-

ściwy moment, może po upływie miesiąca lub kiedy dziewczyna wyznawała, że ma rachunki do zapłacenia albo zalega z czynszem, Chris jak gdyby nigdy nic napomykał, że zna sposób na szybki i łatwy zarobek. Kiedy pytała o szczegóły, wyjaśniał, że to przestępstwo bez ofiary, dodając, że „uderza wyłącznie w system”.

Żadna z dziewczyn nie wiedziała, skąd Chris bierze dane swoich kart kredytowych. Kiedy mówił o Maksie, nazywał go „Whizem”, superhakerem, którego nie miały przywileju nigdy spotkać. Tajnym imieniem Chrisa było „The Dude”. Teraz, kiedy interes kwitł, Dude płacił Whizowi za zrzuty około 10 000

dolarów miesięcznie - przelewając pieniądze przy użyciu prepaidowej karty debetowej Green Dot.

Przeznaczona dla studentów i klientów z małymi zdolnościami kredytowymi Green Dot

Visa lub MasterCard jest kartą kredytową bez kredytu. Klient spłaca ją awansem, przelewami z konta bankowego lub gotówką. Dzięki tej ostatniej możliwości stała się ona idealnym rurociągiem finansowym łączącym mieszkającego w Orange County Chrisa z Maksem w San Francisco. Chris wpadał do pobliskiego 7-Eleven lub Walgreens i kupował numer doładowania Green Dot, zwany MoneyPak, za jakąkolwiek sumę do 500 dolarów. Następnie komunikatorem internetowym lub mailem wysyłał numer Maksowi, który używał go z jedną ze swych kart Green Dot na stronie firmy. Mógł potem pła-cić kartą za zakupy lub wybierać pieniądze z bankomatów w San Francisco.

Kiedy już jego załoga się pojawiła, gotowa do pracy, Chris rozdał dziew-czynom karty classic z niskim limitem oraz srebrne i złote z wysokim limitem.

Tymi pierwszymi mają płacić za drobne zakupy, mniej więcej do 500 dolarów, przypominał im. Kart z wysokim limitem powinny używać w wypadku drogich rzeczy, od 1000 do 10 000 dolarów. Wszystkie dziewczyny miały niewiele 109

ponad dwadzieścia lat, ale ich elegancka młodość uprzywilejowanych panien z Orange County sprawiała, że mogły wejść do Nordstroma i zgarnąć kilka torebek Coacha po 500 dolarów sztuka, nie budząc zdziwienia, a potem przejść na drugą stronę centrum handlowego i zrobić to samo w Bloomingsdale'u.

Nowe dziewczyny zawsze na początku były nerwowe, lecz kiedy tylko pierwsza transakcja fałszywą kartą się powiodła, łapały bakcyla. Błyskawicznie wysyłały Chrisowi entuzjastyczne esemesy ze swych zakupowych wycieczek:

„Czy możemy używać Ameksa w nowym Bloomingdale'u?" albo „Łał! Zrobi-

łam ponad 7 tysi na mc".

Pod koniec dnia spotykały się z Chrisem na parkingu i przekładały torby z bagażnika do bagażnika. Płacił im na miejscu 30 procent wartości detalicznej i starannie zapisywał transakcje na arkuszu wypłat jak prawdziwy biznesmen.

Damskie torebki, eleganckie ubrania i zamszowe kozaki ze sprzączkami trafia-

ły do pudełek, czekając na moment, kiedy Clara, żona Chrisa, znalazła na nie klientów na eBayu.

Kiedy nad Villa Siena zapadała noc, nad kortami tenisowymi błyskały światła i zapalały się ogrodowe kominki. Wiele kilometrów dalej Chris siedział ze swą ekipą w eleganckim lokalu, świętując kolejny sukces przy kolacji i butelce wina. Jak zwykle on stawiał.

ROZDZIAŁ 14

Nalot

„Ładny telewizor” - powiedział Tim, podziwiając sześćdziesięciojednocalową plazmę Sony wiszącą na ścianie. Charity, nałogowa czytelniczka, nienawidziła płaskiego ekranu, który zdominował living room w ich nowym mieszkaniu, ale Max lubił gadżety, a ten był czymś więcej niż tylko zabawką o wysokiej rozdzielczości. Był symbolem ich uzyskanego właśnie finansowego bezpieczeń-

stwa.

Przyjaciele Maksa wiedzieli, że znalazł jakieś zajęcie, i to nie tylko dlatego że już nie walczył, by jakoś związać koniec z końcem. Max zaczął wsuwać Timowi CD-ROM-y z ostatnimi exploitant z podziemia, dzięki czemu ten jako administrator systemu mógł lepiej zadbać o bezpieczeństwo komputerów w pracy. Potem Max zaczął rzucać dziwne komentarze na comiesięcznych obia-dach Głodnych Programistów w Jing Jing w Palo Alto. Kiedy każdy opowiedział o swoich najnowszych projektach, on stwierdzał tylko tajemniczo, z zazdrością w głosie: „Super, chciałbym robić coś konstruktywnego”.

Nikt jednak nie naciskał, by zdradził szczegóły swego nowego przedsię-

wzięcia: mogli tylko żywić nadzieję, że jest to coś choćby półlegalnego.

Mimo że ciągle obracał się w ich kręgu, skrupulatnie unikał obarczania przyjaciół wiedzą o swym podwójnym życiu. Przynajmniej do momentu kiedy jedna z ofiar jego ataków nie poszła za nim do domu.

Dochodziła 6.30 rano i ciągle jeszcze było ciemno, kiedy Chrisa Toshoka obudził dźwięk dzwonka przy drzwiach - długie ciągłe brzęczenie, jakby ktoś trzymał kciuk na przycisku. Myśląc, że to pijany sąsiad, Toshok obrócił się na drugi bok i próbował zasnąć. Brzęczenie przeszło jednak w natarczywe ryt-miczne *bzzz, bzzz, bzzz,* jak sygnał zajętego telefonu. Niechętnie wypełzł z łóż-

ka, złapał spodnie i koszulkę i półprzytomny zszedł na dół.

Kiedy otworzył drzwi, zmrużył oczy pod ostrym światłem latarki.

- Czy pan nazywa się Chris Toshok? - spytał kobiecy głos.

-Tak.

- Jesteśmy z FBI. Mamy nakaz przeszukania domu.

Agentka - długowłosa blondynka - pokazała Toshokowi swą odznakę i wcisnęła świstek papieru w jego dłoń. Drugi agent położył ciężką rękę na jego ramieniu i wyprowadził go do przedsionka, robiąc przejście grupie ludzi w garniturach, którzy zalali dom. Postawili na nogi współspacza Toshoka i zaczę-

li przetrząsać sypialnię Chrisa, przerzucając książki na półkach i grzebiąc w jego bieliźniarce.

Blondynka wraz z agentem służb specjalnych usiedli obok Toshoka, żeby wyjaśnić mu, dlaczego tu przyszli. Przed czterema miesiącami z komputerów Valve Software w Bellevue w stanie Waszyngton został skradziony kod źró-

dłowy niewydanej pierwszoosobowej strzelania *Half-Life 2.* Najpierw pojawił

się na chwilę w IRC-u, a potem na serwisach służących wymianie plików.

Half-Life 2 był prawdopodobnie najbardziej oczekiwaną grą wszech czasów i pojawienie się tajnego kodu źródłowego zelektryzowało świat graczy. Valve ogłosiła, że będzie zmuszona do opóźnienia premiery gry, a dyrektor generalny firmy publicznie wezwał fanów *Half-Life* do pomocy w wyśledzeniu 112

złodzieja. Dokonując szacunków na podstawie sprzedaży oryginalnej gry, Valve wyceniła oprogramowanie na ćwierć miliarda dolarów.

Agentka wyjaśniła, że FBI wytropiło ślady hakowania prowadzące do internetowego adresu IP w tym starym domu. Sędzia będzie łagodniejszy, jeśli Toshok powie im, gdzie ukrył kod źródłowy.

Tosohok zarzekał się, że jest niewinny, przyznał jednak, że wie o włamaniu.

Jego dawny przyjaciel Max Vision mieszkał z nim w czasie, kiedy doszło do tej kradzieży, i był bardzo podniecony, gdy kod źródłowy pojawił się w sieci.

Słysząc nazwisko Maksa Visiona, agenci zaczęli pracować na wyścigi, chcąc jak najszybciej skończyć rewizję, wrócić do biura i przygotować nakaz przeszukania nowego mieszkania Maksa. Chris patrzył ponuro, kiedy zabierali jego dziewięć komputerów, płyty z muzyką i Xboksa. Blondynka zauważyła jego minę. „Tak - powiedziała - to nie będzie przyjemne”.

Kiedy Max usłyszał o nalocie, wiedział, że nie ma zbyt wiele czasu. W po-

śpiechu zaczął ukrywać sprzęt. Zewnętrzny dysk twardy schował w szafie pod stertą swetrów, drugi w pudełku płatków śniadaniowych. Jeden z laptopów wcisnął pod sofę, drugi powiesił za oknem w łazience, chowając go w worku na śmieci. Wszystkie wrażliwe dane na jego komputerze były zaszyfrowane, więc nawet gdyby agenci znaleźli sprzęt, nie mieliby żadnych dowodów na hakowanie. Ale biorąc pod uwagę wymogi jego warunkowego zwolnienia, nie mógł używać szyfru. Co więcej, byłoby naprawdę kiepsko, gdyby FBI zabrało wszystkie jego komputery.

Federalni pojawili się licznie - aż dwudziestu agentów roiło się jak mrówki po mieszkaniu. Znaleźli tylko typowe atrybuty komputerowego geeka z San Francisco z hipisowskimi skłonnościami: półkę, na której stał *Rok 1984* Orwel-la, *Nowy wspaniały świat* Huxleya, klasyk *science fiction* Orsona Scotta Carda *Gra Endera* i trochę Asimova oraz Carla Sagana. Były tam jeszcze rower i walające się wszędzie pluszowe pingwiny. Max je uwielbiał.

Agenci nie odnaleźli ani jednej z kryjówek, a tym razem haker nie miał nic do powiedzenia. Wyszli bez żadnych dowodów, które łączyłyby Maksa z włamaniem do Valve, ani nie znajdując śladów jego przestępczej działalności z Chrisem. Zobaczyli tylko

stertę CD-ROM-ów, uszkodzony twardy dysk i komputer Vanilla Windows, zostawiony dla odwrócenia uwagi.

Ale Charity właśnie się dowiedziała, co oznacza życie w świecie Maksa Visiona. Zarzekał się, że nie ma nic wspólnego z kradzieżą kodu źródłowego.

Zapewne była to prawda. Kilku fanów pierwszoosobowych strzelanek krążyło wokół dziurawych jak szwajcarski ser zabezpieczeń Valve, oczekując *Half-Life 2.* Max był tylko jednym z nich.

FBI złapało później innego hakera podejrzanego w sprawie Valve. Był nim dwudziestoletni Niemiec Axel „Ago" Gembe, który przyznał się do swoich włamań do maili dyrektora generalnego Valve, ale on także zaprzeczył, jakoby ukradł kod.

Gembe cieszył się już złą sławą jako twórca Agobota, pionierskiego robaka komputerowego, którego celem było coś więcej niż tylko mnożenie się. Kiedy Agobot przejął maszynę, użytkownik mógł nie zauważyć niczego poza lekkim spowolnieniem jej pracy. Ale głęboko w swej podświadomości pecet dołączał

do prywatnej armii hakera. Malware został zaprogramowany tak, aby automatycznie zalogować się w wybranym wcześniej czat roomie IRC-a, zgłosić swą obecność, a następnie czekać na przyjęcie poleceń od swego pana w kanale czatowym.

Tysiące komputerów odpowiadało w tym samym czasie, tworząc coś w rodzaju supermózgu zwanego botnetem. Za pomocą jednej linijki tekstu haker mógł aktywować keyloggery na wszystkich komputerach, by przechwycić ha-sła i numery kart kredytowych. Mógł kazać komputerom otworzyć tajne proxy maili, żeby wrzucić spam. Co gorsza, był w stanie wykorzystać wszystkie pecety do połączenia się równocześnie z wybraną stroną internetową - przeprowadzając atak DDoS (Distributed Denial of Service, zablokowanie poprzez 114

zajęcie wszystkich wolnych zasobów), który na wiele godzin kładł nawet najlepszą stronę, podczas gdy administratorzy sieci blokowali każdy z adresów IP

atakujących komputerów pojedynczo.

Ataki DDoS zaczęły się jako sposób na skłócenie hakerów, by wygryźli się nawzajem z IRC-a. W lutym 2000 roku piętnastoletni Kanadyjczyk Michael

„MafiaBoy" Calce zrobił eksperyment, programując swego botneta tak, by skutecznie zaatakował najczęściej odwiedzane strony WWW, jakie mógł znaleźć. Ofiarą padły CNN, Yahoo!, Amazon, eBay, Dell i E-Trade, co odbiło się szerokim echem w prasie i zaowocowało zwoływanymi w trybie pilnym zebra-niami ekspertów od bezpieczeństwa w Białym Domu. Od tamtej pory ataki DDoS nasiliły się, stając się jednym z największych problemów Internetu.

Boty takie jak Ago wyznaczyły największą innowację dekady w dziedzinie złośliwego oprogramowania, inaugurując epokę, w której każdy wkurzony skryptowy dzieciak mógł położyć część sieci WWW, jeśli miał na to ochotę.

Zeznania Gembego w sprawie hakowania Valve dostarczyły FBI rzadkiej okazji do schwytania jednego z innowatorów, na których ciążyła największa odpowiedzialność. FBI próbowało ściągnąć Gembego do Ameryki, kusząc go pracą w stylu Invity zaoferowaną

przez Valve. Po miesiącach negocjacji i telefonicznych rozmów o pracę z szefami Valve haker wydawał się gotowy, by wskoczyć do samolotu i wylądować w Stanach.

Ale wtedy wkroczyła do akcji niemiecka policja, aresztując hakera i oskar-

żając go na miejscu jako młodocianego przestępcę. Gembe został skazany na rok nadzoru sądowego.

Nalot na dom był dla Maksa szokiem, wypełniając jego głowę nieprzyjem-nymi wspomnieniami z rewizji FBI w sprawie ataków BIND. Stwierdził, że potrzebuje bezpiecznego domu w mieście, miejsca, w którym mógłby uprawiać swój proceder - czegoś takiego jak fabryka Chrisa w Villa Siena.

Pod przybranym nazwiskiem Chris wynajął dla Maksa drugie mieszkanie, przestronny penthouse w Fillmore District z balkonem i kominkiem - Max 115

lubił pracować przy ogniu i żartował, że w razie zagrożenia będzie mógł spalić dowody.

Starał się codziennie wracać do Charity, ale mając wygodny i bezpieczny hakerski dom, gdzie mógł być sam, zaczął znikać na całe dnie, pojawiając się, kiedy dziewczyna przerywała jego pracę ponaglającym telefonem.

- Koleś, czas wrócić do domu. Tęsknię za tobą.

Kiedy przedsięwzięcie Maksa i Chrisa zaczęło przynosić zyski, pojawił się również brak zaufania. Niektóre z dziewczyn Chrisa lubiły imprezować i ciągła obecność kokainy, ecstasy i trawki powracała do niego jak zapomniana melo-dia. W lutym zatrzymano go w pobliżu domu i aresztowano za jazdę pod wpływem. Zaczął regularnie znikać ze swymi atrakcyjnymi pracownicami na weekendowe bachanalia w Vegas: dzień był przeznaczony na zakupy, nocą Chris wciągał trochę koki i zabierał dziewczyny do Hard Rocka na imprezę lub rezerwował VIP-owski stolik w ekskluzywnym Ghostbar na szczycie Palms, gdzie wydawał 1000 dolarów na kolację i drugie tyle na wino. Po powrocie do Orange County znalazł sobie kochankę, osiemnastolatkę, którą poznał przez jedną ze swych dziewczyn.

Zarówno narkotyki, jak i niewierność małżeńska wywoływały u Maksa nie-smak. Ale tym, co naprawdę go wkurzało, były sprawy finansowe. Chris płacił

mu nieregularnie - ile mu się akurat spodobało i kiedy mu się spodobało. Max chciał dostawać równe 50 procent zysków. Był pewien, że Chris wyciągał z ich przedsięwzięcia dużo więcej.

Wspólnik próbował go uspokoić i wysyłał Maksowi maile z dokładnymi rozliczeniami kosztów i zysków. Na sto kart około pięćdziesięciu nadawało się do użytku, a tylko połowa z nich pozwalała na kupienie czegoś, co opłacało się sprzedać - reszta to plewy, karty z limitem bezpieczeństwa 500 dolarów, które nadawały się tylko do drobnych płatności za benzynę czy posiłki. Chris miał

również sporo wydatków - rozszerzenie terenu łowieckiego oznaczało, że jego drużyna musiała latać do odległych miast, a miejsca w samolotach nie taniały.

Płacił też za wynajem swej fabryki kart kredytowych w Villi Siena.

Nie przekonało to Maksa. „Oddzwoń, kiedy nie będziesz naćpany”.

Kroplą przepełniającą kielich goryczy było potknięcie Chrisa, który trzy miesiące po nalocie policji związanym z *Half-Life* sam o mały włos nie wpadł.

Jechał do San Francisco, by spotkać się z Maksem i zrobić kilka kursów z kartami w centrach Półwyspu. On i jego ekipa właśnie zajęli zarezerwowane są-

siadujące z sobą pokoje w W - eleganckim hotelu w dzielnicy Soma, kiedy Chris dostał telefon z recepcji. Jego karta kredytowa została odrzucona.

Chris, któremu kręciło się w głowie z powodu kaca i grypy, zjechał windą do marmurowego lobby i wyciągnął kolejną podrabianą kartę ze swego portfela. Patrzył, jak recepcjonistka przesuwa ją przez terminal. Znowu odmowa.

Wyciągnął trzecią, ta zadziałała, ale dziewczyna zdążyła już nabrać podejrzeń i gdy Chris wracał na dwudzieste siódme piętro, podniosła słuchawkę i zadzwoniła do firmy oferującej karty kredytowe.

Po chwili do jego drzwi zapukali ludzie z policji San Francisco. Skuli go i przeszukali pokój i samochód, zabierając laptopa Sony, MSR206 i SUV-a, który miał fałszywy numer identyfikacyjny VIN - Chris eksperymentował z wynajmowaniem samochodów, używając swego plastiku w Las Vegas, a na-stępnie wysyłał je do Meksyku, by dopasować do nich czyste VIN-y.

Wylądował w więzieniu okręgowym. Jego zniknięcie zaniepokoiło Maksa, ale Chris wkrótce wyszedł za kaucją i przyznał mu się do błędu. Na szczęście policyjne śledztwo nie posunęło się dalej. Chris został miesiąc później skazany na trzy lata dozoru policyjnego, otrzymał też zakaz pojawiania się w W. Potem przechwalał się, że był beneficjentem liberalnego systemu sprawiedliwości w San Francisco.

To była tylko drobna wpadka, jedna z tych, które ciągle zdarzały się dziew-czynom Chrisa, dlatego właśnie opłacał poręczyciela od kaucji, a nawet pozwalał mu wpadać do fabryki w Villi Siena. Ale Max był wściekły. Dla kogoś z pozycją Chrisa wpadka przy płaceniu kartą za hotel była czymś niewybaczal-nym.

Max zdecydował, że nie może już dłużej polegać wyłącznie na swym wspólniku. Potrzebował planu B.

ROZDZIAŁ 15

UBuyWeRush

Chris zajechał pod zaniedbane małe centrum handlowe w środkowej części hrabstwa Los Angeles, która nie pojawia się na pocztówkach. Znajdowało się ono na obszernej równinie tak bardzo oddalonej od oceanu i wzgórz, że przy-sadzisty budynek pokryty stiukiem mógłby służyć za plan filmowy, z czystym niebem za nim jako błękitnym tłem, które w postprodukcji należało wypełnić górami lub drzewami.

Skierował samochód na zaśmiecony parking. Wielki szyld nad wejściem zapraszał do Cowboy Country Saloon, a pod nim można było zobaczyć typowy dla południowego Los Angeles miszmasz: sklep z alkoholem, lombard, salon kosmetyczny. Wśród nich znajdował się jeszcze jeden lokal, raczej niezwykły: UBuyWeRush (Wy kupujecie, my się sprężamy) - jedyny szyld w Los Angeles, który był także nickiem na CarderPlanet i Shadowcrew.

Wszedł do holu, gdzie puste okienko recepcji sugerowało, że ten wynajmowany za małe pieniądze lokal był kiedyś kliniką. Na ścianie wisiała naszpikowana pinezkami mapa świata w odwzorowaniu Mercatora. Następnie Chris został ciepło przywitany przez samego UBuya - Cesara Carrenzę.

119

Cesar dotarł do podziemia okrężną drogą. Ukończył DeVry Institute w 2001

roku z dyplomem programisty komputerowego, licząc na znalezienie pracy w branży internetowej. Kiedy to się nie powiodło, postanowił spróbować swoich sił w sieci jako niezależny biznesmen.

Z ogłoszenia w „Daily Commerce” dowiedział się o zbliżającej się aukcji w publicznych magazynach w Long Beach, gdzie właściciele sprzedawali zawartość opuszczonych schowków. Kiedy się pojawił, zaobserwował, że aukcja odbywała się według osobliwego rytuału. Menedżer, wymachując imponują-

cym szczypcami przegubowymi, odcinał kłódkę dotychczasowego najemcy i otwierał drzwi, podczas gdy licytujący próbowali zobaczyć, co jest w środku.

Mieli oni ocenić zawartość z miejsca, gdzie stali, z odległości ponad metra.

Zwycięzca zamykał miejsce własną kłódką i zabierał cały towar w ciągu 24

godzin.

Łatwo było dostrzec doświadczonych licytantów: z ich pasków zwisały kłódki, w dłoniach trzymali latarki, by zobaczyć, co kryje się w ciemnych schowkach. Cesar nie był tak dobrze przygotowany, ale równie zdeterminowany jak inni. Był jedynym licytantem przy pierwszym miejscu, zainteresowa-nym schowkiem pełnym starych ubrań za 1 dolara.

Sprzedał je na wyprzedaży garażowej i na eBayu za blisko 60 dolarów. Są-

dząc, że znalazł małą sympatyczną niszę, zaczął częściej bywać na aukcjach w magazynach i zamykanych firmach, zgarniając całe fury towaru i sprzedając go z czystym

zyskiem na eBayu. Pieniądze zainwestował w biznes, otwierając sklepik w centrum handlowym Long Beach, by móc brać od sąsiadów w komis meble biurowe i niemarkowe dżinsy, które sprzedawał w sieci.

To była dobra, uczciwa praca - w przeciwieństwie do jego poprzedniego za-jęcia. W latach dziewięćdziesiątych Cesar oszukiwał na kartach kredytowych.

Był szczęśliwszy, sprzedając na eBayu, ale wspomnienie skłoniło go do sprawdzenia, czy istnieje rynek dla urządzeń, których używał jako oszust. Zamówił

kilka MSR206 od producenta i wystawił je za pośrednictwem sklepu 120

UBuyWeRush na eBay-u. Był zaskoczony tym, jak szybko zostały rozchwyta-ne.

Później jeden z jego klientów powiedział mu o stronie, na której mógł naprawdę dużo sprzedać. Przedstawił Cesara Scriptowi, który zaakceptował

UBuyWeRush jako sprzedawcę na CarderPlanet. Cesar napisał wprowadzają-

cego posta 8 sierpnia 2003 roku. „Mam zamiar dostarczać towar wszystkim, którzy robią poważne interesy, więc jeśli potrzebujecie drukarek do kart, embosserów, tipperów, koderów, zgłoście się do mnie. Wiem, że to brzmi jak reklama, ale dla was będzie to BEZPIECZNE miejsce do robienia zakupów".

Biznes rozkręcił się z dnia na dzień. Cesar stworzył własną stronę, zaczął

sprzedawać na Shadowcrew, dostał numer 800 i przyjmował płatności przez egold oraz wirtualne waluty, preferowane przez carderów. Słynął ze świetnej obsługi klienta. Mając nabywców we wszystkich strefach czasowych, sumiennie odbierał każdy telefon, niezależnie od tego, czy ktoś dzwonił w dzień czy w nocy. Po drugiej stronie kabla zawsze były pieniądze.

Jako obrotny biznesmen gwarantował dostarczenie towaru jeszcze tego samego dnia. Nawiązał kontakty ze swoją konkurencją, więc jeśli nie miał czegoś na stanie, mógł kupić towar od innego sprzedawcy, by zrealizować zamówienie i zadowolić klienta. Tego typu strategiczne posunięcia wkrótce uczyniły z UBuyWeRush czołowego dostawcę sprzętu dla światowej społeczności hakerów i złodziei tożsamości. „Naprawdę dobry człowiek, świetnie się z nim robi interesy", napisał carder znany jako Fear, doradzając żółtodziobowi z Shadowcrew: „Nie rób numerów UBuyWeRush, bo to równy gość i będzie trzymał

informacje o tobie w sekrecie".

Cesar wkrótce poszerzył swą ofertę o setki różnych produktów, takich jak skimmery, aparaty do zdjęć paszportowych, czyste plastikowe karty, drukarki kodów paskowych, embossery, papier do drukowania czeków, kartridże z atramentem do kart magnetycznych, a nawet urządzenia do nielegalnego odbio-ru telewizji kablowej.

Sam sprzęt nie był nielegalny, pod warunkiem że jego nabywca nie miał

zamiaru wykorzystywać go niezgodnie z prawem. Cesar miał nawet kilku uczciwych klientów, którzy kupowali maszyny, by robić firmowe karty identyfikacyjne i bloczki na szkolne obiady.

Kiedy już sam nie nadążał z realizacją zamówień, zaczął zatrudniać ludzi do pracy w magazynie, pakowania i wysyłania sprzętu. Kiedy otworzyły się dodatkowe biura, rozbudował je, by zyskać więcej miejsca, w ten sposób stopniowo podwoił, a potem potroił powierzchnię, która znajdowała się w jego posiadaniu. Zafascynowany globalnym zasięgiem swojego niskonakładowego przedsięwzięcia, kupił ścienną mapę i za każdym razem kiedy wysyłał zamó-

wienie do nowego miasta, wbijał szpilkę w odpowiednie miejsce. Po sześciu miesiącach mapa była naszpikowana od Stanów Zjednoczonych i Kanady po Europę, Afrykę i Azję. Gęsty metalowy las wyrósł nad Morzem Czarnym.

Ukraina.

Chris zaprzyjaźnił się z Cesarem, zapraszał go nawet na kolacje wraz z pa-nią UBuyWeRush, swoją żoną Clarą i ich dwoma synami - dobrze wychowa-nymi dziećmi, które nie wstawały od stołu, dopóki nie zjadły deseru. Bardzo lubił kręcić się po biurze Cesara. Nigdy nie wiadomo, kto pojawi się w UBuyWeRush. Nadmiernie podejrzliwi carderzy, którzy bali się zamawiać służący do podrabiania sprzęt, pielgrzymowali do Los Angeles, by osobiście odebrać towar, otworzyć drzwi wejściowe przez rękaw, nie zostawiając odcisków palców, i zapłacić gotówką. Zagraniczni carderzy spędzający wakacje w Kalifornii zatrzymywali się tu tylko po to, by zobaczyć legendarny magazyn na własne oczy i uścisnąć dłoń Cesara.

Tego dnia blisko dwumetrowy haker z włosami spiętymi w kucyk, który przyszedł odebrać MSR206, był ostatnią osobą, jaką Chris spodziewał się zobaczyć w sklepie Cesara.

Chris był w szoku. Max ostatnio rzadko opuszczał San Francisco i nawet nie wspomniał, że ma zamiar wyjechać z miasta. Max był równie zaskoczony, widząc Chrisa. Speszeni wymienili uprzejmości.

Chris wiedział, że jest tylko jeden powód, dla którego Max wymknął się do Los Angeles, by kupić swój własny koder pasków magnetycznych - jego wspólnik miał dość dzielenia się swymi najbardziej wartościowymi danymi.

Max poznał sekret jednego z największych błędów w systemie bezpieczeństwa w historii bankowości, o którym większość klientów nigdy się nie dowiedziała, nawet jeśli carderzy wzbogacili się dzięki niemu o miliony dolarów.

Średniej wielkości Commerce Bank w Kansas City w stanie Missouri mógł

być pierwszym, w którym zorientowano się, co się dzieje. W 2003 roku kie-rownika odpowiedzialnego za bezpieczeństwo banku zaalarmowało odkrycie, że konta klientów były okradane na 10 000 do 20 000 dolarów dziennie za pośrednictwem bankomatów we Włoszech. Kiedy w poniedziałek przyszedł do pracy, zobaczył, że bank stracił przez weekend 70 000. Po zbadaniu sprawy dowiedział się, iż wszyscy klienci padli ofiarą ataków phishingowych, mają-

cych na celu zdobycie numerów kart debetowych i PIN-ów.

Ale coś tu nie grało: CVV miało zapobiegać właśnie takim przekrętom. Bez kodu

bezpieczeństwa CVV zaprogramowanego na pasku magnetycznym prawdziwej karty zdobyte przez phishing informacje nie powinny wystarczyć do skorzystania z żadnego bankomatu na świecie.

Zaczął kopać głębiej i odkrył prawdę: jego bank po prostu nie sprawdzał

kodów CVV przy wypłatach z bankomatów ATM i zakupach na karty debetowe, kiedy klient wprowadza PIN przy kasie. W rzeczywistości bank nie jest w stanie tego sprawdzać przez cały czas, nawet gdyby chciał: zewnętrzna sieć wykonująca usługę, z której korzysta bank, nie wysyła nawet tajnego kodu.

Włoscy phisherzy mogli w polu CVV zaprogramować cokolwiek i karta zosta-

łaby zaakceptowana jako prawdziwa.

Menedżer przeniósł bank do innej sieci i zaprogramował swe serwery na nowo, by zweryfikować CVV. Tajemnicze wypłaty z bankomatów ustały z dnia na dzień.

123

Commerce Bank to był dopiero początek. W 2004 roku prawie połowa amerykańskich banków, kas pożyczkowych i firm wydających karty kredytowe ciągle jeszcze nie dbała o sprawdzanie CVV przy transakcjach debetowych w bankomatach i dlatego właśnie amerykańskie skrzynki zalewały phishingowe maile, których celem było wyciągnięcie kodów PIN klientów banków nazywa-nych przez carderów „łatwymi do obskubania".

Citibank, największy pod względem liczby klientów amerykański holding bankowy, stał się główną ofiarą. „Ten mail został wysłany przez serwer Citibanku, by zweryfikować twój adres mailowy - pisano w mailu wysłanym z Rosji w czasie kampanii z września 2003 roku. - Musisz zakończyć ten proces, klikając na link poniżej i wpisując w małe okienko numer twojej karty bankomatowej lub debetowej Citibanku i PIN, którego używasz w bankomatach".

Bardziej wyrafinowany spam z 2004 roku wykorzystywał uzasadniony lęk przed cyberprzestępczością. „Ostatnio miało miejsce wiele prób kradzieży toż-

samości klientów Citibanku - pisano w mailu ozdobionym ikonografią Citi. -

Aby zabezpieczyć swoje konto, musisz zaktualizować PIN do karty bankomatowej/debetowej Citibanku". Po kliknięciu na link klient trafiał na doskonałą imitację strony Citibanku, hostowaną w Chinach, gdzie proszono go o ujawnienie danych.

Pozwalające na zdobycie gotówki PIN-y był świętym Graalem cardingu.

Największe sukcesy w tym poszukiwaniu odnosił King Arthur z CarderPlanet.

King, jak nazywali go przyjaciele, prowadził międzynarodową grupę, która specjalizowała się w atakowaniu klientów Citibanku, i był legendą w świecie cardingu. Jednemu z oficerów Kinga Arthura, amerykańskiemu imigrantowi z Anglii, wymknęło się kiedyś przy koledze, że King zarabia milion dolarów tygodniowo na swych operacjach na całym świecie. A był on tylko jednym z wielu wschodnioeuropejskich oszustów działających w Ameryce.

Max podłączył się do wyciągania pieniędzy z Citibanku na swój własny sposób: zainstalował trojana na dysku amerykańskiego pośrednika znanego jako Tux i zaczął

przejmować PIN-y i numery kont, które carder dostał od 124

swojego dostawcy. Po jakimś czasie skontaktował się ze źródłem - anonimo-wym facetem z Europy Wschodniej, który w mniemaniu Maksa był samym Kingiem Arthurem - i przyznał szczerze, co zrobił: Tux, napisał, zawinił zanie-dbaniem bezpieczeństwa: dla równowagi stwierdził też, co było nieprawdą, że okradał on swego dostawcę.

Dostawca błyskawicznie zakończył współpracę z Tuksem i zaczął dostarczać Maksowi swoje PIN-y, uznając go za swego nowego pośrednika.

Kiedy pierwsze PIN-y zaczęły napływać, Max przekazał je Chrisowi, który rzucił się na nie jak dziki. Wybierał po 2000 dolarów - dzienny limit w bankomatach - a potem wysyłał dziewczyny, by robiły debetowe zakupy w sklepach na karty z PIN-ami, dopóki konto nie zostało wyczyszczone do zera. Gwałcił

karty. Nie podobało się to Maksowi. Chodziło przecież o to, by dostać gotów-kę, a nie kupować rzeczy, które można było sprzedać za ułamek ich wartości.

Przy trochę subtelniejszym podejściu PIN-y mogły przynieść znacznie większy zysk.

Potem okazało się, że wcale nie potrzebuje już swego wspólnika do tej operacji.

Kiedy wrócił z UBuyWeRush ze swym własnym MSR206, sam wszedł w ten interes. Zaprogramował stertę kart Visa danymi konta i do każdej z nich przykleił fiszkę z PIN-em. Następnie siadał na rower lub szedł na długi spacer, klucząc po mieście, i odwiedzał bankomaty w miejscach, gdzie nie było kamer monitoringu.

Wstukiwał PIN, potem wybierał określoną sumę i szur, szur, szur - bankomat wypluwał gotówkę niczym automat do gry. Max chował pieniądze do kieszeni, zapisywał nowy, niższy bilans na fiszkach, a potem rozglądał się dyskretnie, by sprawdzić, czy nie zwrócił na siebie uwagi, zanim wyciągnął na-stępną kartę ze swej talii. Aby nie zostawiać odcisków palców na bankomacie, naciskał klawisze przez kawałek papieru lub paznokciami albo pokrywał

opuszki palców hydroksychinoliną - przezroczystym, lepkim antyseptykiem, sprzedawanym w drogeriach jako płynny bandaż New-Skin.

125

Max sumiennie wysyłał ustalony procent swych zysków do Rosji przez Western Union MoneyGram, tak jak umówił się z dostawcą. Teraz był uczciwym przestępcą, robiącym czyste interesy w podziemiu.

Wizyty w bankomatach raczej nie przypinały wyczynów Robin Hooda, ale Max znajdował moralną pociechę w tym, że podbieranie pieniędzy zawsze kończyło się zablokowaniem karty. Oznaczało to, że oszustwa zostały odkryte i Citibank był zmuszony wyrównać klientom szkody poniesione na skutek kradzieży.

Po kilku miesiącach Max całkiem nieźle się wzbogacił na stratach Citibanku: przeniósł się razem z Charity do wynajmowanego za 6000 dolarów miesięcznie domu w Cole Valley w San Francisco i zainstalował sejf na swe oszczędności: 250 000 dolarów w gotówce.

Jego zyski były tylko małą częścią strat powstałych w wyniku błędu CVV.

W maju 2005 roku analityk Gartnera przeprowadził badania 5000 konsumentów online i

ekstrapolując wyniki, stwierdził, że w przybliżeniu kosztowało to instytucje finansowe USA 2 miliardy 750 milionów dolarów. Tylko w ciągu roku.

ROZDZIAŁ 16

Operacja „Firewall”

Coś podejrzanego działo się na Shadowcrew.

Max nie angażował się zbytnio w życie czołowego cyberprzestępczego forum. Shadowcrew była dla niego tylko terenem łowieckim z mnóstwem łatwych do znakowania carderów. Ale w maju 2004 Cumbajohnny, jeden z adminów, przedstawił ofertę, która zwróciła uwagę Maksa. Cumba reklamował

nową usługę VPN dostępną tylko dla członków Shadowcrew.

VPN - wirtualna prywatna sieć - jest zazwyczaj używany do umożliwiania telepracownikom dostępu do sieci pracodawcy z domu. Ale godny zaufania podziemny VPN był atrakcyjny dla carderów z innego powodu. Korzystanie z tej usługi oznaczało, że każdy bajt wysyłany z komputera będzie zaszyfrowany

- odporny na wścibskie ISP lub agencje bezpieczeństwa mające pozwolenie na monitoring. Każda próba wytropienia aktywności carderów skończy się na centrum danych Cumbajohnnyego.

Cumbajohnny był nowym nabytkiem przywództwa Shadowcrew - byłym moderatorem, który zyskiwał władzę i wpływy, zmieniając klimat na stronie.

Inni admini skarżyli się na nowego podłego ducha na forum. Na górze strony 127

pojawił się baner: „Dość gadania. Róbcie interesy. Polecajcie swe usługi.

Skontaktujcie się z Cumbajohnnym”. Shadowcrew zaczynała przypominać nocny klub w Las Vegas - krzykliwe reklamy obiecywały rozrywkowe życie, piękne kobiety i całe sterty gotówki.

Gollumfun, wpływowy założyciel, ogłosił już publicznie swe odejście, kiedy inny założyciel BlackOps również napisał, że kończy działalność. „Shadowcrew straciła swój dawny charakter, stając się miejscem spotkań zdegene-rowanych dzieciaków, którym brak wiedzy, umiejętności lub chęci do kon-struktywnej współpracy z innym członkami. Dobre pomysły i rady przestały się pojawiać, odeszli wszyscy cieszący się szacunkiem członkowie i zniknęła życzliwość. Nie pomagamy już żółtodziobom w znalezieniu ich własnej drogi -

po prostu gnoimy ich, aż odejdą, a potem uskarżamy się, że nie ma żadnych nowych członków”.

„BlackOps, będzie nam ciebie brakować, dzięki za twe usługi - napisał kur-tuazyjnie Cumbajohnny - SC się zmienia, i to na lepsze”.

Max nie zwracał uwagi na politykę cardingowego światka. Ale ogłoszenie o VPN sprawiło, że poczuł się niepewnie. Okazało się, że od trzech miesięcy z usługi VPN Cumbajohnny’ego korzystali prywatnie przywódcy Shadowcrew.

Teraz, pisał admin, każdy członek forum cieszący się dobrą opinią może kupić spokój

ducha za 30-50 dolarów miesięcznie.

VPN-y miały jedną dobrze znaną słabość: wszystko, co płynęło przez sieć, musiało przejść przez jeden centralny punkt niezaszyfrowane, a więc łatwe do przechwycenia. „Jeśli FBI albo ktokolwiek inny naprawdę zechce, może wejść do centrum danych, zmienić niektóre ustawienia w VPN boksie i zalogować się, a wtedy bylibyśmy udupieni - zauważył jeden z członków. - Ale to tylko moja paranoja".

Cumbajohnny przywrócił jego zaufanie. „Nikt nie może tknąć VPN bez mojej wiedzy".

Max nie był przekonany. W czasach kiedy był białym kapeluszem, napisał

program dla Projektu Miodowej Sieci zwany Privmsg - skrypt PERL, który czerpał dane ze sniffera i używał ich do zrekonstruowania czatów IRC-a. Kiedy intruz został zwabiony do jednego z miodowych punktów projektu, często 128

używał tego systemu, aby podtrzymywać rozmowę online z innymi hakerami.

Używając Privmsg, białe kapelusze mogły to wszystko obserwować. To była ważna innowacja w tropieniu hakerów, zmieniająca bierne punkty miodowe w cyfrowe podsłuchy i otwierająca okno na podziemny świat i motywy działania jego mieszkańców.

Tę samą taktykę podsłuchową dostrzegał Max w VPN-ie Cumbajohnny'ego.

Był jeszcze inny dowód. Kiedy hakował przypadkowego cardera, dostrzegł list wysłany na konto admina; brzmiał on jak agent federalny dający rozkazy informatorowi. Max nie mógł pozbyć się wrażenia, że ktoś przekształcał Shadowcrew w największy miodowy punkt.

Kiedy pogadał o tym z Chrisem, wysłał na forum kilka postów, w których dał wyraz swym podejrzeniom. Te posty błyskawicznie zniknęły.

Domysły Maksa były słuszne.

Nowojorska policja złapała Alberta „Cumbajohnny'ego" Gonzaleza dziewięć miesięcy wcześniej, kiedy wybierał gotówkę z bankomatu w nowojorskiej Upper West Side. Pochodzący z Miami Gonazalez miał 21 lat, był synem pary kubańskich imigrantów. Był także hakerem z długim stażem, dostatecznie od-danym sprawie, by wybrać się do Vegas na DefCon w 2001 roku.

Secret Service przesłuchała Gonzaleza w areszcie i szybko oceniła jego wartość. Haker mieszkał w apartamencie z ogrodem w Kearny w New Jersey, za który płacił 700 dolarów miesięcznie. Miał 12 000 dolarów debetu na karcie kredytowej i był oficjalnie bezrobotny. Ale jako Cumbajohnny był zaufanym i kolegą carderów na całym świecie i - co najważniejsze - moderatorem na Shadowcrew.

Był w brzuchu bestii i jeśli zostałby właściwie pokierowany, mógł zadać temu forum śmiertelny cios.

Secret Service przejęła jego sprawę i skłoniła Gonzaleza, by został jej informatorem. VPN był mistrzowskim pociągnięciem agencji. Wyposażenie zostało zakupione i zapłacone przez federalnych, którzy dostali pozwolenie na 129

podsłuchiwanie wszystkich użytkowników. VPN Cumbajohnny'ego, który miał

służyć wyłącznie carderom, był w rzeczywistości zaproszeniem do internetowego panoptikonu.

Najwięksi gracze Shadowcrew zostali nieubłaganie wciągnięci w sieć monitoringu służb specjalnych. Przejęty VPN wyjawił wszystkie szczegóły, które carderzy starali się trzymać z dala od dostępnego dla wszystkich forum - twarde negocjacje prowadzone głównie drogą mailową i przez komunikatory internetowe.

Transakcje, zarówno drobne, jak i gigantyczne, miały miejsce każdego dnia i nocy, osiągając największy obrót w niedzielne popołudnia. 10 maja agenci obserwowali Scareface'a przesyłającego 115 695 numerów kart kredytowych innemu użytkownikowi; w lipcu APK sprzedał podrabiany brytyjski paszport, w sierpniu Mintfloss sprzedał fałszywe nowojorskie prawo jazdy, kartę ubezpieczenia zdrowotnego Empire Blue Cross i legitymację studencką City University of New York członkowi potrzebującemu całego portfolio dokumentów tożsamości. Kilka dni później miała miejsce kolejna sprzedaż Scarface'a, tym razem tylko dwóch kart, potem MALpadre kupił ich dziewięć. We wrze-

śniu Deck sprzedał 18 milionów zhakowanych kont mailowych z nazwiskami właścicieli, hasłami i datami urodzenia.

Secret Service miała 15 agentów przeczesujących forum, którzy pracowali w pełnym wymiarze godzin - każda transakcja stanie się kolejnym punktem w wyroku Sądu Najwyższego. A najlepsze w tym wszystkim było to, że wielu stałych bywalców Shadowcrew mimowolnie płaciło Secret Service za przywilej bycia monitorowanym.

Ale prowadzenie gry przeciwko hakerom nigdy nie było łatwe, o czym agencja przekonała się 28 lipca 2004. Wtedy właśnie Gonzalez poinformował

swoich mocodawców, że carder znany jako Myth, jeden z pośredników pracujących dla Kinga Arthura, jakimś sposobem zdobył jeden z tajnych dokumentów agencji dotyczący operacji „Firewall". Myth przechwalał się tym w czat roomie IRC-a.

Federalni kazali Gonzalezowi znaleźć źródło przecieku, i to szybko. Jako Cumbajohnny nawiązał on kontakt z Mythem i przekonał się, że dokumenty 130

zawierają zaledwie kilka odprysków z całego przecieku z Secret Service. Myth wiedział o kilku wezwaniach sądowych w sprawie Shadowcrew, zorientował

się też, że agencja monitoruje jego konto ICQ. Na szczęście w dokumencie nie było nic na temat informatora.

Myth nie chciał powiedzieć Gonzalezowi, od kogo to dostał, ale zgodził się umówić go z tą osobą. Następnego dnia Gonzalez, Myth i tajemniczy haker, używający tymczasowego nicka „Anonyman", spotkali się w IRC-u. Gonzalez robił wszystko, by zdobyć zaufanie Anonymana, i haker w końcu ujawnił się jako Ethics, sprzedawca, którego Cumba już znał z Shadowcrew.

Tajemnica przecieku zaczynała się wyjaśniać. W marcu siły specjalne zauważyły, że Ethics oferował dostęp do bazy danych dużego bezprzewodowego dostawcy, T-Mobile. „Oferuję odwrócone wyszukiwanie informacji na temat właściciela komórki T-Mobile przez numer telefonu. W najgorszym razie do-staniesz nazwisko, numer ubezpieczenia i datę urodzin. W informacji zwrotnej otrzymasz nazwisko użytkownika sieci/hasło, hasło

do poczty głosowej, sekretne pytanie/odpowiedź”.

T-Mobile nie załatał bardzo ważnej dziury w bezpieczeństwie w komercyj-nej aplikacji na serwerze, którą kupił z firmy BEA Systems z San Jose w Kalifornii. Dziura odnaleziona przez badaczy z zewnątrz była boleśnie łatwa do wykorzystania: nieudokumentowana funkcja pozwalała każdemu zdalnie czytać lub zmieniać dowolny plik w systemie, wysyłając mu specjalnie przygotowane zapytanie. BEA stworzyła łatę na tę dziurę w marcu 2003 roku i wydała ostrzeżenie, w którym oceniła to jako bardzo poważną słabość. W lipcu tego roku badacze, którzy odkryli dziurę, poświęcili jej więcej uwagi, prezentując ją na konwencji Black Hat Briefings w Las Vegas, corocznym spotkaniu poprze-dzającym DefCon, w którym uczestniczyło 1700 specjalistów od bezpieczeń-

stwa i członków kierownictwa korporacji.

Ethics dowiedział się o dziurze BEA z ostrzeżenia, stworzył własny dwu-dziestolinijkowy exploit w Visual Basic, potem zaczął skanować Internet w poszukiwaniu potencjalnych celów, które nie załatały dziury. Do października 131

2003 roku odniósł sukces w T-Mobile. Napisał własny front-end do bazy danych klientów, do której mógł powracać, kiedy tylko chciał.

Najpierw wykorzystał swój dostęp, aby wykraść pliki hollywoodzkich gwiazd, puszczając w obieg ukryte niewyraźne zdjęcia Paris Hilton, Demi Mo-ore, Ashtona Kutchera i Nicole Richie, skradzione z komunikatora PDA. Było teraz oczywiste, że dostał się także do komunikatora służb specjalnych.

Wystarczyło zgooglować numer ICQ Ethicsa, by znaleźć jego prawdziwe nazwisko na CV z 2001 roku, kiedy szukał pracy w branży bezpieczeństwa komputerowego. Nazywał się Nicholas Jacobsen, miał 22 lata i pochodził z Oregonu, a ostatnio przeniósł się do Irvine w Kalifornii, by podjąć pracę administratora sieci. Pozostało tylko sprawdzenie, który z agentów specjalnych zła-mał regulamin, udostępniając dane wrażliwe na swym komunikatorze PDA.

Tu znowu Gonzalez udowodnił swoją wartość. Teraz, kiedy Ethics kum-plował się z Cumbajohnnym, poprosił lidera Shadowcrew o założenie konta na własnym VPN-ie, sądząc, że będzie to łatwiejszy sposób na dostęp do T-Mobile.

Gonzalez spełnił prośbę, a jego mocodawcy z Secret Service zaczęli śledzić Ethicsa surfującego po stronach serwisu dla klientów T-Mobile i logującego się poprzez wpisanie nazwiska użytkownika i hasła nowojorskiego agenta Petera Cavicchia III, weterana walki z cyberprzestępczością, który wyróżnił się poj-maniem byłego pracownika AOL za kradzież 92 milionów adresów mailowych klientów, by sprzedać je spamerom.

Przeciek został znaleziony. Cavicchia po cichu przeszedł na emeryturę kilka miesięcy później, a Ethicsa wpisano na listę celów operacji „Firewall”.

Było jeszcze tylko jedno zagrożenie dla śledztwa, i co dziwne - jego źródłem był jeden z atutów FBI.

132

David Thomas był długoletnim oszustem, który odkrył forum przestępcze w czasach Counterfeit Library i wkrótce uzależnił się od szybkiego załatwiania interesów i

przestępczej przyjaźni. Mający teraz 44 lata El Mariachi, jak się podpisywał, był jednym z najbardziej poważanych członków społeczności carderów, pełniącym funkcję mentora dla młodych oszustów, z którymi dzielił się swym bogatym doświadczeniem profesjonalnym i życiowym, zdobytym w ciągu dekad życia na marginesie.

Doświadczenie nie uodporniło go jednak na ryzyko związane z jego profesją. W październiku 2002 roku Thomas pojawił się w kompleksie biurowym w Issaquah w stanie Waszyngton, gdzie wraz ze wspólnikiem wynajęli dziuplę dla jednego z założycieli CarderPlanet. Przyjechali odebrać wart 30 000 dolarów towar zamówiony przez Ukraińca z Outpost.com. Zamiast tego spotkali miejscowych policjantów, którzy na nich czekali.

Policja aresztowała Thomasa, detektyw odczytał mu jego prawa i dał formularz do podpisania, by potwierdził, że je rozumie. Thomas wyśmiał miejscowych policjantów, którzy chcieli go przesłuchać. „Nie wiecie, z kim macie do czynienia" - powiedział. Przynaglił detektywa, by zadzwonił do federalnych. W Secret Service będą wiedzieć, kim jest El Mariachi, a on może im pomóc w śledztwie dotyczącym sprawy, w którą są zaangażowani Rosjanie i

„miliony dolarów".

Agent Secret Service odwiedził go w więzieniu okręgowym, ale 30 000-dolarowy przekręt Thomasa nie zrobił na nim wrażenia. Potem pojawił się agent z terenowego biura FBI w Seattle. Na drugie spotkanie przyprowadził

zastępcę prokuratora krajowego, miał też dla Thomasa ofertę: federalni nie mogą mu pomóc w tej lokalnej sprawie, ale kiedy wyjdzie, będzie mógł pracować dla Northwest Cyber Crime Task Force (NCCTF, Północno-Zachodni Oddział Specjalny do spraw Cyberprzestępczości) w Seattle.

Będzie to misja zbierania informacji, oficjalnie określona jako operacja FBI bez ustalonych z góry celów. Biuro da Thomasowi nowy komputer oraz ładne mieszkanie, pokryje wszystkie koszty i będzie mu wypłacać 1000 dolarów 133

miesięcznie na drobne wydatki. On w zamian za to zbierze informacje na temat podziemia i przekaże je NCCTF.

Thomas nienawidził kapusiów, ale podobał mu się pomysł dostawania pieniędzy za obserwowanie i analizowanie podziemia, które było jego obsesją.

Zbieranie informacji to nie to samo co kablowanie, tłumaczył sobie, będzie też mógł wykorzystać zebrany materiał do napisania książki o światku carderów, o czym ostatnio dużo myślał.

Wiedział też doskonale, jak zbierać informacje, których szukała grupa do zadań specjalnych.

Thomas został wypuszczony z więzienia pięć miesięcy po aresztowaniu. W

kwietniu FBI zyskało nowy atut w walce przeciw cyberprzestępczości: El Mariachiego i jego nowe, wspaniałe, założone przez rząd forum - The Grifters.

Ze swego wynajętego przez biuro korporacyjnego mieszkania w Seattle El Mariachi wkrótce zbierał informacje o kolegach carderach, zwłaszcza tych z Europy Wschodniej.

Ale mimo że Thomas pracował dla FBI, nie czuł szczególnego pokrewieństwa z innymi rządowymi agencjami i ogłoszenie VPN

przekonało go - słusznie - że Cumbajohnny jest informatorem federalnych.

Ujawnienie rywala stało się dla Thomasa obsesją. Ignorując ostrzeżenia od mocodawców z FBI, nieustannie prowokował Gonzaleza na forum. Także Gonzalez wydawał się walczyć z El Mariachim - wygrzebał kopię policyjnego raportu dotyczącego aresztowania Thomasa w Seattle i udostępnił ją wschodnioeuropejskim carderom, zwracając ich uwagę na część, w której Thomas złożył ofertę pomocy w ujęciu Rosjan. Za sprawą dwóch informatorów między FBI a Secret Service wybuchła na całego wojna proxy.

Był to nieodpowiedni moment do rozpraszania facetów z Europy Wschodniej dramatem amerykańskich carderów. W maju 2004 roku jeden z ukraiń-

skich założycieli CarderPlanet trafił na mocy ekstradycji do USA, po tym jak został aresztowany na wakacjach w Tajlandii. W następnym miesiącu brytyjska policja wkroczyła do domu jedynego anglojęzycznego native speakera admini-strującego forum w Leeds.

Script, czując że za sprawą FBI z Orange County i US Postal Inspection Service robi się gorąco, już wycofał się z interesu, przekazując władzę Kingowi Arthurowi. 28 lipca 2004 roku King zamieścił oświadczenie.

„Nadszedł czas, aby przekazać złe wieści - forum powinno zostać zamknię-

te. Tak, to oznacza naprawdę zamknięte, i jest po temu wiele powodów”.

Łamaną angielszczyzną wyjaśnił, że CarderPlanet stała się celem dla policji z całego świata. Kiedy któryś z carderów wpadł, śledczy zadręczali go pyta-niami o forum i jego liderów. Pod bezlitosną presją - dawał do zrozumienia -

nawet on sam mógłby się ugiąć. „Każdy z nas jest tylko człowiekiem i może popełnić błąd”.

Zamykając CarderPlanet, pozbawił swych wrogów największego atutu.

„Nasze forum sprawiało, że byli dobrze poinformowani na bieżąco i mogli tu, podobnie jak pracownicy banków, po prostu podnosić poziom profesjonalnych kwalifikacji i wiedzy”.

„Teraz wszystko pozostanie bez zmian, ale oni nie będą wiedzieli, skąd wie-je wiatr i co robić”.

Tym pożegnalnym wpisem King Arthur, niemal z pewnością będący wówczas milionerem, przeszedł do legendy carderów. Zostanie zapamiętany jako ten, który delikatnie zwinął wspaniałą CarderPlanet, zanim ktokolwiek inny mógł się cieszyć jej zniszczeniem.

Liderzy Shadowcrew nie będą mieli tyle szczęścia. We wrześniu FBI zakoń-

czyło operację Thomasa i dało mu miesiąc na wyprowadzenie się z mieszkania

- kończąc w ten sposób jego wojnę z Cumbajohnnym. Miesiąc później, 26 paź-

dziernika, szesnastu agentów Secret Service spotkało się w waszyngtońskiej centrali, by przyspieszyć zakończenie operacji „Firewall”. Ich cele zostały zaznaczone na mapie USA, wypełniając całą ścianę komputerowych wydruków.

Agenci widzieli, że każdy z członków forum będzie w domu, ponieważ na polecenie Secret Service Gonzalez zwołał spotkanie online na ten wieczór, a nikt nie odmawiał Cumbajohnny’emu.

135

O dziewiątej wieczorem agenci uzbrojeni w półautomatyczne karabinki wpadli do domów członków Shadowcrew w całym kraju, zgarniając trzech założycieli, Ethicsa, który zhakował T-Mobile, i siedemnastu innych kupują-

cych i sprzedających. To była największy atak na złodziei tożsamości w historii Ameryki. Dwa dni później federalna ława przysięgłych wydała na podstawie paragrafu 62 oskarżenie o uczestnictwo w zorganizowanej grupie przestępczej, a Departament Sprawiedliwości upublicznił operację „Firewall”.

„Oskarżenie uderza w serce organizacji, którą podejrzewa się o bycie ryn-kiem zbytu dla złodziei tożsamości - przechwalał się w prasie prokurator generalny John Ashcroft. - Departament Sprawiedliwości jest oddany walce z tymi, którzy trudnią się kradzieżą tożsamości lub związanymi z nią oszustwami, niezależnie od tego, czy działają w Internecie czy poza nim”.

Z pomocą Gonzaleza Secret Service odcięła pozostałe 4000 użytkowników od forum, tworząc nową stronę startową, na której umieściła baner Secret Service i zdjęcie więziennej celi. Na nowej stronie dawne hasło: „Dla tych, którzy lubią grać w cieniu”, zostało zastąpione nowym mottem: „Nie jesteście już anonimowi!”.

Spanikowani carderzy na całym świecie chłonęli wiadomości i oglądali te-lewizyjne relacje, martwiąc się o siebie i o kumpli, którzy wpadli. Zebrali się na małym forum zwanym Stealth Division, aby oszacować straty i policzyć tych, którzy ocaleli.

„Umieram ze strachu. Co teraz będzie z moją rodziną - z moimi dziećmi? -

napisał jeden z cyberzłodziei. - Właśnie się dowiedziałem, że każdy mój ruch został zarejestrowany”.

Wkrótce zorientowali się, że Cumbajohnny’ego nie było na liście oskarżonych. Dokładnie wtedy gdy zalogował się, by złożyć ostatnie oświadczenie.

„Chcę, żeby wszyscy wiedzieli, że uciekam i nie miałem pieprzonego poję-

cia, że Secret Service była zdolna do zrobienia tego, co zrobiła - napisał Gonzalez. - Na podstawie tego, co mówi i pisze, przypuszczam, że monitorowała 136

mój VPN i serwer Shadowcrew. To mój ostatni post, powodzenia wszystkim”.

Nicka Jacobsena, Ethicsa, trzymano z dala od dziennikarzy. Został bez rozgłosu skazany w oddzielnym procesie w Los Angeles - jego włamanie do maila Secret Service nie wypłynęło przez długi czas, do chwili gdy agencja nie zebra-

ła pochwał za operację „Firewall”. Nawet gdy sprawa wyszła na jaw, obława została uznana przez władze za wielki sukces. CarderPlanet była w rozsypce, a teraz forum

Shadowcrew zostało zamknięte na zawsze, jego zaś przywódcy - z wyjątkiem Gonzaleza - siedzieli w więzieniu.

Carderzy byli zdezorientowani, podejrzliwi i przez chwilę bezdomni. „Zbu-dowanie czegoś takiego jak Shadowcrew zabierze całe lata - napisał jeden z nich. - I kiedy (lub jeśli) ono powstanie, policja znowu je zniszczy.

I wątpię, że wiedząc, jak to się skończy, ktokolwiek podejmie ryzyko stworzenia nowego forum”.

ROZDZIAŁ 17

Pizza i plastik

Na najwyższym piętrze Post Street Towers komputery Maksa spoczywały w ciszy na fornirowej podłodze. Sklepy i mieszkania za wykuszowym oknem były gotowe mimowolnie udzielić mu dostępu do sieci przez wielką antenę.

Po zgromadzeniu sterty gotówki z Citibanku Max na kilka miesięcy zawiesił działalność. Opuścił swój penthouse, a hakowanie zeszło na drugi plan. Nie potrafił jednak zbyt długo bez tego wytrzymać. Poprosił Chrisa, by znalazł dla niego nowe bezpieczne miejsce, w którym będzie miał więcej możliwości skorzystania z WiFi niż w wypadku ostatniego mieszkania. „Wystarczy mi szafa, nie potrzebuję przestrzeni” - powiedział wspólnikowi.

Chris spełnił jego życzenie. Wokół Post Street Towers było gęsto od WiFi, a mieszkanie rzeczywiście przypominało szafę. Kawalerka o powierzchni 28

metrów kwadratowych wyglądała na niewiele większą od więziennej celi. Wy-

łożona jasnym drewnem, ze stołem Formila, dużą lodówką i składanym łóż-

kiem, była czystym i funkcjonalnym McMieszkaniem, w którym nic Maksa nie rozpraszało, a jednocześnie mógł znaleźć tam wszystko, czego potrzebował w 138

czasie swych całonocnych hakerskich sesji. Dzięki dużej rotacji lokatorów mógł pozostawać anonimowy. Wystarczyło, że Chris pokazał swoje dokumenty, oczywiście fałszywe, w biurze nieruchomości, zapłacił 500 dolarów kaucji i podpisał umowę na sześć miesięcy.

Max podłączył komputery, a antena złapała sieć jakiegoś frajera, ale powrót do pracy zajął Maksowi jeszcze trochę czasu. Jak zwykle obrał za cel oszustów, wpadł jednak na nowy sposób ich okradania. Śledził ostrzeżenia wysyła-ne przez organizację znaną jako Anti-Phishing Working Group [Antyphishin-gowa Grupa Robocza], która była na bieżąco z ostatnimi atakami phishingowym. Ostrzeżenia te zawierały adresy internetowe stron phishingowych, po-wiązanych z fałszywymi mailami, co pozwalało Maksowi hakować serwery oszustów i ukraść im nielegalnie zdobyte dane, kasując je przy okazji. W ten sposób jednocześnie wkurzał phisherów i gromadził cenne informacje.

Inne ataki nie były tak wyraźnie ukierunkowane. Max ciągle funkcjonował

w świecie białych kapeluszy, będąc na prywatnej liście mailingowej, na której informacje o nowych dziurach w systemie bezpieczeństwa pojawiały się często po raz pierwszy. Jego komputery skanowały Internet przez całą dobę, szukając serwerów, na których działało oprogramowanie niezabezpieczone przed atakami, tylko po to by zobaczyć, co się pojawi. Max obrał sobie za cel ataki buffer overflow na serwery działające na Windowsie, dokonując odkrycia, za sprawą którego miał otwarcie pojawić się w świecie carderów.

Skanowanie doprowadziło go do wnętrza komputera z Windowsem, który jak się okazało - mieścił się w biurze na zapleczu restauracji Pizza Schmizza w Vancouver w stanie Waszyngton. Max znał to miejsce, lokal znajdował się niedaleko domu jego matki. Kiedy rozejrzał się po komputerze, zorientował

się, że służył on jako ostatnie ogniwo systemu terminali płatniczych w restauracji - gromadził przeprowadzone w ciągu dnia transakcje kartami kredytowymi i co wieczór wysyłał je w jednej partii do procesora kart kredytowych. Max stwierdził, że te dane przechowywane są jako zwykły plik tekstowy z pełnym zapisem paska magnetycznego karty każdego z klientów.

139

Co lepsze, system ciągle przechowywał wszystkie poprzednie pliki sięgają-

ce czasów, kiedy w pizzerii zainstalowano system, czyli około trzech lat temu.

Było to jakieś 50 000 transakcji, po prostu spoczywających sobie tam i czekających na niego.

Max skopiował pliki, po czym skasował je - Pizza Schmizza ich nie potrzebowała - przechowywanie ich było przede wszystkim naruszeniem standardów bezpieczeństwa Visy. Po uporządkowaniu i odrzuceniu powtarzających się danych i nieaktualnych kart zostało mu około 2000 zrzutów.

Po raz pierwszy miał dane z pierwszej ręki i były to dziewicze karty, niemal na sto procent zdatne do użytku.

Chris skarżył się na nieaktualność części zrzutów Maksa. Teraz to się skoń-

czy. Klient mógł pójść do Pizzy Schmizzy i zamówić trzydziestocentymetrowy placek dla rodziny, a jego karta kredytowa trafiała na dysk Maksa, kiedy reszt-ki jedzenia jeszcze stygły w śmietniku. Kiedy już uporządkował swe numery, rzucił coś Chrisowi na zanętę. „To superświeży towar - powiedział - sprzed dwóch dni".

Nie było szans, by Chris i jego ekipa przerobili 50 zrzutów z Pizzy Schmizzy dziennie. Max postanowił więc zrobić swój pierwszy krok jako sprzedawca w świecie cardingu.

Chris zaoferował, że zajmie się sprzedażą w zamian za połowę zysków. Je-go lekkomyślność ciągle martwiła Maksa - Chris o mały włos nie został aresztowany, kupując złoto, między innymi w Indiach, skąd ledwie zdążył uciec przed policją. Ale wspólnik zbyt wiele wiedział o Maksie, by ten mógł go tak po prostu porzucić, pozwolił zatem występować Chrisowi w roli swego przedstawiciela w podziemiu. Wspólnik wkrótce ogłosił sukces w sprzedaży zrzutów Maksa, ale Max - mając dostęp do jego komputera - zorientował się, że Chris tak naprawdę sam używa kart, biorąc 50 procent ceny i twierdząc, że je sprzedał. Z finansowego punktu widzenia nie było różnicy, ale Max nie mógł znieść tego, że znowu ktoś go oszukuje.

140

Znalazł kogoś, kogo łatwiej było kontrolować - nastoletniego cardera z Long Island Johna Giannonego, który stał się pomocnikiem Chrisa.

Giannone był bystrym dzieciakiem z klasy średniej lubiącym kokainę i ży-wiącym gorące pragnienie bycia bezwzględnym złym cyberpunkiem. Jego wczesne osiągnięcia nie były zbyt imponujące: przechwalał się innemu carderowi, że kiedyś przed wyjściem z windy wcisnął wszystkie guziki, więc na-stępny pasażer musiał się zatrzymywać na każdym piętrze. Innym razem, jak twierdził, wszedł do banku i napisał na odwrocie formularza

wpłaty: „To jest napad. Mam bombę. Dajcie mi pieniądze albo wysadzę bank”. Potem położył

papier na kupce, jako niespodziankę dla następnego klienta.

W wieku 17 lat Giannone dołączył do Shadowcrew i CarderPlanet pod nickiem MarkRich i zaczął robić drobne przekręty. Stracił reputację, gdy został

złapany, płacąc kartą za bilet lotniczy, i rozeszły się plotki, że regularnie kablował na członków forum, kiedy był w poprawczaku.

Niezrażony zapłacił bardziej ustawionemu carderowi za wyłączne prawo do przejęcia jego nicka i reputacji. Jako „Enhance” był bardziej śmiały, ale nie przysporzyło mu to sukcesów. W maju 2003 roku, stosując metodę wymusza-nia doprowadzoną do perfekcji przez Rosjan, wypożyczył od innego hakera botnet i dokonał ataku DDoS na JetBlue, zdejmując jej stronę na jakieś 25 minut, a potem wysyłając maila z żądaniem 500 000 dolarów haraczu. Ale JetBlue nie okazały szacunku, na jaki zasługiwał cybergangster, i odrzuciły żądania finansowe. „Prześlemy to odpowiednim służbom - napisała firma w odpowiedzi. - Wczorajsza awaria była spowodowana uaktualnianiem systemu”.

Kiedy Max trafił na Giannonego dzięki swej akcji „Darmowy Amex”, nastolatek hakował, korzystając z komputera w sypialni swej matki. Max i Chris przejrzeli jego pliki i stwierdzili, że mimo wszystko można z niego zrobić wspólnika. Szczególnie Chris mógł dostrzec we wciągającym kokainę nasto-latku, który bardzo chciał być gangsterem, podobieństwo do siebie z lat młodo-

ści. Giannone regularnie odwiedzał Orange County - lubił spędzać wakacje w 141

tym słonecznym miejscu - i zaczął chodzić z Chrisem na imprezy. Chris nazywał swego ucznia „The Kid” (Dzieciak).

Max wiedział o nim wszystko, podczas gdy Giannone nie wiedział o hakerze zupełnie nic. Dla Maksa była to idealna sytuacja do współpracy. John sprzedał trochę zrzutów Maksa i zapoznał go z innymi carderami, którzy byli zainteresowani kupnem przez ICQ. Max przybrał nową tożsamość jako sprzedawca: „Generous” (Szczodry).

Robienie interesów z obcymi było dla Maksa wielką nowością, dlatego też przedsięwziął nadzwyczajne środki bezpieczeństwa. Kiedy korzystał z forów carderów lub komunikatorów internetowych, łączył się przez swą prywatną sieć zhakowanych pecetów z całego świata - by mieć pewność, że nikt nie był

w stanie łatwo wyśledzić nawet znakowania wifi. Pisząc online, starał się zmieniać styl, w obawie że jakieś nierozważnie osobliwe sformułowanie lub interpunkcja mogłyby zostać zestawione z artykułami Maksa Visiona na temat bezpieczeństwa lub postami na Bugtraqu - FBI zwróciło uwagę na liczne wie-lokropki w jego anonimowej nocie do Lawrence Berkeley Laboratory, kiedy przeprowadzał ataki na BIND.

Aby odebrać zapłatę, przyjmował pieniądze przez anonimowe konto e-gold, z którego mógł pobierać gotówkę, korzystając z bankomatu. Giannone pomógł

mu z zorganizować drugi element tego systemu przelewów. Nastolatek założył

konto firmowe w Bank of America na warsztat mechaniki samochodowej A&W Auto

Clinic, a następnie wysłał Maksowi dane z paska magnetycznego i PIN do jego karty bankomatowej, pozwalając mu na skopiowanie karty za pomocą MSR206. Kupcy zrzutów w Stanach wpłacali gotówkę na konto A&W w najbliższym oddziale Bank of America, a Max mógł ją w wolnej chwili wypła-cić, używając swej karty.

Max nie potrzebował już pieniędzy tak jak dawniej. Większość swych oszczędności pochodzących z wyciągania pieniędzy z Citibanku roztrwonił na rozmaite rzeczy, począwszy od ulotek dla bezdomnych po psa-robota Sony AIBO za 1500 dolarów. Ale jeszcze nie był spłukany, a Charity zaczęła 142

właśnie dobrze płatną pracę jako administrator systemu w Linden Lab - realnej firmie, która stworzyła kompletny trójwymiarowy wirtualny świat Second Life, powiększający się co miesiąc o tysiące mieszkańców.

Był tylko jeden powód, dla którego nastawiał teraz swoją antenę. Uzależnił

się od bycia zawodowym hakerem. Lubił te zabawy w kotka i myszkę, wolność, ukrytą władzę. Zamknięty w anonimowości swego bezpiecznego mieszkania, mógł podążać za każdym impulsem, odkrywać każdy zakazany korytarz Internetu, zaspokoić każde przelotne zainteresowanie - wszystko bez obaw o konsekwencje, ograniczany tylko przez własne sumienie. W głębi duszy mistrzowski przestępca ciągle pozostawał dzieckiem, które nie mogło się powstrzymać przed wślizgnięciem się w środku nocy do szkoły i zostawieniem swego znaku.

ROZDZIAŁ 18

Odprawa

W pokoju odpraw w pobliżu Waszyngtonu ponad 20 męskich twarzy wypełnia-

ło ekran komputera na ścianie. Część z nich krzywiła się na zdjęciach z poli-cyjnych kartotek, inne uśmiechały się ze zdjęć paszportowych. Kilka z nich zdawało się należeć do nastolatków, którzy ledwie wyszli z okresu dojrzewa-nia, inne były starsze, niechlujne, w jakiś sposób budzące niepokój.

Wokół stołu zgromadzili się agenci FBI w garniturach i pod krawatem, przyglądając się twarzom przestępców komputerowych z międzynarodowego półświatka. Jednemu z policjantów wszystko nagle zaczęło się układać w sen-sowną całość.

Trzydziestopięcioletni J. Keith Mularski był agentem FBI od siedmiu lat. W

wydziale przestępczości komputerowej znalazł się jednak dopiero dwa miesią-

ce temu i jeszcze wiele musiał się nauczyć. Niezwykle przyjacielski i skory do śmiechu, chciał być agentem już od pierwszego roku studiów w Westminster College w Pensylwanii, kiedy na jedne z zajęć przyszedł człowiek z FBI rekrutujący nowych agentów. Mularski robił wszystko, by spełniać wymogi listy kwalifikacyjnej, nawet kiedy jego kariera nie odbiegała od przeciętnej. Zaczynał

jako sprzedawca mebli w Pittsburghu, a potem dorobił się w krajowej sieci meblowej stanowiska menedżera, któremu podlegały cztery sklepy z pięćdziesięcioma pracownikami.

W 1997 roku, po ośmiu latach czekania, stwierdził ostatecznie, że jest gotowy zacząć pracę w FBI. Po trwającym rok procesie aplikacyjnym i szesnastu tygodniach treningu w akademii FBI w Quantico został zaprzysiężony jako agent w lipcu 1998 roku.

Świeżo upieczony agent został poinstruowany, zgodnie ze zwyczajem zwią-

zanym z ukończeniem akademii, by ułożył listę wszystkich terenowych oddzia-

łów FBI według miejsc, do których najbardziej chciałby trafić. Na pierwszej pozycji umieścił rodzinny Pittsburgh - tam dorastał, chodził do szkoły, poznał

swoją żonę. Szanse na dostanie się tam zniknęły w następnym miesiącu, kiedy islamscy terroryści podłożyli bomby w budynkach amerykańskich ambasad w Kenii i Tanzanii. Starzy agenci FBI zostało oddelegowani z terenowego oddziału w Waszyngtonie, by zająć się śledztwem w tych sprawach, a Mularskiego jako jednego z piętnastu nowych rekrutów wysłano na ich miejsce - trafił

więc do miasta, które na jego liście zajmowało 32. pozycję.

Niemal z dnia na dzień Mularski przeszedł z kierowania sklepami meblar-skimi do pracy w najważniejszych śledztwach objętych klauzulą najwyższej tajności. Kiedy w 1999 roku znaleziono urządzenie podsłuchowe w biurze na ostatnim piętrze centrali Departamentu Stanu, wszedł w skład ekipy, która zidentyfikowała rosyjskiego dyplomatę

monitorującego przekaźnik z zewnątrz.

W 2001 Mularski pomógł schwytać Roberta Hanssena, kolegę po fachu z kontrwywiadu, który przez dwadzieścia lat szpiegował na rzecz KGB i jego następczyni.

To była ekscytująca praca, ale jej sekretny charakter drażnił Mularskiego: miał dostęp do materiałów objętych klauzulą najwyższej tajności i nie mógł

rozmawiać o swej pracy z ludźmi spoza biura, nawet z żoną. Kiedy FBI zgłosi-

ło zapotrzebowanie na dwóch doświadczonych agentów, którzy mieli stworzyć w Pittsburghu ambitną inicjatywę przeciw cyberprzestępczości, dostrzegł w tym szansę na powrót do domu i jednocześnie wyjście z cienia.

145

Jego nowym miejscem pracy nie była siedziba FBI. Został oddelegowany do cywilnego biura przemysłowej grupy non profit w Pittsburghu, znanego jako National Cyber Forensics and Training Alliance. NCFTA została utwo-rzona przez banki i firmy internetowe kilka lat wcześniej i zajmowała się analizą najnowszych oszustw przeciw klientom online, głównie ataków phishingowych. Zadanie Mularskiego nie polegało na śledzeniu pojedynczych oszustów z osobna; każda runda phishingu była zbyt drobnym przestępstwem, by prze-kroczyć próg wysokości szkody wynoszący dla FBI 100 000 dolarów. Agent miał śledzić trendy, które wskazywały na działanie grubej ryby - grupy lub pojedynczego hakera - odpowiedzialnej za dużą liczbę internetowych kradzie-

ży, i przekazywać wyniki do różnych terenowych oddziałów FBI w nadziei, że rozpoczną dochodzenie.

Było to bierne gromadzenie informacji, drobiazgowe i niezbyt ekscytujące.

Mularski nie był odpowiedzialny za prowadzenie dochodzeń i nigdy nie mógł

mieć satysfakcji z zapinania kajdanek na rękach złoczyńcy. Ale po raz pierwszy od siedmiu lat mógł porozmawiać o swej pracy z żoną przy obiedzie.

Teraz był z powrotem w okolicach Waszyngtonu na swojej pierwszej od-prawie związanej ze światkiem cardingu. Z przodu pokoju stał funkcjonariusz US Postal Inspection Service Greg Crabb, dobrze zbudowany mężczyzna o zmęczonych oczach, który pracował w międzynarodowym oddziale do spraw oszustw. Crabb natknął się na półświatek carderów w 2002, kiedy śledził fał-

szerza oprogramowania, który zajmował się również oszustwami na kartach kredytowych. Od tej pory odwiedził 25 krajów, pracując z lokalną policją, by łapać przestępców i budować obszerną bazę danych z surowymi informacjami na temat powiększającej się społeczności: niekarni, adresami IP, mailowymi i komunikatorów internetowych ponad 2000 ludzi. Stał się najlepszym rządowym ekspertem od cyberprzestępczego półświatka, ale ogrom jego krucjaty zaczynał go przerastać. Zgłosił się więc po pomoc do FBI.

Odprawa dla sześciu agentów miała miejsce w niczym niewyróżniającym się biurze w Calverton w stanie Baltimore, gdzie federalni przeprowadzali 146

akcję pod kryptonimem „Niewinne Obrazki” przeciw dziecięcej pornografii.

Mówiąc powoli z burczącym nosowym środkowowschodnim akcentem, inspektor ważył

każde słowo niczym paczkę, przebiegając przez historię pół-

światka: mówił o CardersLibrary, która dała początek CarderPlanet, legendzie Kinga Arthura, wpływie Rosjan i Ukraińców, narodzinach i upadku Shadowcrew. Wyświetlił zrzut ekranu strony CarderPlanet, aby pokazać strukturę pół-

światka. Zarządcą strony był don, admini byli odpowiednikami capo. Do tej metafory FBI było instytucjonalnie dostrojone: hakerzy byli nową mafią.

Operacja „Firewall", wyjaśniał Crabb, rozbiła hakerów, sprawiając, że stali się podejrzliwi i zdezorganizowani. Zaczęli jednak odbudowywać półświatek.

Inaczej niż w wypadku Shadowcrew, teraz nie było jednego określonego celu, który można by śledzić. Zamiast tego pojawiło się mnóstwo nowych mniejszych forów. Crabb tego nie powiedział, ale Secret Service zastosowała wobec carderów połowę dawki penicyliny - ci, którzy przetrwali, byli odporni i rośli w siłę.

Mularski wsłuchiwał się w każde słowo. Podczas swej krótkiej pracy w NCFTA luźne informacje płynące z półświatka zaczęły mu się układać w pewną całość: odniesienia do nicków, zaszyfrowane wiadomości i fora. Teraz na-bierało to sensu. Carderzy reorganizowali się.

Kiedy Crabb zakończył swą prezentację i inni agenci zaczęli się zwijać, Mularski podszedł do niego i z entuzjazmem wyciągnął dłoń: „To było fascynujące. Marzę o tym, by z panem pracować i zostać pańskim partnerem".

Crabb był zaskoczony propozycją: jego doświadczenie podpowiadało, że typowa reakcja agenta FBI wyglądałaby raczej tak: „Proszę podać wszystkie informacje, które pan posiada. Do widzenia". Crabb spotkał się prywatnie z Mularskim i swym szefem, przedstawiając agentowi bardziej szczegółowy obraz półświatka carderów.

Mularski wrócił do Pittsburgha z zamętem w głowie. Sądził, że zostawił za sobą świat rosyjskich szpiegów, podwójnych agentów i ukrytych tożsamości.

Mylił się. Dająca satysfakcję i poczucie bezpieczeństwa rutyna jego nowej pracy miała zostać gwałtownie przerwana.

ROZDZIAŁ 19

Carders Market

Chociaż Max bardzo się starał, nie udało mu się zagnieździć na żadnym z nowych forów powstałych na ruinach Shadowcrew. Wszystkie były zdeprawo-wane, prowadzone przez sprzedawców zrzutów wrogich konkurencji z ze-wnątrz. W pewien sposób wyszło mu to na dobre. Naprawdę nigdy nie mógł

mieć zaufania do żadnego z tych forów, zbyt dobrze wiedział, że cały półświatek był naszpikowany policjantami i konfidentami.

Ostatecznie zdecydował, że jeśli zajmie się sprzedażą, jedynym rozsądnym miejscem będzie strona pozostająca pod jego osobistą kontrolą. Ciągle uważa-jąc się za Robin Hooda, wymyślił idealną nazwę dla swego forum: „Sherwood Forest" (Las Sherwood).

Chris zaaprobował plan - spodobał mu się pomysł sprzedawania własnych podrabianych kart i praw jazdy w bezpiecznym miejscu - ale zdecydowanie odrzucił nazwę. „Sherwood Forest" nie przyjąłby się na przestępczym rynku.

Wspólnicy powrócili do pracy nad projektem i w czerwcu 2005 roku Max użył

fałszywego nazwiska i adresu w Anaheim, aby zarejestrować Cardersmarket.com.

148

Dla Maksa był to ważny moment - zbliżał się termin zakończenia jego warunkowego zwolnienia i jeśli dotrwałby do północy 10 października 2005, stał-

by się wolnym człowiekiem i nie musiałby już dłużej odgrywać przed swym kuratorem sądowym roli mającego problemy ze znalezieniem pracy konsultan-ta komputerowego. Przetrwanie jeszcze tych kilku miesięcy nie powinno być takie trudne. Poza Chrisem tylko dwóch hakerów wiedziało o podwójnym życiu Maksa, obaj byli zresztą kumplami Chrisa: Jeff Norminton i Werner Janer, oszust działający w nieruchomościach, który wypisał Charity czek na 5000

dolarów, co pomogło Maksowi wznowić hakerską działalność.

Wtedy, we wrześniu 2005 roku, Werner Janer został aresztowany.

Od czasu kiedy Chris spiknął się z Maksem, przy różnych okazjach podrzu-cał Janerowi karty - jakieś osiemdziesiąt w ciągu trzech lat - w zamian za 10

procent zysków, które Janer wyciągał ze swych zakupów. Tego miesiąca Janer poprosił o następny zestaw 24 kart - brak pieniędzy zmusił go do sprzedaży rodzinnego domu w Los Angeles i przeprowadzki do Wesport w Connecticut, by zacząć od nowa. Tuż po swoim przyjeździe został okradziony przez wspólnika niemal ze wszystkich pieniędzy, które uzyskał ze sprzedaży domu, i potrzebował zastrzyku gotówki, by utrzymać siebie i żonę z trójką dzieci.

Kiedy pojawiła się przesyłka od Chrisa, Janer, zapalony kolekcjoner zegarków, ruszył prosto do Richards of Greenwich, sklepu z męską garderobą i ak-cesoriami, w którym był duży asortyment wysokiej klasy zegarków. Janer miał

w kieszeni dobrze podrobione karty i pasujące do nich prawo jazdy na nazwisko Stephen Leahy. Tym, czego mu brakowało, była smykałka do cardingu.

Wybrał nie jeden czy dwa, ale aż cztery zegarki Anonimo, z których każdy kosztował od 1000 do 3000 dolarów, i chciał za każdy z nich zapłacić inną kartą Visa, ostentacyjnie wyciągając karty z pliku dwunastu innych. Dwie z dużych transakcji zostały odrzucone, więc Janerowi zostały dwa zegarki warte razem 5777 dolarów, za które zapłacił dwiema kartami Bank of America.

Samochód patrolowy wyprzedził Janera jakieś trzy kilometry dalej. Kiedy policjanci oglądali jego prawdziwe prawo jazdy, jeden z nich zapytał, czy 149

kupował niedawno zegarki, a drugi samochód podjechał z właścicielem sklepu w środku. Facet spojrzał na Janera i potwierdził, że gliniarze złapali właściwego człowieka.

Aresztowali go, przeszukali samochód, zabierając zegarki, 28 kart kredytowych i sześć kalifornijskich praw jazdy. Po rewizji przeprowadzonej w jego domu znaleźli jeszcze więcej zegarków i pistolet Walther P22.

Broń była poważną wpadką. Zamiast oskarżenia o drobną kradzież i naruszenie warunków zwolnienia Janer miał do czynienia z federalnym oskarżeniem o bycie przestępcą nielegalnie posiadającym broń palną. W tej sytuacji, nie zwlekając, zaoferował policji współpracę w doprowadzeniu do źródła podrabianych kart. W standardowej umowie konfidenta zezwolono Janerowi na przekazanie informacji, które posiadał, w zamian za ograniczone gwarancje nietykalności: nic, co powie, nie zostanie wykorzystane bezpośrednio przeciwko niemu. Jeśli okaże się, że informacje są użyteczne, to znaczy doprowadzą do aresztowania - władze rozważą zarekomendowanie zmniejszenia wyroku w sprawie za posiadanie broni.

W trakcie dwóch sesji składania zeznań trwających łącznie około ośmiu godzin Janer wywnętrzał się przed miejscowym agentem Secret Service i prokuratorem federalnym. Powiedział im o Chrisie Aragonie, jego dziewczynach i hakerze Maksie, blisko dwumetrowym komputerowym geniuszu, który włamywał się do sieci bankowych z hotelowych pokoi w San Francisco.

Nie znał jego nazwiska, ale raz wypisał czek na 5000 dolarów dla jego dziewczyny Charity Majors.

Secret Service spisała zeznania i wprowadziła dane do komputera, ale agencja nigdy nie wykorzystała informacji w śledztwie, a prokurator odmówił Janerowi szczególnych względów. Został skazany na 27 miesięcy więzienia.

Max Vision uniknął kary. Zeznania Janera utonęły w gigantycznym komputerze rządowej agencji - równie dobrze mogły zostać ukryte w niezmierzonych magazynach z ostatniej sceny *Poszukiwaczy zaginionej Arki.* Dopóki nikomu 150

nie trafi się okazja, by się do nich dokopać, Max będzie bezpieczny.

Tymczasem Max rozpoczął prace nad uruchomieniem Carders Market. Miał

duże doświadczenie w tworzeniu nielegalnych stron internetowych, ale witryna służąca działalności przestępczej wymagała specjalnych przygotowań. Z jednego powodu - nie mógł po prostu postawić serwera Carders Market na podłodze swojej kryjówki - to byłoby

wystawieniem się na strzał.

Zhakował centrum informacji na Florydzie prowadzone przez Affinity Internet i zainstalował wirtualną maszynę VMware na jednym z jego serwerów -

ukrywając cały symulowany komputer na jednym z jego systemów. Jego ukryty serwer przywłaszczył sobie nieużywany adres internetowy z zasobów adre-sowych Affinity. Strona, oficjalnie do nikogo nienależąca i przez nikogo nie-prowadzona, będzie niczym statek widmo.

Max próbował różnego rodzaju programowania do internetowych forów i w końcu wybrał elastyczną paczkę vBulletin. Siedział miesiącami nad dostoso-waniem layoutu i zaprojektowaniem własnych szablonów, nadając stronie sza-ro-złotą kolorystykę. Praca przynosiła mu satysfakcję. Po raz pierwszy od lat coś tworzył, zamiast kraść. To było jak budowanie Whitehats.com, oczywiście, z wyjątkiem tych aspektów, w których nowy projekt był jego przeciwień-

stwem.

Ostatecznie w pierwszą rocznicę operacji „Firewall" stworzył nowe imię w swym ciągle zmieniającym się zestawie *noms de guerre:* Iceman. Wybrał je po części ze względu na jego powszechność: w półświatku było wielu Icemanów, jeden pojawił się nawet na Shadowcrew. Jeśli policja będzie próbowała go wytropić, znajdzie na swym radarze kilka miraży.

Max jako Iceman bez wielkiej pompy wystartował z Cardersmarket.com pod koniec 2005 roku. Chris został pierwszym współadministratorem, wystę-

pując pod nickiem EasyLivin'.

Ze swojej dokładnej obserwacji Shadowcrew i jego klonów, które pojawiły się później, Max i Chris wiedzieli, że kluczem do sukcesu było powierzenie ważnych funkcji grubym rybom, które mogłyby pomóc w prowadzeniu strony i przyciągać poważnych graczy z kręgu swych przyjaciół. Wspólnicy wkrótce zdołali pozyskać dwa liczące się nazwiska spośród ludzi związanych kiedyś z Shadowcrew.

Bradley Anderson, czterdziestojednoletni kawaler z Cincinnati, był ich pierwszym nabytkiem. Anderson był legendarnym „ncXVI", ekspertem od fałszywych dokumentów tożsamości i autorem wydanej własnym sumptem książki *Shedding Skin,* biblii tworzenia nowej tożsamości. Kolejnym zwerbo-wanym był Brett Shannon Johnson, trzydziestopięcioletni złodziej tożsamości z Charleston w Południowej Karolinie. W Internecie zdobył on sławę jako „Gollumfun", założyciel Counterfeit Library i Shadowcrew, który wycofał się z tego ostatniego forum, zanim zostało ono opanowane przez Secret Service.

Po zniknięciu z półświatka na rok Johnson powoli wychodził z cienia. Pomagier Chrisa John Giannone zauważył go w sieci na wiosnę i nawiązał z nim rozmowę przez ICQ, przekazując mu najnowsze informacje o aresztowaniach i plotki.

Giannone w końcu sprzedał Johnsonowi 29 zrzutów Maksa za jakieś sześć stów, a potem przedstawił go Maksowi, który sprzedał mu kolejne pięćset kart.

„Widzę, że razem będziemy robić dobre interesy w przyszłości” - powiedział

Johnson.

Johnson przyjął zaproszenie Maksa i Chrisa i został adminem na Carders Market, wykorzystując na forum swoje doświadczenie i kontakty jedynego administratora Shadowcrew, który nie poległ w operacji „Firewall”.

Giannone dołączył do Carders Market jako „Zebra”, a Max stworzył dla siebie kolejną tajną tożsamość: „Digits”. Alternatywne nicki były podstawą w nowej strategii biznesowej Maksa. Shadowcrew upadła, ponieważ prokuratorzy dowiedli, że sami założyciele kupowali i sprzedawali skradzione dane oraz wykorzystywali je. Prowadzenie strony zawierającej informacje samo w sobie nie było nielegalne, rozumował Max. Iceman będzie więc oficjalną twarzą 152

Carders Market, ale nigdy nie będzie kupował ani sprzedawał skradzionych danych. Digits, jego *alter ego,* zajmie się tym, upłynniając zrzuty. Max udostępniał zasoby pizzerii w Vancouver każdemu, kogo było na to stać.

Aby w pełni zrealizować swą koncepcję strony, Max potrzebował jeszcze jednego admina z bardzo szczególną umiejętnością: znajomością języka rosyjskiego. Chciał zbudować most nad przepaścią między carderami ze Wschodu i Zachodu, jaka powstała na skutek operacji „Firewall”. Dwu rosyjskich człon-ków Shadowcrew wpadło w zastawioną przez Cumbajohnnyego pułapkę VPN

i cała afera sprawiła, że od tamtej pory Rosjanie traktowali anglojęzyczne fora z głęboką nieufnością.

Max postanowił, że Carders Market wyróżni się, posiadając wschodnioeuropejską sekcję, moderowaną przez rosyjskiego native speakera. Musiał go tylko znaleźć.

Chris zaoferował pomoc i Max ją przyjął. Jeśli Chris miał jakąś umiejęt-ność, której posiadania dowiódł swemu wspólnikowi, był nią talent do wyszukiwania nowych pracowników.

ROZDZIAŁ 20

Starlight Room

Dziewięć żyrandoli wisiało nad aksamitnymi kabinami w Harry Denton’s Starlight Room, a nad parkietem błyszczał gigantyczny stroboskop. Ciężkie karma-zynowe draperie odsłaniały obszerne okna niczym scenę, ukazując powyżej rozgwieżdżone niebo nad San Francisco.

Starlight Room, mieszczący się na dwudziestym pierwszym piętrze Sir Francis Drake Hotel, był luksusowym dodatkiem do bogatego nocnego życia miasta. Wnętrza lokalu wyłożone głęboką czerwienią, złotym adamaszkiem i ręcznie robionym jedwabiem nawiązywały do stylu lat trzydziestych. Bardziej krzykliwy niż modny klub przyciągał klientów, organizując regularnie imprezy tematyczne. Tego wieczoru była rosyjska środa i wyfraczeni kelnerzy nalewali wódkę do kieliszków przy zatłoczonym barze, podczas gdy po sali rozchodziła się muzyka z ojczyzny.

W damskiej toalecie Tsengeltsetseg Tsetsendelger właśnie została pocałowana. Młoda mongolska imigrantka, już nie całkiem trzeźwa, nie wiedziała, jak to się stało, ale piękna wysoka dziewczyna o brązowych pofalowanych włosach postanowiła cmoknąć ją w policzek. Po chwili Tsengeltsetseg zrobiła wielkie oczy. Przed nią stała druga, identyczna dziewczyna.

Michelle i Liz przedstawiły się i szeroki, szczery uśmiech pojawił się na twarzy Tsengeltsetseg. Powiedziała bliźniaczkom Esquere, że mogą ją nazywać

„Tea”.

Tea była stałą bywalczynią rosyjskich nocy i mówiła biegle po rosyjsku i angielsku. Urodzona w północnej Mongolii, w czasach kiedy w jej kraju wciąż silne były wpływy sowieckie, uczyła się rosyjskiego w szkole do momentu, kiedy Związek Radziecki upadł i premier Mongolii ogłosił, że angielski będzie drugim oficjalnym językiem pozbawionego dostępu do morza kraju.

Szukając przygód i lepszego życia, wygrała studencką wizę i w 2001 roku wyjechała do USA. Pierwsza myśl, jaka pojawiła się w jej głowie po wylądowaniu na międzynarodowym lotnisku w Los Angeles tamtego lata, była taka, że Amerykanie są strasznie grubi, ale kiedy dojechała do miasta, zrobiło ono na niej duże wrażenie; lubiła pięknych ludzi, a w Los Angels było ich pełno.

Po jednym semestrze w pomaturalnym studium w Torrance przeniosła się do Bay Area i dostała zieloną kartę. Teraz studiowała w Peralta College w Oakland, zarabiając na mieszkanie i czesne podawaniem lodów w Fentons Creamery.

Liz wydawała się z niewiadomych powodów zachwycona, kiedy dowiedzia-

ła się, że Tea mówi po rosyjsku. Bliźniaczki postawiły jej drinka, a potem powiedziały, że idą na imprezę z przyjaciółmi w ich hotelu cztery budynki dalej.

Było po północy, kiedy dotarły do apartamentu Chrisa Aragona w luksusowym Gift Hotel

w pobliżu Union Square.

Chris właśnie tam odpoczywał. Od razu wydał jej się bardzo przystojny.

Wyglądało na to, że ona również mu się spodobała, szczególnie kiedy bliź-

niaczki powiedziały, że Tea zna rosyjski. Kiedy dołączyły do nich jeszcze dwie pracowniczki Chrisa, otworzyli butelki z alkoholem i balangowali aż do rana -

wszystkie dziewczyny rozeszły się wówczas po swych pokojach, a Tea została na noc u Chrisa.

Następnego ranka, jeszcze dobrze się nie obudziła, gdy w pokoju zaczął się wielki ruch. Liz i kilka innych młodych atrakcyjnych kobiet - wszystkie skon-centrowane i pozbawione śladów nocnej zabawy - zaczęły biegać tam i z 155

powrotem, odbierając koperty i zaszyfrowane instrukcje od Chrisa*.

* Liz była jedną z dziewczyn, które robiły zakupy dla Chrisa, ale nie ma dowodów, by jej siostra również była w to zaangażowana.

Przez cały dzień przychodziły i wychodziły, biorąc kolejne koperty, zostawiając torby z zakupami z domów towarowych, czasem ociągając się z kolejnym wyjściem. Atmosfera imprezy unosiła się w powietrzu, ale teraz towarzyszyło jej coś nerwowego i podniecającego, co budziło ciekawość Tei, ale nie aż do tego stopnia, by wtykać nos w nie swoje sprawy.

Po zachodzie słońca ekipa zebrała się ponownie w apartamencie. Tea pożegnała się, musiała wracać do domu w East Bay, by rano być w pracy w barze z lodami.

Chris miał lepszy pomysł. Rozkręca właśnie stronę ze swoim biznesowym wspólnikiem „Samem” i tak się składa, że potrzebują na pełny etat tłumacza z rosyjskiego. To będzie lepiej płatne zajęcie niż nakładanie lodów Coffee Co-okie Dream różnym yuppies przez cały dzień.

- Nie odchodź - powiedziała Liza. - Z nami zarobisz więcej pieniędzy.

Tea popatrzyła na swoje nowe piękne przyjaciółki. Przypominały jej „nowych Rosjan”, którzy pojawili się po upadku Związku Radzieckiego, błyszcząc bogactwem zdobytym w podejrzany sposób, pozbawionych dobrego smaku i spragnionych dóbr konsumpcyjnych.

Jednak Chris jej się spodobał, wydawał się inny. Praca internetowej tłu-maczki zapewniłaby jej wolność i elastyczność, dzięki którym mogłaby się skupić na swoich studiach. Zgodziła się.

Następnego dnia Chris zabrał swoją ekipę w kolejny etap ich podróży - wyjazd samochodem do Vegas. Powiedział, że Tea powinna się tam z nimi spotkać, by jeszcze poimprezować. Kazał jej założyć maila na Yahoo!, by móc jej wysłać informacje na temat lotu, kiedy już będą na miejscu.

Po powrocie do mieszkania cała przygoda wydała jej się dziwnym snem.

Ale nazajutrz Tea znalazła potwierdzenie zakupu biletu lotniczego do Las Vegas w swojej skrzynce na Yahoo! Spakowała się i ruszyła na lotnisko.

Chris znalazł dla Tei mieszkanie w sąsiedztwie i zapłacił jej, żeby wynajęła pod prawdziwym nazwiskiem mieszkanie w Dana Point, nadbrzeżnym mieście w południowej części Orange County. Na końcu spokojnej, krętej ślepej uliczki, w kolorze umbryjskiego pomarańczu z hiszpańskimi dachówkami wieńczą-

cymi dach, Tea House, jak go nazwał, dzieliły lata świetlne od mongolskiego miasta, w którym dziewczyna się wychowywała.

Kochali się na jej nowym łóżku, a potem Chris zostawił 40 dolarów na jej nocnym stoliku, by zrobiła sobie manikiur. Zraniło to uczucia Tei. Nie była dziwką. Zakochała się.

Chris wraz ekipą przeniósł sprzęt do produkcji kart z Villi Siena do garażu przy mieszkaniu w Dana Point - Tea House stanie się jego nową fabryką i miejscem imprez oraz bazą dla dwudziestoczterogodzinnej pracy Tei na Carders Market. Jej zadaniem będzie przesiadywanie na wschodnioeuropejskich forach cardingowych, takich jak Mazafaka, oraz zdawanie relacji z tego, co się dzieje na rosyjskim oddziale Carders Market.

Chris wyjaśnił jej, że potrzebuje nicka, pseudonimu dla wirtualnego *alter ego.* Wybrała imię „ Alenka” od nazwy rosyjskiego cukierka.

Alenka rozpoczęła pracę od razu, z nosem przyklejonym do monitora w Tea House w dzień i w nocy, starając się ściągnąć potężnych Rosjan na stronę prowadzoną przez Chrisa i „Sama” Whiza.

ROZDZIAŁ 21

Master Splyntr

Siedziba National Cyber Forensics and Training Alliance mieszcząca się na pierwszym piętrze biurowca w kolorze limonici na brzegu Monongahela River była daleka od hermetyczności wywiadowczej wspólnoty z Waszyngtonu, gdzie Mularski zdobywał szlify. Dziesiątki ekspertów bezpieczeństwa z banków i firm technologicznych pracowały tutaj ze studentami z pobliskiego Carnegie Mellon University, siedząc razem w grupie boksów otoczonych pierścieniem biur, w budynku ze ścianami z przyciemnionego szkła. Z krzesłami Ae-ron i wytartymi do czysta stolikami biuro sprawiało wrażenie, że jedna z korporacji z branży technologicznej sporo zainwestowała w NCFTA. FBI dokona-

ło kilku zmian przed wprowadzeniem się, przekształcając jedno z pomieszczeń w centrum elektronicznej komunikacji, wypełnione posiadającymi rządowe certyfikaty komputerami i urządzeniami szyfrującymi, aby bezpiecznie komu-nikować się z Waszyngtonem.

W swoim biurze Mularski przeglądał „diagram", który Crabb, inspektor pocztowy, przesłał mu mailem - potężny schemat organizacji, pokazujący asy-metryczne połączenia między 125 nieuchwytnymi celami w półświatku.

158

Mularski uświadomił sobie, że jego podejście było błędne - czekał na przestępstwo, by potem wytropić sprawcę. Przestępcy wcale się nie ukrywali. Rekla-mowali swe usługi na forach, co było ich słabym punktem. Podobnie jak rytuały i ścisła hierarchia nowojorskiej i chicagowskiej mafii, które stały się dla FBI przewodnikiem umożliwiającym jej rozbicie kilka dekad wcześniej.

Nie pozostawało mu nic innego, jak tylko zostać carderem.

Wybrał forum z listy przysłanej przez Crabba i kliknął na link rejestracyjny.

Według regulacji Departamentu Sprawiedliwości Mularski mógł infiltrować forum bez pozwolenia z Waszyngtonu, pod warunkiem że przestrzegał w swej działalności ścisłych ograniczeń. Aby uniknąć zdemaskowania, mógł wysyłać informacje na bulletin board forum, ale nie wolno mu było kierować ich bezpo-

średnio do kogoś konkretnego, dostał pozwolenie na nie więcej niż trzy „bezpośrednie" kontakty z innym członkiem forum. Branie udziału w przestępstwie lub kontrolowany zakup od sprzedawcy nie wchodziły w grę. Operacja nie mogła wykraczać poza zbieranie informacji. Agent miał być jak gąbka, wchła-niając informacje o swych przeciwnikach.

Kiedy tylko wszedł na forum, musiał podjąć najważniejszą strategiczną decyzję: jaki będzie jego hakerski nick? Mularski poszedł za swym instynktem.

Zainspirowany przez emitowaną w sobotnie poranki kreskówkę *Wojownicze Żółwie Ninja* agent wybrał pseudonim zamieszkującego kanały ściekowe mi-strza karate, poruszającego się na dwóch łapach szczura zwanego Master Splin-ter. Żeby uczynić go bardziej unikalnym i nadać mu hakerskiego sznytu, zapisywał swój nick bez najważniejszych samogłosek.

Tak więc w lipcu 2005 roku Master Splyntr dołączył do swego pierwszego przestępczego forum, CarderPortal, śmiejąc się w duchu z ironii tkwiącej w przyjęciu imienia podziemnego szczura.

Mularski miał wkrótce grać na forach carderów jak na szachownicy, korzystając ze strumienia danych na temat oszustw z NCFTA w swoim pierwszym posunięciu.

159

Centrum miało bezpośrednie połączenie z przeciwdziałającymi oszustwom ekspertami w bankach i sklepach internetowych, kiedy więc przestępcy wymy-

ślili coś nowego, Mularski od razu się o tym dowiadywał. Napisał posta na temat przekrętów z CarderPortal, przedstawiając je jako własne wynalazki.

Doświadczeni oszuści zachwycali się nowicjuszem, który sam wpadł na ich najnowsze triki. A kiedy oszustwa ostatecznie zostały upublicznione w prasie, nowi pamiętali, że najpierw słyszeli o nich od Master Splyntra.

Agent FBI tymczasem wchłaniał historie forów, doskonaląc swój styl pisania, by sprawnie posługiwać się cynicznym, soczystym językiem półświatka.

Po kilku miesiącach Mularski stanął przed pierwszą poważną przeszkodą w zdobywaniu informacji. Pierwsze fora, które pojawiły się po upadku Shadowcrew, były szeroko otwarte dla nowych członków. Wielu oszustów, wystraszo-nych operacją „Firewall", przyjęło nowe nicki, rezygnując tym samym ze zdobytej reputacji, nie było więc sposobu, by carderzy mogli się wzajemnie sprawdzić. Teraz to się zmieniało. Pojawił się nowy gatunek „forów za porę-

czeniem". Jedynym sposobem na dostanie się od nich było zdobycie poparcia dwóch członków. Ograniczony wytycznymi Departamentu Sprawiedliwości Mularski świadomie unikał nawiązywania bliższych znajomości w półświatku, któż więc miałby za niego poręczyć?

Korzystając z pomysłu zaczerpniętego z powieści Roberta Ludluma, agent postanowił, że Master Splyntr potrzebuje legendarnej przeszłości, dzięki której mógłby się dostać na nowe przestępcze fora. Pomyślał o mającej swą siedzibę w Europie organizacji Spamhaus (Dom spamu), walczącej ze spamem, z którą wcześniej współpracował w czasie jednej z operacji FBI.

Założony w 1998 roku przez byłego muzyka Spamhaus prowadził ciągle zmieniający się rejestr adresów internetowych, z których zaśmiecano skrzynki mailowe klientów. Ze stworzonej przez organizację bazy spamerów korzysta dwie trzecie światowych dostawców Internetu, tworząc swoje czarne listy.

Mularskiego interesowała jednak lista najbardziej poszukiwanych, cieszących 160

się złą sławą spamerów. Pełna takich postaci jak Alan „Spam King" Ralsky czy Rosjanin Leo „Bad-Cow" Kuwajew Registry of Known Spam Operation (Rejestr Zidentyfikowanych Spamerów) albo w skrócie ROKSO, jest drugą po liście skazanych przez federalną wielką ławę przysięgłych, i żaden internetowy oszust nie chciałby ujrzeć na niej swojego nazwiska.

Mularski zadzwonił do Monako, do założyciela organizacji Steve'a Linfor-da, by przedstawić mu swój plan. *Chciał* znaleźć się na ROKSO albo przy-najmniej umieścić tam Master Splyntra. Linford zgodził się i agent zabrał się do wymyślania swej historii. Najlepsze kłamstwa mają w sobie trochę prawdy, postanowił więc, że jego przestępcze *alter ego* będzie polskim spamerem. Mularski miał polskie korzenie - przodkowie jego ojca przyjechali z kraju nad Wisłą. Pod swym służbowym mundurem, na lewym ramieniu miał tatuaż orła białego ze złotym dziobem i szponami, godło Polski. Na miejsce zamieszkania Master Splyntra wybrał Warszawę. Był kiedyś w stolicy Polski i w razie czego potrafił ją z grubsza opisać.

W sierpniu słowo stało się ciałem - ROKSO po raz pierwszy umieścił na swej liście „prawdziwe" nazwisko zainspirowanego kreskówką *alter ego* agenta.

Pavel Kamiński, znany jako „Master Splyntr", przewodził luźno zorganizowanej grupie spamerów i oszustów z Europy Wschodniej. Przypuszczalnie związany z BadCow. Przypisuje mu się spamowanie przez proxy spam, phishing, oszustwa giełdowe, exploity javascript, uczestnictwo w forach carderów, ataki przy użyciu botnetów.

Profil zawierał fragmenty spamu, którego wysyłanie przypisywano Kamin-skiemu, sprokurowane przez Spamhaus, oraz analizy jego hostingu.

Teraz carderzy, którzy zgooglowali Master Splyntra, mogli się przekonać, że był on prawdziwym, twardym cyberoszustem z Europy Wschodniej, 161

którego lepkie ręce sięgają po wiele różnych dóbr. Kiedy Mularski zalogował

się na CarderPortalu, w jego skrzynce czekały propozycje wysłane przez oszustów, którzy chcieli z nim współpracować. Nadal pozbawiony możliwości an-gażowania się w takie relacje, wyśmiewał ich oferty.

Nie jesteś poważnym graczem, odpisywał. Nie chcę się z tobą zadawać, bo jestem profesjonalistą, a ty najwyraźniej dopiero zaczynasz. Aby odrzucić oszustów z górnej półki, kwestionował zawartość ich portfeli: nie masz tyle pieniędzy, by wejść w to, czym się zajmuję.

Jak w wypadku niedostępnej dziewczyny na balu maturalnym - wyniosłość Master Splyntra uczyniła go tylko jeszcze atrakcyjniejszym. Kiedy powstało nowe, zamknięte forum International Association for the Advancement of Criminal Activity (Międzynarodowe Stowarzyszenie Rozwoju Aktywności Przestępczej), wysłał krótką wiadomość: „Cześć, potrzebuję poręczenia", i dwóch członków poparło go, ręcząc za jego dobrą reputację.

Potem w ten sposób dostał się na Theft Services i CardersArmy. W listopadzie 2005 roku został jednym z pierwszych członków nowo powstałego forum Darkmarketws.

Kilka miesięcy później kolejna konkurencyjna strona stała się na tyle duża, by zwrócić uwagę Master Splyntra - wkrótce trafił on na Cardersmarket.com.

ROZDZIAŁ 22

Wrogowie

Jonathan Giannone właśnie się przekonywał, że ceną za robienie interesów z Icemanem jest utrata prywatności.

Pracował z tajemniczym hakerem od ponad roku - zajmując się głównie zdobywaniem serwerów, których Iceman używał do skanowania w poszukiwaniu słabych punktów - i ciągle był pod nieustanną elektroniczną kontrolą hakera. Kiedyś Iceman wysłał mu link mający prowadzić do artykułu CNN na temat komputerowych problemów JetBlue, linii lotniczych, od których dawno temu Giannone bez powodzenia próbował wymusić haracz. Chłopak bez zastano-wienia kliknął na link - i tak po prostu Iceman znowu znalazł się w jego komputerze, przeprowadzając zwycięski atak od strony klienta.

Giannone zaczął rutynowo sprawdzać, czy na jego komputerze nie pojawiło się złośliwe oprogramowanie, ale nie mógł nadążyć za włamaniami Icemana.

Max zdobył hasło Giannonego do konta na United Airlines Mileage Plus i za-czął śledzić jego ruchy na całym świecie. Giannone był wielkim miłośnikiem podróży lotniczych i czasem latał tylko po to, by uzbierać dodatkowe mile.

Kiedy wylądował na międzynarodowym lotnisku w San Francisco, w komórce 163

znalazł esemesa od Icemana: „Po co przyleciałeś do San Francisco?”.

Mogłoby to być zabawne, gdyby nie przerażająca huśtawka nastrojów Icemana. W ciągu minuty mógł się obrócić przeciw tobie - jednego dnia byłeś jego najlepszym przyjacielem, „supergościem”, a następnego był przekonany, że jesteś kablem, oszustem albo kimś jeszcze gorszym. Wysłał Giannonemu obszerny, spontaniczny mailowy pamflet, będący długą listą żalów do Chrisa i innych członków społeczności carderów.

Przemawia przez niego zazdrość, pomyślał Giannone. Podczas gdy on wspólnie z Chrisem imprezował w Vegas i OC, Iceman siedział zamknięty w swym mieszkaniu, tyrając jak wół. Rzeczywiście hakerskie porywy często mia-

ły miejsce w czasie, kiedy Giannone przebywał w Kalifornii. W czerwcu 2005

roku Iceman zaatakował, gdy Giannone znalazł się na pokładzie porannego samolotu do Orange County - objechał go za jakieś niedopatrzenie w jednym z ich wspólnych przedsięwzięć. Pierwsza wiadomość trafiła na BlackBerry Giannonego o szóstej rano - trzeciej nad ranem czasu San Francisco - i esemesy płynęły nieprzerwanie przez ponad 4000 kilometrów, zanim Iceman w koń-

cu zamilkł, kiedy samolot lądował. Gdy Giannone sprawdził później maila, znalazł całą masę listów z przeprosinami od hakera: „Sorry, przepraszam cię.

Świrowałem”.

Wcześniej, we wrześniu 2004 roku, Giannone powiedział Icemanowi, że wkrótce poleci odwiedzić Chrisa, a Max napomknął między wierszami, że może sprawić, by ta podróż nie doszła do skutku. Giannone wybuchnął śmiechem. Ale półtorej godziny po starcie samolot gwałtownie zawrócił i skierował

się do Chicago. Kiedy wylądowali na lotnisku O'Hare, kapitan wyjaśnił, że w centrum kontroli ruchu powietrznego w Los Angeles miała miejsce awaria, która zmusiła samolot do zmiany trasy.

Okazało się, że jej przyczyną był błąd komputera. Znany robak w działają-

cym na Windowsie systemie kontroli radiowej w Los Angeles Air Route Traf-fic Control Center w Palmdale wymagał od techników zrestartowania komputera co 49,7 dnia. Zapomnieli tego zrobić, a backup systemu zawiódł w tym 164

samym czasie. W wyniku awarii setki lotów zostało odwołanych, w pięciu przypadkach samoloty przeleciały zbyt blisko siebie, niż na to pozwalają prze-pisy bezpieczeństwa. Nie stwierdzono żadnych zewnętrznych przyczyn awarii, ale kilka lat później, kiedy ujawniony został pełen zakres możliwości Maksa Visiona, Giannone zastanawiał się, czy przypadkiem Iceman nie zaatakował

komputerów FAA, wprowadzając zamęt w Los Angeles tylko po to, by nie mogli sobie z Chrisem połazić po klubach.

W końcu Giannone podjął radykalne kroki, by powstrzymać Icemana przed wtrącaniem się w jego sprawy. Kupił komputer Apple'a. Iceman mógł się dostać niemal wszędzie, ale Giannone był mocno przekonany, że nie będzie w stanie zhakować maca.

Podczas gdy Max kontynuował inwigilowanie swych wspólników, Carders Market powoli zaczął wzbudzać zainteresowanie, podsycane jeszcze tajemniczą wyniosłością jego założycieli. Jako Iceman i Easylivin' Max i Chris nie byli znani innym carderom, ale starzy wyjadacze potrafili wyczuć w ich postach uliczny spryt i to, że można im zaufać. Wieści o nowym forum dotarły do mieszkającego w Seattle Dave'a „El Mariachiego" Thomasa, byłego współpracownika FBI, który - jak Max - próbował zaalarmować carderów z powodu operacji „Firewall". Thomas czuł się zagubiony, odkąd federalni zamknęli jego akcję zbierania informacji, i szukał dla siebie nowego miejsca w sieci.

Początkowo nieufny, zarejestrował się pod innym nickiem, kiedy Iceman zainicjował publiczną dyskusję na temat charakteru i filozofii Carders Market, Thomas zabrał w niej głos, szczegółowo przedstawiając swoją opinię na temat kierunku, w którym powinna się rozwijać strona, by działać z powodzeniem, unikając losu Shadowcrew.

Na początku Chris i Max sądzili, że Thomas może wnieść wiele dobrego.

Wkrótce zauważyli jednak, że czepiał się jednego z ich starannie wybranych adminów, Bretta „Gollumfuna" Johnsona.

165

Plotki na temat Johnsona krążyły od czasu jego powrotu do półświatka -

nikt nie znika tak po prostu na dwa lata, żeby znów pojawić się jakby nigdy nic na przestępczych forach. W sierpniu jeden z carderów o nicku „Manus Dei" -

Ręka Boga - dolał oliwy do ognia, kiedy włamał się do skrzynki mailowej Johnsona i zamieścił jego złośliwy profil na Google Group zwanej FEDwatch.

Ujawnił tam prawdziwe nazwisko Gollumfuna, jego aktualny adres w Ohio i masę osobistych informacji wykradzionych z jego skrzynki. Wśród nich znalazła się sensacyjna

wiadomość: Johnson korespondował z reporterem „New York Timesa”, pisząc o cardingowym półświatku, i zarejestrował domenę o tajemniczej nazwie Anglerphish.com, być może przygotowując się do stworzenia własnej strony.

Nic jednak nie wskazywało na to, że Johnson kablował, i ani Maksa, ani Chrisa te rewelacje szczególnie nie poruszyły. Natomiast Thomas był teraz przekonany, że założyciel Shadowcrew jest konfidentem. W końcu Johnson ogłosił swoje odejście przed operacją „Firewall”, by już po wszystkim pojawić się znowu bez żadnego wytłumaczenia.

Ostatnia rzeczą, jakiej potrzebowali Chris i Max na swej rozwijającej się stronie, była walka między dwoma carderami ze starej szkoły, chowającymi urazy z czasów Shadowcrew. Ciągle pełen ambicji Chris pragnął, aby strona stała się najlepszym z możliwych forów przestępczych. Dotarł więc do Thomasa przez ICQ, aby spróbować rozwiązać problem.

„Nie mam zamiaru robić tutaj żadnego dramatu z powodu Gollumfuna lub innych, kłócić się, kto jest, a kto nie jest kapusiem - napisał Chris. - Po prostu chcę mieć tu czyste, miłe miejsce, w którym można by bezpiecznie się bawić”.

Chris obiecał, że to samo powie Johnsonowi: baw się grzecznie. To było dyplomatyczne zażegnanie konfliktu. Postąpił zgodnie z paternalistycznymi regułami, prosząc Thomasa o radę na temat prowadzenia forum z sukcesem, okazując starszemu carderowi szacunek ze względu na jego wieloletnie do-

świadczenie. Żeby się upewnić, że jego napomnienie zostało potraktowane 166

poważnie, Chris dodał ostrzeżenie. „Nie jesteśmy małolatami, koleś - napisał. -

Reprezentujemy naprawdę starą szkołę. I jesteśmy bardzo dobrzy w tym, co robimy”.

Thomas obiecał poprawę, dodając, że zrobi wszystko, by uczynić Carders Market wolnym od dramatów forum, którego wszyscy pragnęli. Ale w głębi duszy żywił coraz więcej podejrzeń. Dlaczego ktokolwiek miałby bronić Bretta Johnsona, skoro aż bije w oczy, że to kabel?

Zauważył, że Easylivin używał starej wersji ICQ, która przepuszczała adresy IR Thomas spróbował wyśledzić adres i dotarł do Bostonu, znanego jako wylęgarnia informatorów FBI. Carders Market był hostowany w Fort Lauderdale na Florydzie, kolejnym idealnym miejscu do prowadzenia tajnych operacji. A numer telefonu na liście nazw domen prowadził do kalifornijskiej policji, mimo że z innym numerem kierunkowym. Prawdopodobnie był to tylko zbieg okoliczności, ale kto wie?

Kiedy zakończył zbieranie dowodów, zrobiło mu się niedobrze. Carders Market był pułapką zastawioną przez federalnych. Teraz było to oczywiste.

Poprzysiągł sobie, że zrobi wszystko, co w jego mocy, aby zniszczyć tę stronę i wykończyć tych dupków ze starej szkoły, Easylivina i Icemana.

ROZDZIAŁ 23

Anglerphish

Max sam miał pewne podejrzenia wobec Bretta Johnsona. Zaczął uważnie przyglądać się adminowi Carders Market, sprawdzając strony, które odwiedzał, i dokładnie przeglądając jego prywatne wiadomości. Na dokładkę zhakował

konto Johnsona na International Association for the Advancement of Criminal Activity, IAACA, i sprawdził jego działalność. Nie znalazł niczego alarmują-

cego.

Czy naprawdę mógł ściągnąć konfidenta do grona zarządzających swą nową przestępczą stroną?

Problem polegał na tym, że nie istniał wiarygodny sposób, żeby stwierdzić, czy Johnson - lub ktokolwiek inny - pracuje dla rządu. Max bardzo pragnął

jednego: luki w zabezpieczeniach prawa, takiej jak przeładowanie bufora w BIND, której mógłby raz po raz używać przeciw każdemu, kogo podejrzewał.

„Jeśli (jest_kablem(Gollumfun)) banuj(Gollumfuna)". Zwierzał się Davidowi Thomasowi, nie wiedząc, że ten już umieścił Icemana na swej kilometrowej liście wrogów.

Kiedyś dla sprawdzenia przysłał nam pełne dane kont PayPala, które były ważne, i jak ustaliłem, nielegalne. Pomyślałem, że OK, ten facet 168

nie jest federalnym ani sługusem federalnych.

Muszę mieć pewność, ponieważ bazując na tej wiedzy, podejmuję decyzje wymagające zaufania. Liczymy na to, że wątpliwości ostatecznie rozstrzygnie prawnik, mój wspólnik powiedział, że się tym zajął i się dowie. Destem jednak sceptyczny co do tego, czy kiedykolwiek uzy-skamy jasną odpowiedź, ponieważ prawnicy lubią brać od nas pienią-

dze, oferując w zamian raczej domysły niż konkretne fakty. Być może po prostu mam złych prawników.

Naprawdę chciałbym znaleźć jakiś szczególny sposób na znalezienie czegoś, czego gliniarz lub gość z kontrwywiadu nie może zrobić.

Coś, co rozstrzygnęłoby wątpliwości w 100 procentach. Po prostu świę-

ty Graal. Do tej pory żyłem w przekonaniu, że „popełnienie przestępstwa" wyklucza przedstawicieli prawa. Jak ludzie, którzy wypalają z kimś skręta, by się upewnić, że ta osoba nie jest gliniarzem. Lub dziw-ka, która pyta swego klienta: „Jesteś gliniarzem? Wiesz, że jeśli jesteś, to musisz mi o tym powiedzieć".

Brett Johnson faktycznie nie był czysty. Ale wbrew podejrzeniom jego po-wrót na przestępczą drogę po „Firewallu" nie wiązał się z operacją szpiegowską. Wszystko zaczęło się od dziewczyny.

Przestępczy i kokainowy nałogi Johnsona odstraszyły jego żonę dziewięć lat temu - wychodząc, wyrzuciła jego MSR206 za drzwi i musiał szukać pomocy psychologa, żeby

dojść do siebie po tej stracie. Potem w barze w Północnej Karolinie spotkał Elizabeth, dwudziestoczteroletnią tancerkę egzotyczną w miejscowym klubie ze striptizem, i zakochał się od pierwszego wejrzenia.

Przepuścił oszczędności, kupując jej prezenty - a to torebkę za 1500 dolarów, a to buty za 600. Po pięciu miesiącach zamieszkała z nim, ale kiedy kochali się pierwszy raz, nie pozwoliła mu się pocałować.

169

Najgorsze podejrzenia Johnsona potwierdziły się, kiedy znalazł Elizabeth na stronie, gdzie mężczyźni zamieszczają recenzje striptizerek i prostytutek. Tam było wszystko, słowo po słowie, odrażające szczegóły na temat usług, które świadczyły dziewczyny w zamian za kokainę i pieniądze. Pokazał jej dowody, a ona gorąco przyrzekła, że zerwie z prostytucją i narkotykami.

Mając nadzieję, że wyrwie ją z kolein dawnego życia, Johnson zasypywał

Elizabeth jeszcze większą ilością prezentów i zapraszał na drogie kolacje. Wła-

śnie to, a nie tajna współpraca z policją, skłoniło go do powrotu na dawną ścieżkę. Po prostu potrzebował pieniędzy.

Szczęście, dzięki któremu przetrwał operację „Firewall”, opuściło go 8 lutego 2005 roku, kiedy w Charleston w Północnej Karolinie policja zatrzymała go za posługiwanie się podrobionymi czekami Bank of America, którymi płacił

za krugerrandy i zegarki kupione na eBay-u i wysyłał je za pobraniem do swych dziupli. Po wypełnionym tęsknotą za Elizabeth tygodniu odsiadki w Charleston County Detention Center odwiedzili Johnsona agenci Secret Service. Kiedy już przekonał ich, że to on był Gollumfunem, adminem, który wymknął im się z Shadowcrew, zgodzili się pomóc mu w stanowej sprawie, jeśli będzie dla nich pracował.

Secret Service obniżyła kaucję Johnsona do 10 000 dolarów. Kiedy ją wpła-cił, agenci przenieśli go z Charleston do Columbii w Południowej Karolinie, gdzie wynajęli dla niego mieszkanie i płacili mu 50 dolarów dziennie. Teraz był codziennym gościem w terenowym biurze w Columbii, przychodząc o czwartej po południu i pracując do dziewiątej, zabierając Secret Service na Carders Market i inne fora. Wszystko, co przechodziło przez jego komputer, było nagrywane i równocześnie pokazywane na czterdziestodwucalowym ekranie plazmowym powieszonym na ścianie biura.

Nazwali to operacją „Anglerphish” i Johnson pomyślał, że kiedyś napisze o tym świetną książkę. Dlatego właśnie zarejestrował domenę Anglerphish.com i zaczął rozmowy z reporterem z „New York Timesa”. Kiedy Manus Dei wykradł jego maile i udostępnił w sieci zawarte w nich informacje, mocodawcy 170

Johnsona z Secret Service byli wściekli. Natychmiast zakazali mu używania komputera poza biurem i kazali zerwać kontakty z reporterem. Elizabeth zostawiła go - jej nazwisko i zajęcie wyszły na jaw.

Potem Iceman pozbawił Johnsona uprzywilejowanej pozycji na Carders Market i oszuści, których znał od czasów Counterfeit Library, zaczęli unikać robienia z nim interesów. Johnson tracił zaufanie, a Secret Service traciła cierpliwość.

Pod koniec marca 2006 roku postanowili wszcząć postępowanie przeciw jednemu z nielicznych oszustów, którzy wpadli w pułapkę „Anglerphish", kalifor-nijskiemu złodziejowi tożsamości, który skradł 200 000 dolarów, wypełniając w Internecie formularze na fikcyjne zwroty podatku przez H&R Block, a potem samemu zabierając pieniądze. Johnson, ekspert od tego rodzaju przekrę-

tów, czatował z tym oszustem, a Secret Service odkryła, że ślady kontaktów online prowadzą do C&C Internet Café w Hollywood. Agent z Los Angeles odwiedził kawiarnię i usiadł dwa stoliki od mężczyzny, który właśnie wypeł-

niał fałszywe formularze zwrotu.

Jednak gdy miejscowa policja i agenci Secret Service zrobili nalot na mieszkanie w Hollywood, okazało się puste: żadnych komputerów i ani skraw-ka dokumentu, który mógłby posłużyć za dowód. Podejrzany zrobił wszystko z wyjątkiem dokładnego wyczyszczenia dywanów i pomalowania ścian.

Opiekunowie Johnsona w Columbii podejrzewali już, że status ich informatora został odkryty po aferze na Carders Market. Teraz mieli podstawy, by sądzić, że ostrzegł osobę, u której planowali wkrótce przeprowadzić rewizję.

Przynieśli wykrywacz kłamstw i podpięli Johnsona do urządzenia.

Pisaki nie poruszyły się, kiedy Johnson odpowiadał na pierwsze dwa pytania: czy kontaktował się z tą osobą? Czy ktoś inny na jego polecenie się z nią kontaktował? W pierwszym przypadku nie, w drugim też nie. Ostatnie pytanie 171

było szersze: czy Johnson miał nieuprawnione kontakty z kimkolwiek? „Nie" -

odpowiedział znowu, a odruch skórno-galwaniczny wywołał gwałtowny ruch na wykresie.

Johnson przyznał, że mimo ostrzeżeń agentów nadal w tajemnicy prowadził

rozmowy z dziennikarzem „New York Timesa", który bardzo poważnie traktował sprawę wspólnego napisania książki. Federalni przesłuchiwali Johnsona do drugiej nad ranem, po czym podpisał on formularz zgody na przeszukanie jego sponsorowanego przez agencję mieszkania.

Rewizja przypominała wielkanocny zwyczaj szukania pisanek. Agenci znaleźli kartę przedpłaconą w bucie w sypialnianej szafie. Notatnik zawierający numery kont, PIN-y i dane osobowe w łazience włożony do kosmetyczki.

Skarpetę zawierającą 63 karty bankomatowe schowaną w męskich spodniach w szafie. Plastikowa miseczka na dnie kosza na bieliznę zawierała prawie 2000

dolarów w gotówce. W końcu znaleźli też naładowane karty płatnicze Kinko; Johnson płacił nimi w lokalnym punkcie ksero, gdzie korzystał z komputera.

Prowadził potrójne życie niemal od samego początku swej współpracy z agencją, udając oszusta w terenowym biurze w Columbii, a po godzinach zajmował się swymi jak najbardziej prawdziwymi przekrętami.

Specjalnością Johnsona były te same oszustwa, które przeprowadzał facet wyśledzony w Los Angeles. Wyciągał on numery ubezpieczenia społecznego ofiar z internetowych baz danych, w tym także z California's Death Index, gdzie mógł znaleźć numery ostatnio

zmarłych mieszkańców Złotego Stanu, a następnie wypełniał fikcyjny formularz zwrotu podatku w ich imieniu, kierując otrzymane pieniądze na przedpłacone karty debetowe, przy użyciu których mógł wybierać pieniądze z bankomatu. Wyciągnął ponad 130 000 dolarów ze zwrotów podatku pod 41 nazwiskami, cały czas działając pod nosem Secret Service.

Agenci zadzwonili do człowieka, który wpłacił kaucję za Johnsona, i prze-konali go, by domagał się zwrotu 10 000, dzięki którym oszust wyszedł na wolność. Potem wsadzili Johnsona z powrotem do więzienia okręgowego.

172

Po trzech dniach opiekujący się nim agent pojawił się z wyższym rangą kolegą, który nie był zadowolony z informatora. „Zanim zaczniemy, Brett, chcę tylko powiedzieć, że albo opowiesz nam o wszystkim, co zrobiłeś w ciągu ostatnich sześciu lat, albo uczynię z gnojenia ciebie i twojej rodziny moją życiową misję

- warknął superwizor. - I nie mówię tylko o tych najświeższych zarzutach. Kiedy już wyjdziesz, nie dam ci spokoju do końca życia".

Johnson odmówił współpracy i agenci wypadli jak burza z jego celi. Biuro prokuratora krajowego zaczęło pracować nad federalnym oskarżeniem. Oszust miał jednak jeszcze jednego asa w rękawie. Dwa tygodnie później udało mu się przywrócić kaucję, dostać zwolnienie z aresztu i błyskawicznie zniknąć.

Operacja „Anglerphish" zakończyła się klęską. Efektem 1500 godzin pracy była ucieczka informatora i nowe oszustwa na dziesiątki tysięcy dolarów. Został tylko jeden promyk nadziei: pierwszy zestaw 29 platynowych zrzutów, które Johnson kupił w maju za 600 dolarów.

Secret Service znalazła ślad części z tych kart w pizzerii w Vancouver - był

to jednak ślepy zaułek. Ale firmowe konto w Bank of America, którego sprzedawca zrzutów użył do odebrania zapłaty, należało do niejakiego Johna Giannonego, dwudziestojednolatka mieszkającego w Rockville Centre na Long Island.

ROZDZIAŁ 24

Ujawnienie

„Tea, te dziewczyny to blachary. Nie zadawaj się z nimi - powiedział Chris. -

One myślą inaczej”.

Byli w Naan and Curry, całodobowej indyjsko-pakistańskiej restauracji w dzielnicy teatralnej San Francisco. Upłynęły trzy miesiące, odkąd Tea spiknęła się z Chrisem, i właśnie była z nim na jednym z comiesięcznych wypadów do Bay Area, gdzie miał się spotkać z tajemniczym przyjacielem, hakerem „Samem”, tuż przed zmierzchem. Byli teraz tylko cztery przecznice od kryjówki Maksa, ale Tea nie została mu przedstawiona ani tym razem, ani w czasie żadnej z kolejnych wizyt. Nikt nie spotyka się z Samem osobiście.

Była zafascynowana tym, jak to wszystko działa: bezgotówkowym charak-terem przestępstw, sposobem, w jaki Chris zorganizował swą ekipę. Powiedział

jej o wszystkim, kiedy uznał, że jest na to gotowa, ale nigdy nie prosił, by razem z innymi poszła na zakupy. Była kimś specjalnym. Nie lubił nawet, kiedy kręciła się w towarzystwie dziewczyn z ekipy, obawiając się, że w jakiś sposób mogłoby to skazić jej osobowość.

Była też jedyną pracownicą, która nie dostawała wypłaty. Po tym jak odrzuciła 40 dolarów, które Chris zostawił na jej nocnym stoliku. Uznał, że Tea, 174

mimo długich godzin spędzanych na Carders Market i rosyjskich forach przestępczych, w ogóle nie chce od niego żadnych pieniędzy. Dbał o płacenie za wynajem Tea House, kupował jej ubrania i fundował podróże, ale jej to wszystko wydawało się dziwne: życie online, podróżowanie na numery potwierdzenia zakupu zamiast na bilety samolotowe. Stała się duchem, ciałem była w Orange County, umysłem przeważnie na Ukrainie lub w Rosji, nawią-

zując przyjacielskie kontakty z przywódcami zorganizowanej cyberprzestępczości, jako emisariuszka Icemana z cardingowego półświatka Zachodu.

Stwierdziła, że Iceman jest naprawdę spoko. Zawsze był da niej przyjazny i traktował ją z szacunkiem. Kiedy Chris i jego wspólnik rozpoczynali jedną ze swych kłótni, każdy z nich plotkował na temat drugiego i żalił się jej przez ICQ

jak dziecko. Kiedyś Iceman wysłał jej masę zrzutów, sugerując, by sama we-szła w biznes, co bardzo oburzyło Chrisa.

Kiedy Chris i Tea paplali nad talerzami, wysoki mężczyzna z włosami spię-

tymi w kucyk wszedł do lokalu i ruszył w kierunku kasy z tyłu sali, zerknął ku nim, po czym podniósł siatkę z jedzeniem na wynos i zniknął.

Chris uśmiechnął się. „To był Sam”.

Fałszerskie przedsiębiorstwo Chrisa w Orange County przynosiło mu wystarczający dochód, by mógł wysłać dzieci do prywatnej szkoły, płacić za mieszkanie Tei, a w lipcu

zacząć szukać lepszego i większego domu dla siebie i rodziny. Jeździł oglądać domy z Giannonem i znalazł obszerny dom do wynaję-

cia - dwupiętrowy budynek w nadbrzeżnej części Capistrano Beach na końcu spokojnej ślepej uliczki na urwisku wznoszącym się ponad piaszczystą plażą.

Była to okolica przyjazna dla rodziny, z koszami do koszykówki wiszącymi nad garażami i łodziami stojącymi na sąsiedzkich podjazdach. Miał się wprowadzić 15 lipca. Giannone przyleciał znowu na weekend 4 lipca - ostatnie święta Chrisa w starym mieszkaniu - ale ostatecznie znalazł się w Tea House, 175

podczas gdy Chris spędzał te dni z rodziną. To zdarzało się często. Giannone zjawiał się na Lotnisku Johna Wayne'a, oczekując, że spędzi weekend, impre-zując z Chrisem, a zamiast tego kończył u jednej z dziewczyn z ekipy albo musiał siedzieć w domu Chrisa, niańcząc jego synów. Tea była znośna, inna od tanich imprezowiczek wydających pieniądze z kart Chrisa, ale w mieszkaniu w Dana Point czas się dłużył.

Zadzwonił do Chrisa, skarżąc się, że się nudzi. „Przyjedź do mnie -

powiedział Chris. Byli na basenie. - Jest tutaj moja żona z dziećmi".

Giannone zabrał z sobą Teę, która nigdy nie widziała mieszkania Chrisa, znajdującego się zaledwie sześć kilometrów dalej. Kiedy się zjawili Chris, Clara i dwaj chłopcy chlapali się w basenie, ciesząc się słoneczną pogodą.

Giannone i Tea przywitali się i rozsiedli wygodnie na leżakach.

Chris wyglądał na kompletnie zaskoczonego. „Widzę, że przyprowadziłeś przyjaciółkę" - powiedział do Giannonego ze złością.

Clara znała chłopaka, ponieważ czasem zajmował się dziećmi, ale nigdy nie widziała Tei. Popatrzyła na dziewczynę, potem na Giannonego, potem znów na Mongołkę i grymas gniewu, który pojawił się na jej twarzy, świadczył, że wszystkiego się domyśliła.

Giannone uświadomił sobie, że strzelił gafę. Obie kobiety wyglądały zaskakująco podobnie. Tea była młodszą wersją żony Chrisa i wystarczyło jedno spojrzenie, by Clara wiedziała, że jej mąż sypia z tą kobietą.

Chris wyskoczył z basenu i podszedł do miejsca, w którym siedzieli. Jego twarz nie zdradzała uczuć. Przykucnął naprzeciw Giannonego, woda z jego włosów kapała na beton. „Co ty wyprawiasz? - powiedział ściszonym głosem. -

Spadajcie stąd".

Wyszli. Po raz pierwszy od czasu kiedy spiknęła się z Chrisem Aragonem i jego gangiem, Tea poczuła się brudna.

Chris nie był wściekły - widok Tei i Clary obok siebie sprawiał mu wsty-dliwą przyjemność samca alfa. Zadurzenie Tei zaczynało jednak być problemem. Żywił szczere uczucia dla niej i cenił jej indywidualność, ale stawała się dla niego ciężarem.

176

Znalazł jednak idealne rozwiązanie: wysłał ją na przedłużone wakacje do rodzinnego kraju. Kupując bilet lotniczy, dosłownie wygonił swą zbyt żarliwą kochankę do Mongolii

Zewnętrznej.

Podczas gdy Chris był zajęty swym skomplikowanym życiem uczuciowym, Carders Market pożerał coraz więcej czasu Maksa, który poza tym ciągle prowadził jeszcze interesy jako „Digits”. Pracował teraz w branży gastronomicznej, co przynosiło duże zyski.

Zaczęło się to w czerwcu 2006 roku, kiedy pojawiła się poważna luka w oprogramowaniu RealVNC dia „virtual network console” - kontrolowanego zdalnie programu używanego do zarządzania komputerami z Windowsem przez Internet.

Robak był w krótkiej sekwencji uzgodnienia parametrów transmisji danych, otwierającej każdą nową sesję między klientem VNC a serwerem RealVNC.

Kluczowa część uzgodnienia nadchodzi, kiedy serwer i klient negocjują typ zabezpieczeń, który należy zastosować w danej sesji. Proces ten przebiega w dwóch etapach: najpierw serwer RealVNC wysyła klientowi skrótową listę protokołów bezpieczeństwa, które serwer obsługuje. Ta lista jest po prostu szeregiem cyfr, na przykład [2,5], co oznacza, że serwer obsługuje typ 2 zabezpieczenia VNC i relatywnie prosty schemat uwierzytelniania hasła oraz typ 5, w pełni szyfrowane połączenie.

W drugim etapie klient mówi serwerowi, którego z oferowanych protoko-

łów bezpieczeństwa chce użyć, odsyłając swój właściwy numer, jak przy za-mawianiu chińszczyzny z menu.

Problem polegał na tym, że RealVNC nie sprawdzał odpowiedzi od klienta, by zobaczyć, co było w menu na pierwszym miejscu. Klient mógł odesłać jakikolwiek typ zabezpieczeń, nawet taki, którego serwer nie oferował, a serwer akceptował go bez przeszkód. Obejmowało to typ 1, który prawie nigdy nie jest oferowany, ponieważ wcale nie stanowi on zabezpieczenia. Pozwala natomiast zalogować się w RealVNC bez hasła.

Zmodyfikowanie klienta VNC tak, aby zawsze wysyłał typ 1, zmieniając go w wytrych, nie przedstawiało trudności. Włamywacz taki jak Max mógł wykorzystać swój znakowany program na każdym komputerze, na którym działał

RealVNC, i błyskawicznie uzyskać do niego dostęp.

Max zaczął skanowanie w poszukiwaniu podatnego na atak sprzętu z zain-stalowanym RealVNC, gdy tylko dowiedział się o pojawieniu się dziury. Patrzył zdumiony, jak wyniki ukazują się na ekranie; były ich tysiące: komputery w domach i na uczelniach, w biurach Western Union, bankach i hotelowych lobby. Logował się do niektórych, wybierając je na chybił trafił, w jednym znalazł obraz z telewizji przemysłowej monitorującej w holu biurowca. Inny był komputerem w departamencie policji w Midwest, gdzie mógł słuchać rozmów z numerem 911. Trzeci zaprowadził go do systemu kontrolowania klima-tyzacji właściciela domu: Max podniósł temperaturę o 10 stopni i ruszył dalej.

Bardziej interesujący był dla Maksa mały ułamek tego systemu, dobrze mu znany z nadal kontynuowanych włamań do Pizzy Schmizzy: restauracyjne terminale płatnicze. Tu były pieniądze. W przeciwieństwie do banalnie pro-stych terminali spoczywających na ladach sklepów z alkoholem i spożywcza-ków za rogiem, systemy w restauracjach stały się

bardziej wyrafinowane. Wykorzystywały rozwiązania „wszystko w jednym”, które zajmowały się dosłownie wszystkim - od przyjmowanych zamówień po ustawianie krzeseł, i pracowały na Microsoft Windows. Aby obsługiwać maszyny zdalnie, sprzedawcy usług instalowali w nich tylne wejście, w tym VNC. Ze swym wytrychem VNC

Max mógł otworzyć wiele z nich, kiedy tylko chciał.

Tak więc Max, który kiedyś zeskanował cały system obrony USA, szukając podatnych serwerów, teraz ze swego komputera przetrząsał Internet dzień i noc, znajdując i włamując się do pizzerii, włoskich restauracji, francuskich bistro i grill-barów w amerykańskim stylu; zbierał dane z pasków magnetycznych, gdziekolwiek je znalazł.

Po wprowadzeniu przez Visę standardów bezpieczeństwa nie powinno to być możliwe. W roku 2004 firma zakazała używania wszystkich terminali, 178

które zachowują dane z pasków magnetycznych po zakończeniu transakcji.

Starając się nadążyć za standardami, wszystkie duże firmy handlowe stosowały łatki, które miały sprawić, że ich systemy nie będą przechowywać tych danych.

Ale właściciele restauracji nie starali się ściągać uaktualnień, za które czasem trzeba było dodatkowo płacić.

Skanująca maszyneria Maksa miała kilka ruchomych części. Pierwsza była nastawiona na znajdowanie instalacji VNC, wykonując bardzo szybkie „prze-miatanie portów” - standardową technikę rekonesansową, która wykorzystuje otwartość i standaryzację Internetu.

Od samego początku protokoły sieciowe były projektowane tak, by pozwolić komputerom żonglować różnymi typami połączeń równocześnie. Dzisiaj może to dotyczyć także maili, ruchu na stronach, przesyłania plików i setek innych bardziej ezoterycznych usług. Aby trzymać to wszystko oddzielnie, komputer rozpoczyna nowe połączenia z dwiema informacjami: adresem IP

komputera przeznaczenia i wirtualnym „portem” na tym komputerze, posiadającym numery od 0 do 65 535, który identyfikuje typ usługi szukanej przez połączenie. Adres IP jest jak numer telefonu, a port przypomina numer we-wnętrzny, który podajesz, aby centrala mogła wysłać twój telefon do właściwego biurka.

Numery portów są zestandaryzowane i opublikowane online. Oprogramowanie obsługujące maila wie, że należy połączyć z portem 25, aby wysłać wiadomość; przeglądarki internetowe łączą z portem 80, aby odzyskać stronę. Jeśli połączenie w określonym porcie zostaje odrzucone, przypomina to zajęty numer wewnętrzny; usługa, której szukasz, nie jest dostępna pod tym adresem IP.

Max był zainteresowany portem 5900, standardowym portem dla serwera VNC. Ustawił swoje komputery tak, by przeczesywały szeroki pas adresów internetowych, wysyłając do każdego pojedynczy sześćdziesięcioczterobajtowy zsynchronizowany pakiet, który sprawdzał, czy port 5900 był otwarty dla usłu-gi.

Adresy, które odpowiedziały na jego przeczesywanie, spływały do skryptu PERL, który Max napisał, łącząc go z każdą maszyną i próbując zalogować się 179

przez robaka RealVNC. Jeśli exploit nie zadziałał, skrypt próbował popular-nych haseł: „1234”, „vnc” lub pustej sekwencji.

Jeśli się dostał, program zbierał trochę wstępnych informacji o komputerze: jego nazwę, rozdzielczość i głębię koloru monitora. Max lekceważył komputery z monitorami o niskiej jakości obrazu, zakładając, że jest to sprzęt domowy, a nie firmowy. To była bardzo szybka operacja: haker działał na pięciu lub sześciu serwerach jednocześnie, z których każdy mógł przebiec przez sieć klasy B, ponad 65 000 adresów, w ciągu kilku sekund. Jego lista podatnych instalacji VNC rosła o około 10 000 dziennie.

Terminale płatnicze były niczym igły w wielkim stogu siana. Max mógł dostrzec niektóre z nich ze względu na nazwę: „Aloha” oznaczało, że dany sprzęt to najprawdopodobniej Aloha POS, wykonany przez Radiant Systems z Atlanty, jego ulubiony cel. „Maitre’D” był konkurencyjnym produktem z Posera Software w Seattle. W przypadku pozostałych trzeba było zgadywać. Jakikolwiek komputer o nazwie takiej jak „Server”, „Admin” czy „Manager” wymagał

dokładniejszego przyjrzenia mu się. Wślizgując się przez swego klienta VNC, Max mógł zobaczyć, co jest na ekranie komputera, tak jakby znajdował się dokładnie przed nim. Ponieważ pracował w nocy, wyświetlacz na uśpionym pececie był zazwyczaj ciemny, poruszał więc myszką, by wyłączyć wygaszacz ekranu. Jeśli ktoś był w pokoju, mogło to być trochę przerażające. Pamiętasz, kiedy ekran twojego komputera mrugnął bez przyczyny, a kursor drgnął? To mógł być Max Vision, który zaglądał na twój ekran.

Ten „ręczny” test był wolną częścią całego procesu. Max zatrudnił Teę do pomocy - dał jej klienta VNC i zaczął wysyłać jej listy podatnych komputerów, razem z instrukcjami, czego ma szukać. Wkrótce uzyskał dostęp do lokali gastronomicznych w całej Ameryce. Burger King w Teksasie. Sportowy bar w Montanie. Modny klub nocny na Florydzie. Bar z grillem w Kalifornii. Przeniósł się do Kanady i znalazł jeszcze więcej.

Zaczął karierę sprzedawcy od wykradzenia zrzutów z jednej restauracji. Teraz miał sto lokali, które dostarczały mu danych kart kredytowych niemal w 180

czasie rzeczywistym. Digits będzie robił o wiele więcej interesów.

Dave „El Mariachi” Thomas wybrał zły moment na wkurzanie Maksa, który miał mnóstwo pracy. W czerwcu Thomas zrobił coś niemal niespotykanego w całym odizolowanym komputerowym półświatku - przeniósł ich kłótnię z forum do przestrzeni publicznej, atakując Carders Market w komentarzach na popularnym blogu poświęconym bezpieczeństwu, gdzie zarzucił Icemanowi bycie „G” - gliniarzem.

„To jest strona hostowana w Fort Lauderdale na Florydzie - napisał Thomas. - Faktycznie jest hostowana prosto z domu jakiegoś faceta. Jednak G jej nie kasuje. Zamiast tego strona promuje sprzedaż PIN-ów, numerów, PayPali i eBayów i tak dalej, a G przez cały czas obserwuje wszystkich graczy.

G twierdzi, że nie może nic zrobić ze stroną hostowana na amerykańskiej ziemi. Jednak prawda jest taka, że to G prowadzi tę stronę, tak jak to było z Shadowcrew”.

Zwracając uwagę na sprawę hostingu Carders Market, Thomas celował w piętę achillesową Icemana. Strona funkcjonowała bez przeszkód, ponieważ Affinity nie zauważyła nielegalnego serwera wśród dziesiątek tysięcy legalnie hostowanych stron. El

Mariachi pracował nad tym, by to zmienić, nieustannie zalewając firmę skargami. Taktyka była pozbawiona logiki - gdyby Carders Market rzeczywiście był pod kontrolą władz, skargi nie zostałyby wysłuchane; tylko wówczas gdy byłaby to naprawdę przestępcza strona, Affinity by ją zdję-

ła. Jeśli Iceman utonie, będzie to oznaczało, że nie jest czarownicą.

W tydzień po poście Thomasa Affinity nagle skasowała Carders Market.

Zamknięcie strony wkurzyło Maksa, bo właśnie wszystko zaczęło mu się ukła-dać na ValueWeb. Szukał za granicą nowego legalnego hostingu, który byłby odporny na El Mariachiego, rozmawiając z firmami w Chinach, Rosji, Indiach i Singapurze. Zawsze kończyło się to w ten sam sposób: wymagano gotówki z góry jako opłaty za przystąpienie, a potem rozciągano czerwoną taśmę przed 181

drzwiami, pytając o paszport i licencje biznesową lub dokumenty firmy.

„Nie mogło istnieć, ponieważ miałeś KUREWSKO GŁUPIĄ NAZWĘ, CARDERS to lub CARDERS MARKET tamto, a teraz mogłoby istnieć? -

napisał Thomas, nabijając się z Icemana. - Może gdybyś nie krzyczał «ROBOTA DLA CARDERÓW TUTAJ«, mógłbyś utrzymać swoją stronkę i może urósłbyś do rozmiarów bestii, którą tak desperacko pragniesz być".

Teraz Thomas nienawidził Icemana, wszystko jedno, czy był on federalnym czy też nie, a Iceman odwzajemniał to uczucie.

Max ostatecznie postawił stronę w Staminus w Kalifornii w firmie specjali-zującej się w szerokopasmowym hostingu odpornym na ataki DDoS. Do tej pory Thomas dokopywał mu w komentarzach przypadkowego bloga pod na-zwą „Life on the Road" (Życie w drodze). Blogger cytował komentarze Thomasa o Carders Market w krótkich postach na temat forów, nieświadomie użyczając swego bloga jako pola bitwy w wojnie między El Mariachim a Icemanem.

Iceman podjął wyzwanie i opublikował długie publiczne odparcie zarzutów Thomasa, oskarżając swego wroga o „hipokryzję i oszczerstwo".

CM NIE jest ani „przestępczym forum", ani „imperium", żaden z tych bzdurnych zarzutów się do nas nie odnosi. Jesteśmy po prostu forum, które postanowiło dopuścić dyskusję o przestępstwach finansowych.

Użyczamy również autorytetu w ocenianiu, którzy członkowie są prawdziwi, a którzy nie, ale to tylko nasze opinie, nie bierzemy za to pienię-

dzy. Jesteśmy po prostu NOŚNIKIEM informacji, FORUM, za pośrednictwem którego komunikacja może odbywać się bez przeszkód. CM

nie jest zaangażowane w żadne przestępstwa. Prowadzenie forum i umożliwianie dyskusji nie jest zbrodnią. Prowadzenie Craigslist.com nie 182

jest nielegalne, mimo że zamieszczają tam swoje oferty prostytutki, dile-rzy narkotyków i inni przestępcy, ale ludzie nie nazywają Craigslist „me-liną dziwek i ćpunów" ani imperium zbrodni. Jest uważane za MEDIUM, które nie może odpowiadać za zawartość, jaka się w nim pojawia. To jest oświadczenie Carders Market.

W swej natchnionej obronie Max zupełnie pominął szczegółowe wskazówki dotyczące popełniania przestępstw i system ocen na Carders Market, nie wspominając nawet ukrytego impulsu, który stał za powstaniem tej strony -

stworzenie Maksowi miejsca do sprzedaży skradzionych danych.

Zdając sobie sprawę z tego, że hosting w Kalifornii nie zadowoli półświatka, Max wznowił poszukiwania odpowiedniego miejsca za granicą. W następnym miesiącu zhakował nowy serwer, tym razem w kraju tak dalekim od wpływów USA jak żaden inny w sieci. W kraju, po którym nie można było oczekiwać, że zareaguje ani na skargi Davea Thomasa, ani nawet amerykań-

skiego rządu.

„Carders Market jest teraz hostowany w IRANIE - ogłosił Max 11 sierpnia.

- Rejestracja jest ponownie otwarta".

ROZDZIAŁ 25

Wrogie przejęcie

„Na wojnie najważniejsza jest szybkość. Posuwaj się naprzód, korzystając z tego, że wróg jest nieprzygotowany, wybierz ukrytą marszrutę i uderz wtedy, kiedy on się tego nie spodziewa"*.

* Sun Tzu, *Sztuka wojny*, http://comma.dt.pl/e-books/BingFa/Screen/SCREEN.pdf, s. 72 (do-stęp: 19 lipca 2011).

Max czytał *Sztukę wojny* Sun Tzu, używając liczącego sobie 2600 lat tekstu jako podręcznika hakerskiego. Szkicował plany na dwóch tablicach w swej kryjówce. Po kilku starciach i pojawieniu się nowych kandydatów zostało pięć anglojęzycznych stron cardingowych, które liczyły się w półświatku. Zdaniem Maksa o cztery za dużo. Poświęcił całe tygodnie na śledzenie swych konkurentów: ScandinavianCarding, The Vouched, TalkCash, i swego głównego rywala, DarkMarket, strony z Wielkiej Brytanii, która pojawiła się miesiąc przed Carders Market i zyskała solidną reputację jako strefa wolna od ripperów.

W pewnym sensie plan Maksa, by wepchnąć się na inne fora, miał podłoże w tej części jego osobowości, która ciągle pozostawała białym kapeluszem.

Status quo sprzyjał Maksowi przestępcy - nie był chciwy i robił ożywione 184

interesy na Carders Market. Ale po upadku Shadowcrew cardingowy półświatek był rozbity i kiedy Max biały kapelusz widział, że coś się zepsuło, nie mógł

się powstrzymać przed naprawieniem tego, tak jak zrobił to dla Pentagonu kilka lat wcześniej.

Ambicja również odgrywała tutaj dużą rolę. Cały cardingowy półświatek zdawał się myśleć, że Iceman jest tylko kolejnym administratorem forum, po-zbawionym jakichkolwiek umiejętności poza uruchomieniem oprogramowania, na którym funkcjonowało strona. Max dostrzegł świetną okazję, by pokazać carderom, jak bardzo się mylą.

DarkMarket okazał się zupełnie niestrzeżonym miejscem. Brytyjski carder znany jako JiLsi, który prowadził stronę, popełnił błąd, używając do wszystkiego tego samego hasła „MSR206”, również na Carders Market, gdzie Max znał hasła każdego z członków. Max mógł po prostu wejść na DarkMarket i przejąć kontrolę. The Vouched natomiast było fortecą - nie mogłeś nawet wejść na stronę bez uzyskanego prywatnie cyfrowego certyfikatu zainstalowanego na twojej przeglądarce. Na szczęście JiLsi był także członkiem tego forum i posiadał przywileje moderatora. Max znalazł kopię certyfikatu w jednym z kont mailowych JiLsiego, zabezpieczonych znanym hasłem cardera. Kiedy już tam dotarł, wystarczyło tylko zalogować się jako JiLsi i wykorzystać jego dostęp, by dostać się do bazy danych.

Max stwierdził, że na TalkCash i ScandinavianCarding funkcja wyszukiwania w oprogramowaniu forum była podatna na atak „SQL injection”. Nie było to zaskakujące odkrycie. Podatność na SQL injection była najczęściej występu-jącą w sieci słabością.

SQL injection ma do czynienia z zakulisową architekturą większości za-awansowanych technicznie stron internetowych. Kiedy odwiedzasz stronę z dynamiczną zawartością - nowymi artykułami, postami na blogu, kursami akcji na giełdzie, wirtualnymi koszykami na zakupy - oprogramowanie strony wy-ciąga zawartość w surowej postaci z bazy danych back-endu, zazwyczaj znajdującej się na zupełnie innym komputerze niż host, z którym się połączyłeś.

Strona jest fasadą - liczy się serwer bazy danych, który jest zamknięty. W ide-alnej sytuacji nie będzie w ogóle dostępny przez Internet.

Oprogramowanie strony zwraca się do serwera bazy danych w standardowej syntaksie znanej jako Structured Query Language lub w skrócie SQL (wyma-wiane jak „sequel”). Na przykład komenda SQL-a „SELECT” prosi serwer bazy danych o wszystkie informacje, które spełniają określone kryteria. INSERT wkłada nowe informacje do bazy danych. Rzadko używana instrukcja DROP masowo kasuje dane.

Potencjalnie jest to ryzykowne rozwiązanie, istnieje bowiem wiele sytuacji, w których oprogramowanie musi wysłać to, co wprowadził użytkownik, jako część komendy SQL, na przykład w poszukiwaniu zapytania. Jeśli odwiedzają-

cy stronę muzyczną wpisze „Sinatra” w pasku wyszukiwania, strona poprosi bazę danych o wyszukanie pasujących odpowiedzi.

SELECT titles FROM music_catalog

WHERE artist = ‘Sinatra’;

Podatność na SQL injection pojawia się, kiedy oprogramowanie nie oczyści właściwie zapytania klienta przed włączeniem go do komendy bazy danych.

Interpunkcja jest śmiertelną pułapką. Jeśli użytkownik w powyższym przykładzie szuka pod „Sinatra’; DROP music_catalog;” jest niezwykle istotne, by apostrof i średniki nie przeszły. W przeciwnym razie serwer bazy danych widzi to:

SELECT * FROM itiusic_catalog

WHERE artist = ‘Sinatra’; DROP music_catalog;’;

Dla bazy danych są to dwie następujące po sobie komendy rozdzielone średnikiem. Pierwsza znajduje płyty Franka Sinatry, druga „wyrzuca”, czyli kasuje katalog z muzyką.

SQL injection jest standardową bronią w arsenale każdego hakera -dziury w zabezpieczeniach, nawet dziś, są plagą wszelkiego rodzaju stron, łącznie ze stronami sklepów internetowych i banków. W 2005 roku oprogramowanie forum używane przez TalkCash i Scandinavian-Carding było łatwym celem.

186

Aby wykorzystać robaka na TalkCash, Max zarejestrował się na nowym koncie i zamieścił pozornie niewinną wiadomość w jednym z wątków. Jego atak SQL był ukryty między wierszami, kolor czcionki był dopasowany do tła, tak żeby nikt tego nie zauważył.

Przeprowadził kwerendę mającą na celu znalezienie posta i zarobaczone oprogramowanie forum przekazało jego komendę INSERT do systemu bazy danych, który ją wykonał, tworząc nowe konto administratora tylko dla Maksa.

Podobny atak zadziałał na ScandinavianCarding.

14 sierpnia Max był gotowy pokazać członkom cardingowego półświatka, co potrafi. Wśliznął się na ich strony przez dziury, które w tajemnicy wybił w ich murach obronnych, używając swego nielegalnego dostępu admina, by skopiować ich bazy danych. Sun Tzu byłby dumny z planu Maksa: zaatakowanie i wchłonięcie konkurencyjnych forów istotnie było zaskakującym posunięciem.

Większość carderów pragnęła uniknąć uwagi, nie pchała się na świecznik.

Wrogie przejęcie było czymś bezprecedensowym.

Kiedy załatwił już sprawę anglojęzycznych stron, przeniósł się do Europy Wschodniej. Starał się zjednoczyć tamtejszych carderów z Zachodem, ale wy-siłki Tei były niemal zupełnie bezowocne. Rosjanie lubili ją, ale nie ufali amerykańskiej stronie. Dyplomacja zawiodła, nadszedł czas na działanie. Max stwierdził, że Cardingworld.cc i Mazafaka. cc nie są lepiej zabezpieczone niż zachodnie fora, i wkrótce ściągnął ich bazy danych, pełne prywatnych wiadomości i postów z forum. Megabajty cyrylicy zalały jego komputer, tajna historia oszustw i hakowania przeciw Zachodowi, sięgająca miesiące wstecz, teraz na stałe została zmagazynowana na twardym dysku Maksa w Tenderloin w centrum San Francisco.

Kiedy skończył, wprowadził komendę DROP w bazach danych na wszystkich stronach, kasując je. ScandinavianCarding, The Vouched, TalkCash, DarkMarket, Cardingworld - gwarne, całodobowe targowiska będące podporą światowej podziemnej gospodarki, wartej miliard dolarów, po prostu przestały istnieć. Tysiące przestępców na całym świecie, mężczyźni mający w planach 187

sześciocyfrowe transakcje, z żonami, dziećmi i kochankami na utrzymaniu, gliniarzami do przekupienia, ratami do zapłacenia, długami do zwrotu i zamó-

wieniami do zrealizowania - w jednej chwili stali się całkiem bezradni. Zagu-bieni. Stracili pieniądze.

Wszyscy oni poznają imię „Iceman”.

Max zabrał się do roboty nad danymi członków, odkładając carderów z Europy Wschodniej na inną okazję. Po odrzuceniu duplikatów i rzeczy, których nie chciał z anglojęzycznych stron, pozostało 4500 nowych członków Carders Market. Wciągnął ich wszystkich do bazy danych, by carderzy mogli używać swoich starych nicków i haseł do logowania na swojej nowej stronie. Carders Market miał teraz 6000 członków. Był większy niż Shadowcrew.

Ogłosił wymuszone połączenie forów w zbiorowym mailu do nowych członków. Kiedy w San Francisco zaczęło świtać, patrzył, jak się zbierają, zdezorientowani i wściekli, na jego skonsolidowanym forum przestępczym.

Matrix001, administrator niemieckiego DarkMarket, domagał się wyjaśnienia działań Icemana. Milczący dotąd król spamu, znany jako Master Splyntr, odezwał się, by skrytykować uporządkowanie materiału, który Iceman ukradł z innych forów. Cała zawartość konkurencyjnych stron znalazła się teraz w sek-cji Carders Market zwanej „archiwalne posty z dołączonych forów”. Nie były one posortowane i trudno się wśród nich nawigowało. Max uznał, że zawartość stron jest warta zachowania, ale nie uporządkowania.

Max przyglądał się tym narzekaniom przez chwilę, a potem wkroczył, by pokazać wszystkim, kto tutaj rządzi.

@Master Splyntr: jeśli nie masz nic konstruktywnego bądź szczególnego do powiedzenia, to twoje komentarze nie są mile widziane. Jeśli nie podoba ci się layout, to wyjdź i wróć później, bo nie zostało to jeszcze uporządkowane!

@matrix001: Stare fora nie dbały o swe bezpieczeństwo, używając współdzielonego hostingu, nie potrafiły szyfrować danych, ukrywać 188

adresów IP logujących, używano na nich „1234” jako haseł administracyjnych (ludzie, naprawdę tak było!) i zawiniły ogólnym administracyjnym faszyzmem. Niektóre, jak TheVouched, dawały nawet fałszywe poczucie bezpieczeństwa, co jak wiesz, jest o wiele gorsze niż żadne zabezpieczenie.

Pytasz, co „to wszystko” ma znaczyć. Jeśli masz na myśli to, dlaczego połączyliśmy razem pięć cardingowych forów, prosta odpowiedź

brzmi: ponieważ nie mam ani czasu, ani ochoty na dołączenie dodat-kowych czterech, by razem mieć dziewięć.

Przede wszystkim było tego za dużo. Po co mieć pięć różnych fo-rów, z których każde ma taką samą zawartość, rozdzielać użytkowników i sprzedawców i mieszać słabe zabezpieczenia z kiepskim admini-strowaniem i moderowaniem? Nie chcę powiedzieć, że tak było w każ-

dym wypadku, ale niestety w większości tak.

Przy właściwym moderowaniu CM powróci do wcześniejszej ścisłej zasady zero tolerancji dla rippingu i niemal anarchistycznej polityki nie-zamykania wątków i promowania dyskusji. Jak na razie są tu jeszcze

„śmieci” z wcześniejszych forów, ale zostaną usunięte.

Co to daje? Bezpieczeństwo. Wygodę. Podniesienie jakości i zmniejszenie hałasu. Porządek…

Kanadyjski haker zwany Silo protestował przeciw temu, że Iceman zerwał

towarzyskie więzy, które łączyły społeczność carderów. Zniszczył ich zaufanie.

Zburzyłeś bezpieczeństwo naszej społeczności. Kradniesz bazy danych z innych forów. Czy twoja fuzja nie mogła mieć miejsca w porozumieniu z adminami innych forów i za ich zgodą? Jaka jest różnica między 189

znakowaniem maili a czytaniem o twoich sprawach i posłowaniem twojej korespondencji na moim forum?

Z którejkolwiek strony byś na to spojrzał, nadużyłeś zaufania, które istnieje we wspólnocie. Moja sugestia jest taka, byś skasował bazy danych, które teraz masz. Nie są twoje, więc nie masz prawa ich udostępniać. Właściwą rzeczą byłoby ZAPYTANIE adminów tych forów, czy rzeczywiście jedno połączone forum leży w interesie użytkowników, a potem należałoby poczekać i zobaczyć, czy byliby zainteresowani takim forum.

To moje trzy grosze.

Iceman, są tutaj ludzie posiadający wiele umiejętności. To, w jaki sposób ich używają, definiuje naszą społeczność.

The Vouched powróciło do sieci, ale nie na długo. Miało być prywatnym, bezpiecznym forum otwartym tylko dla nielicznych wybrańców. Max złamał

zabezpieczenia, zniszczył jego wiarygodność i nikt nie fatygował się, by tam powrócić. TalkCash i ScandinavianCarding były przegrane - nie miały kopii zapasowych baz danych, które Max skasował. Ich członkowie w większości pozostali na Carders Market.

Poza rosyjskimi forami, z którymi Max miał problem ze względu na barierę językową, było tylko jeszcze jedno miejsce, które dzieliło go od pełnego trium-fu: DarkMarket. Jego główny konkurent miał kopie zapasowe i udało mu się powrócić do życia w ciągu kilku dni. To był policzek wymierzony Maksowi za wszystko, co starał się osiągnąć dla siebie i społeczności. Zaczęła się wojna.

Tymczasem w Orange County Chris również starał się skonsolidować swoją część biznesu. Postanowił, że będzie wygodnie, jeśli wszyscy jego pełnoetato-wi pracownicy zamieszkają pod wspólnym adresem, a sieć kompleksów mieszkaniowych Archstone oferowała możliwość załatwienia wszystkich for-malności przez Internet, co idealnie odpowiadało jego planom. Przyszli lokato-rzy mogli wypełnić umowę wynajmu na firmowej stronie i wpłacić nieduży depozyt w wysokości 99 dolarów i czynsz za pierwszy miesiąc, używając 190

karty kredytowej. Chris mógł przeprowadzić wszystko przez Internet, więc ludzie nie musieli się pojawiać aż do dnia, kiedy się będą wprowadzać, i zatrzymają się w biurze wynajmu, by machnąć swymi podrabianym dowodami i wziąć klucze. Aragon ściągnął dwie ze swych dziewczyn oraz Mareosa, gościa, który dostarczał mu trawkę, do

Archstone Mission Viejo, labiryntu mieszkań w stylu McMansion pomalowanych w kolorach zachodzącego słońca i przyklejo-nych do wzgórza pokrytego palmami i liniami wysokiego napięcia obok autostrady międzystanowej numer 5, biegnącej dziesięć minut od jego domu. Starał

się również powiększyć swą załogę. Jedna z dziewczyn zrezygnowała po swej drugiej wpadce w sklepie i przeniosła się do Toledo, a dwie inne odeszły znie-smaczone, kiedy Chris zrobił dziecko swojej nastoletniej kochance - teraz opłacał jej mieszkanie, trzymając istnienie syna w tajemnicy nawet przed swoją matką.

W biurze NCFTA w Pittsburghu Keith Mularski, jako Master Splyntr, dwa dni po wrogim przejęciu dostał prywatną wiadomość od samego Icemana. Haker chciał przeprosić za swe ostre słowa na forum.

Przewidując kolejny etap konfliktu DarkMarket - Carders Market, Iceman przechwalał się, że odeprze każdy atak DDoS przeciw niemu. Ale poza wszystkim zgooglował Master Splyntra i dowiedział się, że jest on światowej klasy spamerem dysponującym armią botnetów. Iceman najwyraźniej nie chciał, by człowiek, który raz go skrytykował, zmienił się w jego zaciekłego wroga.

Nie obrażaj się na moje sarkastyczne komentarze. To prawda, że jeśli ktoś mnie zaatakuje, wytropię bot-nety i spróbuję przejąć lub zamknąć, ale nie jest to coś, czym chciałbym drażnić ludzi. Nikt nie potrzebuje tracić czasu na takie działania, naprawdę DDoS nie jest zabawny, więc nie wyrabiaj sobie błędnego wyobrażenia o mnie.:-)

191

Mularski zaczynał dostrzegać okazję w tym wrzeniu ogarniającym półświatek. Nikt już nie wiedział, komu można zaufać; wszyscy byli na siebie źli.

Gdyby grał na dwie strony, mógłby rozpocząć akcję przeciw administratorom forum, kiedy starali się zdobyć sprzymierzeńców w zbliżającej się bitwie.

Miał pozwolenie na trzy bezpośrednie kontakty. Postanowił, że jeden z nich wykorzysta, aby odpowiedzieć Icemanowi.

Spoko, bracie, jest OK. Da sam też jestem cwaniaczkiem. Nie interesu-je mnie atakowanie. Kurde, moje boty nie są nawet skonfigurowane do ataku. Na spamowaniu zarabiam o wiele więcej! Naprawdę olewam wszystko, co nie przynosi mi kasy, chyba że muszę się na kimś ze-mścić, ale teraz nikogo takiego nie ma. Jeśli zostaniesz zaatakowany, ja także jestem dobry w śledzeniu i przejmowaniu, więc odezwij się do mnie na ICQ 340572667, jeśli będziesz potrzebował pomocy…:-) MS

Mularski wpatrywał się w ekran, czekając. Po kilku minutach przyszła odpowiedź.

Świetnie, dzięki:-) Przy okazji, czy masz jakieś sugestie co do prowadzenia forum, oprócz oczywiście bałaganu w organizacji? Chciałbym także to zmienić, a ty jesteś sprzedawcą i masz tytuł użytkownika. (Zrobione) Nie wiem, czy sprzedajesz usługi mailingowe przez swoją sieć, ale to jest fajna rzecz, która się przydaje, i jestem pewien, że bylibyśmy lepsi, mając możliwość zatrudnienia ciebie. Więc jeśli byłeś wcześniej sprzedawcą (lub kimś innym?), wtedy proszę przyjmij moje przeprosiny za utratę tytułu. Przechowałem pewne statusy, takie jak sprzedawcy DM, ale wymieszały się na innych forach i pogubiły. Po

prostu, żebyś wiedział. Dzięki, bracie:-) Dodałem cię także do grupy VIP-ów.

192

To była obiecująca odpowiedź. Mularski przegadał sprawę ze swym przeło-

żonym, potem zwrócił się do głównej siedziby o uprawnienie II grupy, niższy z dwóch stopni tajnego zaangażowania dostępnych w FBI, ale chociaż krok dalej od poprzedniego uprawnienia „tylko do biernej obserwacji". Ta nowo uzyskana swoboda nie pozwoli mu na branie udziału w działalności przestępczej, lecz w końcu będzie mógł aktywnie zaangażować się w życie półświatka. Uznał Carders Market i każdego, kto był związany z prowadzeniem tej strony, za przedmiot śledztwa.

Zgoda nadeszła szybko. Mimo zachęcających słów Iceman okazał się wy-mykającym się celem - trzymał Mularskiego na dystans, nie ufał mu i rozmawiał tylko przez wewnętrzny system komunikacyjny Carders Market. Agent FBI miał więcej szczęścia po drugiej stronie pola bitwy. Był jednym z pierwszych członków DarkMarket, a teraz, jako że łatwo nawiązywał kontakty, zało-

życiel strony JiLsi szybko dostrzegł w Master Splyntrze materiał na zarządzającego. Na początku września Splyntr został moderatorem strony.

Wojna się rozkręcała. Mimo nauczki, jaką był sierpniowy najazd, JiLsi nie mógł poradzić sobie z dokładnym zabezpieczeniem DarkMarket. Iceman zaczął

regularnie wkradać się i kasować przypadkowe konta, tylko po to by poigrać sobie z JiLsim. Kiedy DarkMarket odpowiedział ostrym atakiem DDoS przeciw irańskiemu hostowi Carders Market, Iceman odpalił swój DDoS przeciw DarkMarket. Obie strony ugięły się pod ciężarem pakietów śmieci. Iceman po cichu zamówił usługę w amerykańskiej firmie hostingowej z odpowiednią szerokością pasma do zaabsorbowania pakietów DDoS, czyszcząc ruch przed skanalizowaniem go z powrotem na prawdziwy serwer przez zaszyfrowany VPN.

JiLsi rwał włosy z głowy, wylewając swe żale Master Splyntrowi. Mularski odwrócił uwagę od Icemana, kierując ją na brytyjskiego cyberprzestępczego 193

bossa, który zaczynał go traktować jak przyjaciela. Niezobowiązująco zasugerował, by JiLsi rozważył przekazanie DarkMarket komuś doświadczonemu w organizowaniu odpornego na ataki hostingu. Komuś przyzwyczajonemu do prowadzenia stron, których wszyscy nienawidzą. Spamerowi.

Hej, znasz moją historię, napisał na czacie. Jestem naprawdę dobry w usta-wianiu serwerów, zabezpieczam je cały czas. Mógłbym to dla ciebie zrobić.

Mularskiemu wpadł do głowy niezwykły pomysł. W przeszłości zarówno Secret Service, jak i FBI używały adminów jako informatorów: Albert Gonzalez na Shadowcrew i Dave Thomas na The Grifters. Ale obecnie prowadzenie przestępczego forum otworzyłoby dostęp do wszystkiego: od adresów IP

carderów po ich prywatną korespondencję, równocześnie dając Master Splyntrowi jako prowadzącemu stronę wiarygodność, o jakiej żadnemu agentowi nawet się nie śniło.

JiLsi wyraził zainteresowanie ofertą Master Splyntra i Mularski wyruszył w kolejną

podróż do Waszyngtonu.

ROZDZIAŁ 26

Co masz w portfelu?

Sprzedaż 100% pewnych amerykańskich ZRZUTÓW •NOWOŚĆ* Ob-niżka cen na zrzuty:

MasterCard 11$

Visa Classic 8$

Visa Gold/Premiuml3$

Visa Platinum 19$

Visa Signature 24$

Visa Business 24$

Visa Corporate 19$

Visa Purchasing 24$

American Express = nowa obniżka 19 $ (było 24)

Discover = nowa obniżka 24$ (było 29)

Minimalne zamówienie: 10 sztuk.

Zrzuty sprzedawane według rodzaju karty. Brak listy

numerów identyfikacji bankowej.

Celem wrogiego przejęcia, którego dokonał Max, było poprawienie funkcjonowania społeczności, a nie osobista korzyść, ale po połączeniu forów 195

jego interesy na skradzionych danych z pasków magnetycznych szły lepiej niż kiedykolwiek. Zarabiał 1000 dolarów dziennie, sprzedając teraz zrzuty carderom z całego świata, a dodatkowo wyciągał jeszcze 5000-10 000 na miesiąc ze swej spółki z Chrisem.

Publicznie na zebraniach FTC i w innych miejscach branża kart kredytowych starała się, jak mogła, ukryć znaczący wzrost kradzieży danych z pasków magnetycznych na całym świecie. Wiodąca firma Visa stawiała za wzór finansowany przez branżę raport Javelin Strategy and Research, który stwierdzał, że przedmiotem przeważającej większości kradzieży tożsamości i oszustw na kartach kredytowych byli indywidualni klienci, nie firmy: liczba ta wynosiła jakieś 63 procent i dotyczyła przede wszystkim skradzionych lub zgubionych portfeli, następnie kradzieży dokonanych przez zaufanych znajomych, skradzionych listów i rachunków wyciągniętych z kosza na śmieci.

Raport był bardzo mylący - mówił wyłącznie o wypadkach, w których ofiary wiedziały, w jaki sposób ich dane zostały skradzione. Prywatne obliczenia Visy pokazywały prawdę. Skradzione portfele nie były głównym źródłem oszustw od połowy 2001 roku, kiedy gwałtownie wzrosła liczba kradzieży kart kredytowych ze stron sklepów internetowych wysyłających oszukańcze transakcje „card not present” - zakupy online i przez telefon - podczas gdy wszystkie inne kategorie pozostawały niezmienne.

W 2004 roku, kiedy skradzione dane z pasków magnetycznych stały się po-

żądanym towarem, straty z powodu fałszowania kart osiągnęły astronomiczną wielkość. W pierwszym kwartale 2006 roku podrabianie kart w stylu Chrisa Aragona po raz pierwszy przewyższyło oszustwa „card-not-present”, powodując 125 milionów dolarów kwartalnych strat tylko wśród banków wydających karty Visy.

Przyczyną niemal wszystkich tych strat były listy cen, takie jak ta Maksa.

Jako Digits strona po stronie gromadził pozytywne recenzje na Carders Market za dobre prowadzenie interesów, zyskał bardzo dobrą reputację. Było to powodem do dumy i przejawem podwójnej moralności, którą przejawiał od 196

dzieciństwa. Max beztrosko hakował cardera, kopiując całą zawartość jego twardego dysku, ale wystarczyło, że klient płacił mu za informacje, a on nawet nie brał pod uwagę tego, że może go oszukać.

Dobrze znana była także jego szczodrość. Kiedy Max miał zrzuty, których data ważności się kończyła, raczej oddawał je za darmo, niż pozwolił, by się zmarnowały. Wzorowe praktyki biznesowe i jakość jego produktów uczyniły Maksa jednym z pięciu najlepszych na świecie sprzedawców zrzutów, na rynku tradycyjnie zdominowanym przez carderów z Europy Wschodniej.

Max był ostrożny w dokonywaniu transakcji. Nie sprzedawał zrzutów we-dług numerów identyfikacji bankowej (BIN), co sprawiało, że federalni mieli trudności z wykryciem jego włamań: władze nie mogły po prostu kupić dwudziestu zrzutów pochodzących z jednej instytucji finansowej i poprosić banku, by uważał na często pojawiające się punkty sprzedaży w zapisach ich transakcji. Zestaw dwudziestu kart kupionych od Maksa mógł należeć do dwudziestu różnych banków. Aby znaleźć źródło, wszystkie musiałyby z sobą współpracować.

Na dodatek tylko kilku zaufanych znajomych wiedziało, że Digits i Iceman to ta sama osoba - głównie admini: Chris, kanadyjski carder NightFox i świeżo zwerbowany Th3C0rrupted0ne.

Ze wszystkich, których spotkał w półświatku, Th3C0rrupted0ne wydawał

się tym, z którym Max jako haker miał najwięcej wspólnego. Będąc nastolatkiem, C0rrupted odkrył świat warez na osiągalnych przez połączenie telefoniczne bulletin board systemach, potem zajął się hakowaniem dla rozrywki pod niekarni Acid Angel, -null- i innymi. Rozwalał strony internetowe dla zabawy i dołączył do gangu hakerów zwanego Ethical Hackers Against Pedophiles

[Etyczni Hakerzy przeciw Pedofilom]. Była to obywatelska straż szarych kapeluszy zwalczająca dziecięcą pornografię w Internecie.

I tak jak Max - kiedyś uważał siebie za dobrego faceta, zanim stał się Th3C0rrupted0ne.

Cała reszta wyglądała jednak zupełnie inaczej. C0rrupted - produkt trudnego dzieciństwa w wielkomiejskim osiedlu - został dilerem narkotyków w młodym wieku i po raz pierwszy trafił za kratki (za posiadanie broni) w 1996 roku, kiedy miał 18 lat. Na studiach

zaczął fałszować dokumenty tożsamości dla przyjaciół i jego internetowe poszukiwania zaprowadziły go do Fakeid.net, sieciowego bulletin boardu, gdzie zaczynali eksperci tacy jak ncXVI.

C0rrupted awansował na fałszerza czeków i kart kredytowych, mniej więcej kiedy upadła Shadowcrew, a potem trafił na powstałe później fora.

Dyplomatyczny i zrównoważony, był powszechnie lubiany w półświatku i cieszył się przywilejami moderatora lub admina na większości forów. Max uczynił go adminem na Carders Market latem 2005 roku, powierzając mu rolę nieoficjalnego rzecznika po wrogim przejęciu. Jakiś tydzień po swej demon-stracji siły Max ujawnił C0rruptedowi swoją podwójną tożsamość.

Oczywiście jestem także Digitsem. Mógłbym równie dobrze powiedzieć o tym wprost, odkąd zdjąłem maskę na ICQ (mówiąc o „naszym forum” etc.)

Utrzymywanie tego w tajemnicy przed ludźmi, których znam i którym ufam tak jak tobie, jest upierdliwe. Więc teraz wiesz…

W każdym razie uzasadnienie jest takie: Iceman działa legalnie, Digits łamie prawo. Zakładam, że gdybym utrzymał tożsamość tych dwóch w tajemnicy, nie byłoby żadnej prawnej możliwości, by mnie do-paść jako admina forum.

Największym zagrożeniem dla bezpieczeństwa Maksa pozostawał Chris. Za każdym razem kiedy się kłócili, przypominał Maksowi, jak bardzo jest wobec niego bezbronny, ponieważ to on był jedynym carderem, który zna jego prawdziwą tożsamość. „Nie mogę uwierzyć, jak wiele o mnie wiesz” - warczał Max zły na siebie.

198

Tymczasem Chris próbował przekonać Maksa do zrobienia jednego wielkiego skoku, czegoś, co pozwoliłoby im porzucić przestępczy proceder na dobre i być może pomogło Chrisowi otworzyć legalny biznes w Orange County.

Stworzył plan, który każdy z nich krok po kroku powinien realizować, i nazwał

go „Whiz List”.

Max miał przeniknąć do sieci bankowych, by mieć możliwość przelewania milionów dolarów na konta wskazane przez Chrisa. Max ze swej strony robił

to, co powinien, od samego początku ich spółki. Kiedy jeszcze pracował z ga-rażu Chrisa, włamywał się do małych banków i kas oszczędnościowo-pożyczkowych. Teraz miał większy dostęp do nich i mógł przelewać pieniądze z kont klientów, kiedy tylko chciał. Ale powodzenie planu zależało od Chrisa -

musiał znaleźć bezpieczne miejsce na pieniądze, które miał ukraść Max, dziuplę, z której okradziony bank nie mógłby ich już odzyskać. Jak do tej pory nie udało mu się tego zrobić.

Dlatego też kiedy we wrześniu Max znalazł dziurę zero-day w nowym Internet Explorerze, podzielił się wieścią nie z Chrisem, ale z innym wspólnikiem, który miał lepszą orientację w międzynarodowych finansach - z adminem Carders Market zwanym NightFox.

Dziura w zabezpieczeniach była gigantyczna: kolejne przeładowanie bufora, tym razem w kodzie Internet Explorera zaprojektowanym, by pozwolić stronom internetowym na rysowanie wektorowych grafik na ekranie odwiedzają-

cego. Max ze smutkiem stwierdził, że wschodnioeuropejscy hakerzy pierwsi odkryli robaka i robili z niego użytek. Firma zajmująca się bezpieczeństwem komputerowym już znalazła rosyjski exploit zakażający odwiedzających strony pornograficzne i wysłała go do Microsoftu. Departament Bezpieczeństwa Krajowego wysłał otwarte ostrzeżenie do użytkowników Internet Explorera: „Nie klikajcie na niesprawdzone linki".

Wieści się rozeszły, ale nie było jeszcze łatki. Każdy użytkownik Internet Explorera był narażony na atak. Max dostał kopię rosyjskiego exploitu wcze-

śnie rano 26 września i entuzjastycznie doniósł o tym NightFoksowi.

199

„Załóżmy, że dostaliśmy dziś darmowe hasło, pozwalające nam mieć każdą firmę, której chcemy - napisał Max, korzystając z systemu komunikacyjnego Carders Market. - Tu masz wszystko. Żadnych ograniczeń. Visa.com. Master-card.com. egold.com. Skądkolwiek możesz uzyskać adresy mailowe pracowników. Google. Microsoft. Nieważne. W tym momencie wszystko możesz mieć".

Microsoft wysłał łatkę jeszcze tego samego dnia, ale Max wiedział, że nawet firmom, które bardzo dbają o bezpieczeństwo, przetestowanie i zainstalo-wanie aktualizacji zabierze całe dni, a nawet tygodnie. Rosyjski exploit był już wykrywalny przez oprogramowanie antywirusowe, więc Max zmodyfikował

go, zmieniając sygnaturę, i przepuścił przez antywirusa, by upewnić się, że nie uda się go wykryć.

Pozostała tylko inżynieria społeczna: Max musiał zwabić swoje cele do odwiedzenia strony, na której znajdował się exploit. Zdecydował się na domenę o nazwie Financialedgenews.com, wybierając hosting na Value Web.

NightFox powrócił z listą celów: CitiMortage, GMAC, Experian's Lowe-rmybills.com, Bank of America, Western Union MoneyGram, Lending Tree i Capital One Financial, jedna z największych w kraju instytucji oferujących karty kredytowe. NightFox posiadał obszerną bazę danych wewnętrznych adresów mailowych różnych korporacji, którą uzyskał z firmy zajmującej się „analizą konkurencyjności". Dostarczył Maksowi tysiące adresów, obejmujących wszystkie cele.

29 września Max odpalił swoje oprogramowanie spamujące i wysłał sper-sonalizowane maile do swych ofiar. Podpisał je nazwiskiem „Gordon Reily" z adresem zwrotnym g.reily@lendingnewsgroup.com.

Jestem reporterem Lending News pracującym nad artykułem o ostatnim wycieku danych klientów z Capital One. Zobaczyłem nazwisko Mary Rheingold w artykule z Financial Edge i chciałbym przeprowadzić z Pa-nią wywiad na potrzeby mojego artykułu.

200

http://financialedgenews.com/news/09/29/Disclosure_CapitalOne Jeśli może Pani

poświęcić chwilę czasu, byłbym bardzo wdzięczny za możliwość podyskutowania na temat szczegółów tego artykułu.

Każda kopia wiadomości została dostosowana tak, by każdy pracownik czy pracownica myśleli, że on lub ona zostali wymienieni z nazwiska w wymyślonym artykule z Financial Edge. Pięćset osób z Capital One, od zarządzających po rzeczników PR i pracowników IT, dostało tę wiadomość. Około 125 z nich kliknęło na zatruty link i zostało odesłanych do strony o typowym wyglądzie wiadomości z branży finansowej. Kiedy błądzili po stronie, ukryty ładunek prześliznął się przez firmowy firewall do ich komputerów.

Oprogramowanie otworzyło tylne drzwi, które pozwoliły Maksowi wślizgiwać się w wolnym czasie i sprawdzać twarde dyski ofiar w poszukiwaniu wrażliwych danych, węszyć w wewnętrznych sieciach banków, kraść hasła.

Nie różniło się to zbytnio od tego, co zrobił z tysiącami komputerów w Departamencie Obrony wieki temu. Wtedy gdy to wszystko było tylko zabawą.

ROZDZIAŁ 27

Pierwsza wojna sieciowa

Keith Mularski stał na podium, z tyłu za nim znajdował się wielki ekran LCD, na którym wyświetlała się właśnie jego prezentacja w PowerPoincie. Przed nim piętnastu wyższych rangą urzędników z FBI i Departamentu Sprawiedliwości oraz prawników siedziało wokół konferencyjnego stołu w głównej siedzibie Departamentu. Byli bardzo skupieni. Mularski proponował coś, czego jeszcze nikt wcześniej nie zrobił.

Przyznanie komuś upoważnienia grupy I „do działania w szczególnych okolicznościach" było w biurze czymś niezwykle rzadkim. Mularski najpierw napisał dwudziestostronicowy wniosek, uwzględniający każdy szczegół planu i gromadzący opinie prawne ekspertów z FBI. Rada Generalna FBI była zachwycona możliwościami - jeśli ten wniosek zostanie zaakceptowany, operacja może stworzyć precedens dla przyszłej tajnej pracy online. Największą przeszkodę dla Justice Department's Undercover Review Committee (Komitetu Inspekcji Tajnych Operacji Departamentu Sprawiedliwości) stanowił problem odpowiedzialności cywilnej za pozwolenie, by przestępstwa były popełniane za pośrednictwem strony będącej w posiadaniu i zarządzanej przez rząd USA.

W jaki sposób Mularski zredukuje szkody tak, by niewinni ludzie i instytucje nie ucierpiały? Keith miał już gotową odpowiedź. Działalność przestępcza na DarkMarket będzie się odbywać niezależnie od tego, czy FBI prowadzi forum czy nie. Ale jeśli biuro będzie kontrolować serwer, a Master Splyntr kierować stroną, to FBI potencjalnie mogłoby przechwycić dużą ilość skradzionych danych, które w przeciwnym razie przepływały swobodnie przez czarny rynek. W

jego wniosku było zastrzeżenie, że wszelkie finansowe dane zostaną niezwłocznie wysłane do poszkodowanych banków. Skradzione karty kredytowe będą mogły zostać anulowane, zanim ktoś ich użyje.

Zebranie trwało dwadzieścia minut. Kiedy wrócił do Pittsburgha 7 paź-

dziernika, Mularski miał pisemne pozwolenie na przejęcie DarkMarket. Iceman nadal figurował na liście celów tajnej operacji, ale teraz i inni liderzy DarkMarket stali się głównymi obiektami śledztwa.

Kiedy już jego żona poszła spać, Mularski usadowił się na tapczanie, włą-

czył „Saturday Night Live" i zaczął szukać JiLsiego na ICQ. Po kilku grzecznościach przeszedł do interesów. DarkMarket znowu przeżywał atak DDoS i Mularski, jako Master Splyntr, był gotów przenieść stronę na bezpieczny serwer - wystarczyło, że JiLsi powie tylko słowo, i jego problemy z Icemanem przejdą do historii.

JiLsi miał pewne obiekcje. DarkMarket był jego dzieckiem i nie chciał, by społeczność odebrała to jako oddanie kontroli. Nie ma problemu, odpowiedział

Mularski. Master Splyntr będzie ukrytym administratorem. Nikt oprócz niego i JiLsiego nie będzie wiedział, że to on prowadzi stronę. Dla innych wciąż pozostanie tylko moderatorem.

„Bracie - odpisał JiLsi. - Przygotuj swój serwer. Przenosimy się”.

Mularski od razu zabrał się do pracy. Wynajął serwer od teksańskiej firmy hostingowej Planet i zajął się wzmacnianiem fundamentów, kupując za 500

dolarów na miesiąc usługę zabezpieczenia przed DDoS od Rosjanina znanego jako Quazatron. Zapłacił za to przez e-gold. Quazatron skonfigurował stronę tak, by jej publiczna część znajdowała się na Staminusie, odpornej na DDoS i dysponującej szerokim pasmem firmie hostingowej. Przewody tej firmy 203

mogły przetrwać potop, a oprogramowanie Quazatrona przepuszczało tylko legalny ruch na prawdziwy serwer DarkMarket za kulisami.

Wszystko będzie zrobione w stylu wschodnioeuropejskich cyberoszustów.

Kiedy Mularski chciał zalogować się na zaplecze strony, szedł przez KIRĘ, firmę z Wirginii oferującą „shell accounts” Linuksa - usługę która pozwala użytkownikom IRC-a łączyć się z czat roomami, uniemożliwiając wyśledzenie ich domowych adresów IR Nikt nie zobaczy, że polski król spamu logował się z Pittsburgha.

Kiedy ten etap był zakończony, Mularski poszedł do sądu i uzyskał utajnio-ny nakaz rewizji własnego serwera pozwalający mu na przeglądanie bazy danych użytkowników DarkMarket, odwiedzanych przez nich stron i prywatnych wiadomości.

Została jeszcze jedna rzecz do zrobienia. Po Shadowcrew wymogiem dla forów carderów było sprawienie, by użytkownicy klikali na umowę zawierają-

cą warunki korzystania z usługi, zakazującą zamieszczania nielegalnej zawartości i zastrzegającą, że prowadzący stronę nie odpowiadają za nic, co jest na niej publikowane. Prowadzący forum wierzyli, że prawniczy żargon może uchronić ich przed postępowaniem sądowym. DarkMarket miał bardzo szczegółową umowę użytkowania, więc nikt nie zauważył, kiedy Master Splyntr dodał linijkę.

„Korzystając z tego forum, wyrażasz zgodę, by administratorzy mogli oceniać każdą wiadomość wysłaną przez to forum, by zapewnić zgodność z regu-laminem”. Mularski dopisał: „lub dla jakichkolwiek innych celów”.

„Sadzę, że warto zauważyć, iż ten cały Iceman jest głupim, początkującym hakerem, który krąży i hakuje strony dla zabawy i przyjemności”. El Mariachi znał czuły punkt Icemana. Po wrogim przejęciu Dave Thomas powrócił na blog

„Life on the Road”, aby bezlitośnie kopać swego wroga, nazywając go „Icebo-yem”, „Officerem Ice’em” i „pieprzonym kawałkiem gówna na moim bucie”.

204

Wzywał Icemana, by spotkali się osobiście i rozstrzygnęli spór po męsku. Sugerował też, że może wynająć płatnego mordercę, by wyśledził króla cardingu i skończył z nim.

Max zareagował z furią. Nie zapomniał zamieszania i kosztów znalezienia nowego hosta po tym, jak Thomas doprowadził do zamknięcia strony na Florydzie. Agresja, którą głęboko w sobie dusił od czasów Boise, zawrzała w nim.

„Ty mały zwiędły kutasie, jesteś marnym worem gówna. Mógłbym cię, kurwa, zmiażdżyć gołymi rękami, ale TCHÓRZLIWY kabel, jak ty, na sam mój widok wezwałby gliny i

sięgnął po broń - napisał. - Lepiej módl się, żebym nigdy nie został ujawniony, bo wtedy nie tylko wyglądałbyś na większego osła niż teraz, ale nic by mnie nie powstrzymywało przed wyjściem i złamaniem twego karku, konfidencki śmieciu".

Kiedy ochłonął, wysłał Thomasowi prywatnego maila. Myślał o zwinięciu Carders Market i wysłaniu Icemana na emeryturę. Nie byłoby to poddanie się, ale raczej największe zagrożenie dla kampanii Thomasa, jakie można sobie wyobrazić.

Nie czytałeś *Sztuki wojny*, nie, szmato?

Nie wiesz o mnie NIC. Da wiem o tobie WSZYSTKO.

Zniszczę CM, zniszczę Icemana, ale gdzie ty wtedy będziesz, ścier-wo? Walka z cieniem? Jesteś UDUPIONY. Masz wroga, który będzie cię gnoił przez lata, a ty nie będziesz miał możliwości OBRONY, ŻADNEGO CELU, by mu odpłacić.

Jestem twoim najgorszym koszmarem, ty mała dziwko, i ty, i twoja rodzina przez długi, długi czas będziecie słono płacić za straty, które przez ciebie poniosłem.

Dwa dni później Max pokazał, że nie żartował. Włamał się na stronę El Mariachiego, The Grifters, zmienioną przez Thomasa w półlegalną stronę poświę-

coną bezpieczeństwu i obserwowaniu forów cardingowych. Max skasował

zawartość twardego dysku. Strona zniknęła na zawsze.

Iceman ogłosił swe zwycięstwo ostateczne w publicznym oświadczeniu na blogu. „Nie muszę niczego udowadniać i teraz, kiedy załatwiłem Davida Rens-hawa Thomasa, federalnego kabla, wychodzę - napisał. - W przeciwieństwie do was, ludzie, pilnuję własnego interesu. Miejcie nauczkę. Ruszcie się i zostaw-cie mnie, kurwa, w spokoju".

Ale Max nie był już zdolny do usunięcia się z powrotem w cień. Dwóch reporterów z „USA Today" zauważyło publiczną wojnę carderów i potwierdziło szczegóły wrogiego przejęcia w firmie zajmującej się bezpieczeństwem, która monitorowała fora. Nazajutrz po tym jak Max ogłosił zwycięstwo nad El Mariachim, czwartkowe wydanie gazety trafiło pod więcej niż milion drzwi w całym kraju. Na pierwszej stronie dodatku biznesowego opisano całą historię aneksji forów cardingowych przez Icemana.

Pozwalając, by ambicja doprowadziła go do publicznej bitwy z Davidem Thomasem, Max sprawił, że o istnieniu Icemana dowiedzieli się czytelnicy największej pod względem nakładu amerykańskiej gazety.

„Secret Service i FBI odmówiły komentarzy na temat Icemana lub przejęć -

napisano w artykule. - Mimo to działalność tej tajemniczej postaci pokazuje rosnące zagrożenie bezlitosną ekspansją cyberprzestępczości w dużej części możliwej dzięki istnieniu forów".

Artykuł nie był zaskoczeniem. Reporterzy zwrócili się do Icemana o komentarz, a Max wysłał długiego maila, forsując swoją obronę w stylu Craigslist. Jego poglądy nie znalazły się w artykule, co nadało wizerunkowi hakera jeszcze bardziej wyzywającego charakteru. Max umieścił cytat z artykułu na stronie logowania Carders Market: „Stworzył coś w rodzaju nielegalnego WalMartu". Max pokazał gazetę Charity. „Wygląda na to, że

narobiłem niezłe-go zamieszania”.

Chris dostał apopleksji, kiedy dowiedział się, że Max korespondował z dziennikarzami. Widział już, jak jego wspólnik marnuje całe godziny, użerając 206

się z Thomasem. A teraz udzielał wywiadów prasie?

- Kurwa, straciłeś rozum - powiedział.

Max był zawalony robotą. Prośby o poręczenie napływały do Carders Market szerokim strumieniem. Zdawało się że artykuł w „USA Today” dał każdemu dresiarzowi nadzieję na stanie się oszustem komputerowym. Strona przyjęła ponad trzystu nowych członków z dnia na dzień. Dwa tygodnie później wciąż ich przybywało.

Przerzucił tyle pracy, ile mógł, na adminów. Miał teraz inne zmartwienia.

Jego harpunniczy atak przeciw instytucjom finansowym zakończył się sporym sukcesem, ale samo przeniknięcie przez bankowe firewalle okazało się najłatwiejszą rzeczą w całym przedsięwzięciu. Banki, szczególnie Bank of America i Capital One, były wielkimi instytucjami i Max zgubił się w ich gigantycznych sieciach. Mógł spędzić całe lata wyłącznie na szukaniu danych i dostępu, któ-

rego potrzebował, by zrobić wielki skok. Miał problem z motywacją do ogłu-piającej pracy, którą musiał wykonać po włamaniach - łamanie zabezpieczeń i wchodzenie do sieci było częścią, która go bawiła, a teraz to się skończyło.

Odłożył banki na bok, by skupić się na wojnie cardingowej. Jego nowy dostawca hostingu otrzymywał skargi z powodu galopującej przestępczości na Carders Market. Max widział jeden z maili wysłanych z anonimowego konta.

Na chybił trafił Max spróbował zalogować się na stronę, używając hasła JiLsiego. Udało się. To JiLsi próbował doprowadzić do zamknięcia jego forum.

Max odpowiedział, hakując konto JiLsiego na rosyjskim forum Mazafaka i wysyłając lawinę wiadomości, w których pisał po prostu: „Jestem federalnym”.

Potem ujawnił dowody występku JiLsiego; kablowanie firmie hostującej Carders Market było nieczystym zagraniem. DarkMarket po prostu nie miał na tyle przyzwoitości, by zniknąć. Max mógł ponownie wykasować bazę danych przeciwnika, ale to nie przyniosłoby nic dobrego - wcześniej przecież strona 207

powróciła. Jego ataki DDoS również stały się nieskuteczne. Z dnia na dzień DarkMarket przeszedł do drogiego, szerokopasmowego hostingu i miał wy-dzielone serwery poczty mailowej i bazy danych. Nagle stał się trudnym celem.

Potem Max usłyszał intrygującą plotkę na temat DarkMarket.

W historię zamieszany był Silo, kanadyjski haker znany z niesamowitej zdolności do żonglowania dziesiątkami fałszywych nicków, bez wysiłku zmieniający styl pisania i osobowość. Drugim powodem do sławy Sila było jego kompulsywne hakowanie innych carderów. Nieustannie zamieszczał oprogramowanie z ukrytym kodem, który pozwalał mu szpiegować swych kolegów.

Kierowany obydwoma tymi impulsami Silo założył nowe konto na DarkMarket pod nowym nickiem i poddał kawałek hakerskiego oprogramowania ocenie sprzedawcy. Jak

zwykle umieścił w oprogramowaniu ukrytą funkcję, która szmuglowała pliki użytkownika na jeden z jego serwerów.

Kiedy Silo przyjrzał się rezultatom, znalazł mały schowek z pustymi sza-blonami Microsoft Word, wśród których był formularz „raportu na temat zło-

śliwego oprogramowania". Na szablonach widniało logo organizacji National Cyber Forensics and Training Alliance z Pittsburgha. Max sprawdził ją; to była firma federalnych. Ktoś związany z DarkMarket pracował dla władz. Zdeterminowany do przeprowadzenia śledztwa Max ponownie włamał się na DarkMarket przez tylne drzwi. Tym razem była to misja zwiadowcza. Wszedł w root shell i wprowadził komendę, by przywołać całą historię poprzednich logowań, a potem otworzył listę w drugim oknie, sprawdzając zapisy publicznych rejestracji dla każdego z adresów IP używanych przez administratorów.

Kiedy dotarł do Master Splyntra, zatrzymał się. Ten podający się za Polaka spamer łączył się z adresu IP należącego do prywatnej firmy w USA, Pembrooke Associates.

Wyciągnął zapisy rejestracji Whois.net dla strony tej firmy - Pembetal.com.

Adres pocztowy, który się tam znajdował, był skrzynką pocztową w Warrenda-le w Pensylwanii, 32 kilometry na północ od Pittsburgha. Był tam również numer telefonu.

Kolejne kliknięcie myszką i następne okno przeglądarki - odwrócone białe strony na Anywho.com. Wstukał numer telefonu i tym razem dostał adres prawdziwej ulicy: 2000 Technology Drive, Pittsburgh, Pensylwania.

To był adres, który już znalazł na National Cyber Forensics and Training Alliance. Master Splyntr był federalnym.

ROZDZIAŁ 28

Cardingowy sąd

Keith Mularski był udupiony.

Najpierw dostał informacje od agenta w terenowym biurze Secret Service w mieście. „Myślę, że możesz mieć poważne kłopoty". Jeden z agentów usłyszał, że Iceman odkrył niezbity dowód, iż Master Splyntr jest albo kapusiem, szpie-giem z firmy zajmującej się bezpieczeństwem komputerowym, albo agentem federalnym. Iceman zawarł tymczasowy sojusz ze swym niegdysiejszym wro-giem Silem i przygotował przejrzystą prezentację dla przywódców Carders Market i DarkMarket. Iceman i Silo mieli zamiar wytoczyć Master Splyntrowi proces.

Wszystko zaczęło się od kodu Sila. Reputacja Master Splyntra jako spamera i programisty uczyniła z niego faceta, do którego na DarkMarket szło się po ocenę złośliwego oprogramowania. Był to jeden z bonusów jego tajnej operacji: Mularski rzucał okiem na kod ostatnich ataków z półświatka, a potem mógł

to przesłać do CERT-u, który z kolei przekazywał go firmom antywirusowym.

Złośliwy kod był wykrywalny, nawet zanim trafił na czarny rynek.

Tym razem Mularski dał kod jako ćwiczenie dla jednego ze studentów CMU odbywającego staż w NCFTA. Jako standardową procedurę ów student 210

uruchomił program w izolacji na wirtualnej maszynie - czymś w rodzaju softwareo'wej szalki Petriego, z której później może zostać usunięty. Zapomniał

jednak, że miał pendrive'a w porcie USB. Ten pendrive był wypełniony czy-stymi formularzami raportów na temat złośliwego oprogramowania, na których znajdowało się logo NCFTA i misja firmy. Zanim stażysta zorientował się, co się dzieje, dokumenty były już w rękach Sila.

Sześciu adminów i moderatorów DarkMarket dostało kopię kodu Sila i teraz Kanadyjczyk wiedział, że jeden z nich jest federalnym.

Silo miał dziką kartę. W prawdziwym życiu nazywał się Lloyd Liske i był

menedżerem w salonie samochodowym w Vancouver i fałszerzem kart kredytowych, którego złapano kilka miesięcy po operacji „Firewall". Kiedy został

skazany na 18 miesięcy aresztu domowego, Liske zmienił swe nazwisko z Buckell i swój nick z Canucka, by ponownie pojawić się w cardingowym pół-

świątku.

Teraz Kanadyjczyk był nietykalny. W policji wszyscy wiedzieli, że Silo był

informatorem glin z Vancouver. Właśnie dlatego ciągle hakował innych carderów: trojan, który zinfiltrował NCFTA, nie miał na celu ujawnienia operacji prowadzonej przez stróżów prawa. To tylko Silo próbował zdobyć dla policji informacje o członkach DarkMarket.

Silo nie był zobowiązany do lojalności wobec FBI, ale prawdopodobnie chciał zdemaskować tajnego agenta biura. Tak się nieszczęśliwie złożyło, że Iceman dowiedział się o tym odkryciu i zrobił rekonesans na DarkMarket.

Właśnie tu Mularski przerżnął sprawę. Jak zwykle zalogował się na DarkMarket przez KIRE shell, ukrywając swoją lokację. Ale JiLsi był wymagającym szefem, nieustannie bombardującym Master Splyntra zadaniami związanymi z utrzymaniem strony - jak wymiana banerów reklamowych - i po prostu musiało to być zrobione natychmiast. Czasem, kiedy Mularski dostawał jedno z tych poleceń, KIRE nie działało, więc szedł na skróty i logował się bezpośrednio.

Iceman go dopadł.

Mimo to był względnie bezpieczny. Usługa połączenia z Internetem była zarejestrowana pod nazwą fikcyjnej firmy z numerem telefonu - dzwonił na 211

linię VoIP w centrum komunikacyjnym, która nie odbierała połączeń. Linia telefoniczna miała być ukryta. Jednak nie wiedzieć czemu, nie była. Dzięki temu Iceman zdobył adres i rozpoznał go jako NCFTA.

Mularski wszedł w pośpiechu do centrum komunikacyjnego, przeciągnął

swą kartę dostępu, wstukał kod do drzwi i zamknął się od środka. Wybrał bezpieczną linię do Waszyngtonu. Agent FBI nie upiększał swego raportu. Po tym jak włożył tyle wysiłku

w zdobycie autorytetu w półświatku i przejęcie DarkMarket, otrzymaniu zielonego światła od wierchuszki Departamentu Sprawiedliwości i wysokich urzędników biura, Iceman miał zamiar zdmuchnąć go zaledwie trzy tygodnie od rozpoczęcia operacji.

Max walczył z przygotowaniem *expose* po swych atakach na DarkMarket.

Wiedział, że jego odkrycie będzie postrzegane jako partyzancka akcja. Rozwa-

żał skasowanie Carders Market przed ujawnieniem Master Splyntra, aby uniknąć wrażenia, że cała sprawa jest tylko kolejną bitwą w cardingowej wojnie.

Zamiast tego postanowił wysłać swego nowego porucznika, Th3C0rrupted0ne, aby reprezentował ich stronę.

Proces odbywał się za pośrednictwem należącego do Sila „Carder IM" -

darmowego, prawdopodobnie szyfrowanego komunikatora, zarabiającego na wyświetlaniu reklam sprzedawców zrzutów, który kanadyjski haker zaoferował

jako alternatywę do AIM i ICQ. Ze strony DarkMarket pojawił się Matrix001 -

JiLsi był zajęty usuwaniem skutków ataku Maksa na Mazafaka. Silo i dwaj inni kanadyjscy carderzy również byli obecni. Silo otworzył spotkanie, wręczając wszystkim skompresowane pliki RAR zawierające dowody zebrane przez niego i Icemana.

Kiedy część carderów rozpakowała pliki, ich programy antywirusowe za-częły wariować. Silo wprowadził swój kod do dowodów. Niezbyt obiecujący początek spotkania.

Corrupted i Silo zapoznali pozostałych ze sprawą: szablony dokumentów Sila pokazywały, że ktoś z NCFTA zajmował uprzywilejowaną pozycję na 212

DarkMarket, a zapisy logowań, które wykradł Iceman, wskazywały, że to Master Splyntr jest kablem.

„Stuprocentowy dowód nie do obalenia - napisał C0rrupted. - Pracowaliśmy ciężko, aby to sprawdzić i uspokoić sytuację, i jeśli to upublicznimy, to psy OSTRO się za nas wezmą. Ale jeśli będziemy milczeć, będziemy odpowie-dzialni za tych wszystkich, którzy zostali wyruchani".

„To prawda, koleś" - stwierdzi Silo.

Matrix nie był przekonany. Prowadził własne „Kto jest Kto" na domenie Pembrooke Associates i wrócił z anonimową listą Domains by Proxy: żadnej ulicy, numeru telefonu. „Ble, ble, ble - wystukał Matrix. - Nie sprawdziłeś nawet informacji, kto to jest w firmie, nie? Kto dał ci te rzeczy?"

„To nie moje rzeczy - napisał Silo - tylko Icemana".

„Wierzysz w każde gówno, które ci ktoś podsunie? Nawet bez sprawdzania tego?"

Dowody Sila nie były już dla Matriksa przekonujące: formularze NCFTA zawierały błędy ortograficzne i błędy formatowania - czy FBI lub organizacja non profit zajmująca się bezpieczeństwem naprawdę odwaliła tak partacką robotę? Co więcej, pogarda Icemana wobec DarkMarket była dobrze znana, a Silo był stałym upierdliwcem na forum.

Temperatura dyskusji się podniosła. C0rrupted odpadł, a inni milczeli, gdy Silo i Matrix

zaczęli obrzucać się błotem. „Dlaczego niby miałbym ci wierzyć?” - pytał Matrix.

„Nie wierz - powiedział w końcu Silo. - Nie wierz mi. Spierdalaj z mojego komunikatora… i daj się złapać”.

Mularski został wykluczony z zebrania, ale gdy się skończyło, Matrix wy-słał Master Splyntrowi sprawozdanie. Agent ucieszył się, widząc, że jego oczyszczenie w ostatniej chwili przyniosło rezultaty: gdy tylko dowiedział się, że Iceman planuje go ujawnić, skontaktował się z rejestratorem domeny i poprosił firmę, by usunęła z Pembrooke Associates zapis z nazwiskiem i numerem telefonu. Potem poprosił Anywho o zabranie listy z zastrzeżonymi liniami telefonicznymi. Przykrywka umocniła tylko Icemana w przekonaniu, że Master 213

Splyntr jest federalnym, ale nikt inny nie był w stanie niezależnie zweryfikować jego odkryć.

Teraz Mularski rozpoczął swoją kampanię przez ICQ. Powiedział Matrik-sowi i wszystkim innym, którzy słuchali, że jest niewinny. Skierował uwagę carderów na zapisy logowań, podkreślając wszystkie wypadki, kiedy logował

się z adresu IP na KIRĘ. To są moje wejścia, napisał, nie wiem, do kogo należą pozostałe.

Następnie zrobił zwrot i zaatakował. Wątpliwości, które Iceman rozsiewał

na temat JiLsiego, zadziałały na korzyść Mularskiego. Wszystko zaczęło wariować, napisał. JiLsi zachowywał się podejrzanie. Instruował Master Splyntra, by nie mówił nikomu, że prowadzi serwer. A kiedy JiLsi utrzymywał wrażenie, że DarkMarket jest hostowany w kraju leżącym poza zasięgiem zachodniego wymiaru sprawiedliwości, naprawdę był hostowany w Tampa na Florydzie, gdzie federalni mogli wchodzić kiedy, chcieli, i użyć nakazu rewizji. To rzeczywiście było dziwne zachowanie.

JiLsi krzyczał, że jest niewinny, ale wyglądało to dla niego niedobrze. Master Splyntr publicznie podziękował Icemanowi za zwrócenie uwagi na problem i zapowiedział, że od razu przenosi DarkMarket poza granice USA.

Mularski sięgnął po kontakty w milicji na Ukrainie, a ta szybko pomogła mu znaleźć tam hosting. W mgnieniu oka DarkMarket znalazł się w Europie Wschodniej. Większość carderów musiała przyznać, że żaden federalny nie przenosiłby strony-pułapki do kraju z byłego Związku Radzieckiego.

Ostateczny werdykt nie został wydany, ale powstał konsensus co do tego, że Master Splyntr jest niewinny. Carderzy nie mieli już takiej pewności w stosun-ku do JiLsiego.

Kiedy spór został zażegnany, Mularski powrócił do rutynowej pracy prowadzenia swej tajnej operacji. Kilka tygodni później siedział za biurkiem, pisząc raporty, kiedy zadzwonił do niego inny agent.

214

Agent specjalny Michael Schuler był legendą wśród agentów FBI zajmują-

cych się cyberprzestępczością. To właśnie on włamał się do komputerów Rosjan w Invicie. Teraz stacjonował w biurze terenowym w Richmond, w Wirginii. Schuler dzwonił w sprawie włamania w pobliżu Capital One. Pracownicy zajmujący się bezpieczeństwem

banku wykryli atak z użyciem exploitu do Internet Explorera. Wysłali Schulerowi kopię tego kodu, a on chciał, żeby Mularski ściągnął jednego z geeków z NCFTA, by ten rzucił na to okiem.

Mularski słuchał, jak Schuler opisuje śledztwo, aż do tego momentu. Skupił

się na fałszywej stronie serwisu Financialedgenews.com, z której dokonywano ataków przy użyciu złośliwego oprogramowania. Domena była zarejestrowana na fałszywą tożsamość w Georgii. Ale kiedy rejestrator Go Daddy sprawdził jej zapisy, znalazł tego samego użytkownika, który kiedyś zarejestrował w firmie inny adres.

Cardersmarket.com.

Mularski od razu pojął znaczenie tego faktu. Iceman ustawił siebie jako niewinnego prowadzącego stronę, na której - tak się złożyło - dyskutowano o nielegalnych transakcjach. Teraz Schuler miał dowód, że Iceman był także działającym dla zysku hakerem, który włamał się do sieci piątego największego wydawcy kart kredytowych w Ameryce. „Chłopie, masz sprawę! - powiedział Mularski ze śmiechem. - Masz *teraz* śledztwo przeciw gościowi, którego próbowaliśmy trafić w naszej grupie II. Musimy nad tym pracować razem".

W innej części miasta agenci Secret Service z terenowego biura w Pittsburghu dokonali własnego odkrycia na temat Icemana: informator podpowiedział

im, że szef Carders Market ma także drugą tożsamość jako sprzedawca zrzutów

- Digits. Cztery dni po artykule w „USA Today" agenci wykorzystali tę wiedzę, używając drugiego konfidenta, który dokonał kontrolowanego zakupu od Digitsa: 23 zrzuty za 480 dolarów przez e-gold.

To było więcej, niż potrzeba, by postawić mu zarzuty.

ROZDZIAŁ 29

Jedna platyna i sześć klasyków

Keith Mularski nie wiedział, w co się pakuje, kiedy przejął DarkMarket.

Każdy jego dzień był teraz szalony. Zaczynał o ósmej rano, logując się na swym tajnym komputerze w biurze i sprawdzając na ICQ wiadomości, które przyszły w nocy: czy było coś pilnego do Master Splyntra. Potem wchodził na DarkMarket, by upewnić się, czy forum działa. Nigdy nie mógł mieć pewności, dopóki Iceman był na wolności.

Następnie przychodziła kolej na uciążliwe robienie kopii zapasowych bazy danych SQL. Iceman jakimś sposobem dwukrotnie skasował tabele od czasu nieudanej próby ujawnienia Mularskiego, więc teraz kopie zapasowe należały do porannej rutyny agenta. Służyły także śledztwu - podczas gdy bazy danych były kopiowane, prosty skrypt stworzony przez kodera NCFTA skanował każ-

dą linijkę w poszukiwaniu szesnastocyfrowych numerów rozpoczynających się cyframi od 3 do 6. Skradzione numery kart kredytowych były automatycznie sortowane według BIN-ów i wysyłane do właściwych banków, gdzie natychmiast je anulowano.

Potem Mularski musiał przejrzeć wszystkie prywatne wiadomości, podjąć interesujące rozmowy i sprawdzić je w ELSUR, centralnej bazie danych 216

elektronicznego nadzoru FBI. Następnie przez godzinę lub dwie pisał raporty.

Jako Master Splyntr Mularski rozpoczął własną skromną operację wyciągania gotówki. Pewne banki zgodziły się wydać mu jednorazowe zrzuty jako przynę-

tę, z fałszywymi nazwiskami, ale prawdziwymi liniami kredytowymi, które FBI miało pokryć z budżetu swego śledztwa. Master Splyntr sprzedawał je wraz z PIN-ami carderom z całego kraju, podczas gdy instytucje finansowe zgłaszały codziennie miejsca i daty wypłat z bankomatów. Kiedy ludzie z jego forum płacili fałszywymi kartami, Mularski przekazywał informacje miejscowym agentom, za każdym razem spisując szczegółowy raport.

O trzeciej, kiedy carderzy tłumnie pojawiali się w sieci, drugie życie Mularskiego przyspieszało. Każdy czegoś chciał od Master Splyntra.

Były spory do rozsądzenia, na przykład kiedy sprzedawca zrzutów skarżył

się, że jego reklama nie została równie dobrze wyeksponowana jak konkurenta, lub kupujący oskarżał kogoś o oszustwo. Do Master Splyntra zwracali się też żebracy, prosząc o darmowe zrzuty lub usługi spamerskie.

Agent wracał pod koniec dnia do domu tylko po to, by znowu zalogować się na forum. Utrzymywanie wiarygodności jako Master Splyntr oznaczało, że musi pracować w tych samych godzinach co prawdziwy carder, więc co noc Mularski siadał w domu na sofie, włączał telewizor, nie patrząc na to, jaki program jest nadawany, i odpalał laptopa podłączonego do sieci. Był na DarkMarket, AIM i ICQ, odpowiadając na pytania, podpisując recenzje, przyjmując sprzedawców i banując ripperów. Prawie codziennie pozostawał w sieci jako Master Splyntr do drugiej nad ranem, zajmując się półświatkiem.

Aby wkraść się w łaski głównych podejrzanych, dawał im prezenty lub sprzedawał ze zniżką towary, które miały zostać zakupione przy użyciu kradzionych kart kredytowych, a w rzeczywistości płaciło za nie biuro. Cha0, turecki boss przestępców i admin DarkMarket, pragnął bardzo lekkiego peceta za 800 dolarów sprzedawanego w Stanach, więc Mularski wysłał mu dwa takie na adres dziupli Cha0 w Turcji. Udawanie Świętego Mikołaja należało teraz do jego obowiązków: musiał się pojawiać, by prowadzić operacje i zarabiać 217

pieniądze, i z całą pewnością nie miał zamiaru nikogo spamować.

Odkrywał że bycie bossem cyberprzestępczości jest ciężką pracą.

Kiedy podróżował lub był na urlopie, musiał o tym wcześniej dawać znać.

Na forum nawet krótka nieusprawiedliwiona nieobecność mogłaby wzbudzić podejrzenia, że został złapany i odwrócony. W styczniu 2007 roku wysłał na forum informację, że przez chwilę będzie w samolocie. Nie powiedział gdzie ani dlaczego. Leciał do Niemiec porozmawiać ze śledczymi o jednym ze współzałożycieli DarkMarket – Matriksie001.

Oprócz innych funkcji, które pełnił, Matrix001 był prawdziwym artystą DarkMarket. Tworzył i sprzedawał szablony z Photoshopa używane przez fał-

szerzy do produkcji kart kredytowych lub podrabianych dokumentów tożsamo-

ści. Miał wszystkie: Visa, MasterCard, American Express, Discover, amerykańskie karty

ubezpieczenia społecznego, pieczęcie notarialne i prawa jazdy dla kilku stanów. Swoje szablony amerykańskich paszportów sprzedawał po 45

dolarów. Karta Visa Bank One kosztowała 125 dolarów.

Matrix001 i Master Splyntr zaprzyjaźnili się z sobą od czasu próby ujawnienia tego ostatniego trzy miesiące wcześniej: Mularski i Niemiec lubili gry wideo i rozmawiali o ostatnich tytułach do późnej nocy. Dyskutowali także o interesach i Matrix001 wyznał, że otrzymał przelewy za swe transakcje w Eislingen w południowych Niemczech. To była pierwsza wskazówka, by go wytropić.

Od tej chwili była to kwestia śledzenia pieniędzy. Jak niemal wszyscy carderzy Matrix chciał, by płacono mu przez e-gold, system elektronicznych płat-ności stworzony przez byłego onkologa z Florydy Douglasa Jacksona w 1996

roku. Konkurent PayPala, e-gold, był pierwszą wirtualną walutą, która miała zabezpieczenie w prawdziwych sztabkach złota i srebra przechowywanych w bankowych sejfach w Londonie i Dubaju.

Marzeniem Jacksona było stworzenie prawdziwie międzynarodowego systemu monetarnego, niezależnego od żadnego rządu. Przestępcy to pokochali.

W przeciwieństwie do prawdziwego banku, e-gold nie stosował żadnych środków, by zweryfikować tożsamość swych użytkowników - wśród posiadaczy kont byli „Myszka Miki” i „Bezimienny.” Aby wpłacić lub wybrać pieniądze z e-gold, użytkownicy korzystali z któregoś z setek niezależnych biur wymiany e-gold na całym świecie, firm, które przyjmowały przelewy bankowe, anonimowe polecenia zapłaty lub nawet gotówkę do ręki i zmieniały to na e-gold, potrącając procent dla siebie. Firmy dostawały kolejną działkę, kiedy użytkownicy chcieli wymienić swe pieniądze w drugą stronę - za wirtualne dostać miejscową walutę, otrzymując ją przez Western Union, PayPal bądź przelew internetowy. Jedna z firm oferowała nawet przedpłaconą kartę bankomatową „G-Card”, która pozwalała właścicielowi konta wybierać e-gold z dowolnego bankomatu.

Wszystko wskazywało na to, że przestępcy są powszechnymi klientami egold. Do grudnia 2005 roku wewnętrzne śledztwo firmy zidentyfikowało ponad 3000 kont zaangażowanych w carding i kolejne 3000 używanych do sprzedaży i kupna dziecięcej pornografii, a 13 000 kont było związanych z różnego rodzaju oszukańczymi inwestycjami. Łatwo było je zauważyć: w polu „memo” w wypadku zakupu dziecięcej pornografii znajdowało się na przykład słowo

„Lolita”; w oszustwie Ponziego „HYIP” - akronim od „high-yield investment program” (inwestycje o wysokiej stopie zwrotu). Carderzy dołączali skrótowe opisy zakupionego towaru: „Za 3 IDs”; „za zrzuty”; „10 klasyków”; „zrzuty Famea”; „10 M/C”; „jedna platyna i sześć klasyków”; „20 vklasyków”; „18

nus”; „10 AZIDs”; „4 vklasyki”; „za cw2s”; „za 150 klasyków”.

Przez długi czas e-gold w większości wypadków przymykał oko na przestępczy proceder. Pracownicy zamknęli trochę kont handlarzy dziecięcą pornografią, ale nie powstrzymali ich przed wybraniem pieniędzy. Postawa firmy zmieniła się jednak radykalnie w grudniu

2005 roku, kiedy agenci FBI i Secret Service wydali nakaz rewizji biura e-gold w Melbourne na Florydzie i oskarży-li Jacksona o prowadzenie nielicencjonowanego transferowania pieniędzy.

219

Wtedy były onkolog zaczął dobrowolnie przeglądać swą bazę danych, szukając śladów przestępstw, i wysyłał wskazówki jedynej agencji, która chciała wsadzić go do więzienia - US Postal Inspection Service. Jego świeże podpo-rządkowanie się prawu i porządkowi było dobrodziejstwem dla Mularskiego.

Przez Grega Crabba i jego ekipę w urzędzie pocztowym Mularski poprosił

Jacksona o informacje na temat konta e-gold Matriksa001, które zostało zało-

żone na alias „Ling Ching". Kiedy Jackson zajrzał do bazy danych, okazało się, że konto początkowo zostało założone pod innym nazwiskiem: Markus Kellerer, z adresem w Eislingen. W listopadzie Mularski wysłał formalną prośbę o pomoc do niemieckiej policji przez amerykański konsulat we Frankfurcie. Policja potwierdziła, że Kellerer jest prawdziwą osobą, a nie tylko kolejnym aliasem, a Mularski zarezerwował lot do Stuttgartu.

Matrix001 był pierwszym z aresztowanych, którzy wpadli w pułapkę DarkMarket. Mularski musiał znaleźć kogoś innego do rozmów o grach wideo.

Kiedy już wrócił do Pittsburgha, zaczął opracowywać nową, wyszukaną teorię na temat Icemana. Sprawdzał każdego „Icemana", którego mógł znaleźć; był

jeden na Shadowcrew i inni na IRC-u. Za każdym razem okazywało się, że to strata czasu. Teraz Mularski zabawiał się nowym pomysłem, że Iceman naprawdę nie istnieje.

Domniemana współpraca Icemana z kanadyjskim informatorem Lloydem

„Silem" Liske mocno go zaintrygowała. Silo pracował z Icemanem, próbując ujawnić Mularskiego. To, samo w sobie, wiele nie znaczyło - informatorzy często prowokowali podejrzanych o bycie gliniarzami i kapusiami, by odsunąć podejrzenia od siebie. Ale Silo powiedział swemu opiekunowi w policji w Vancouver, że znakował komputer Icemana, ale kiedy go przyciśnięto, nie potrafił podać ani prawdziwego nazwiska Icemana, ani nawet dobrego adresu IP. Okazało się też, że Silo ma dziesiątki kont na e-gold, w tym jedno na nazwisko „Keyser Söze".

220

Jeśli Liske był fanem *Podejrzanych*, mogło mu wpaść do głowy stworzenie fantomowego superprzestępcy, a następnie jako informator karmił policje fał-

szywymi informacjami o domniemanym bossie.

Mularski poleciał do Waszyngtonu i przedstawił swą teorię Secret Service w jej głównej kwaterze. Koncepcja od razu został obalona. Agencja współpracowała ściśle z oficerem prowadzącym Sila z policji w Vancouver i znała informatora jako jednego z tych dobrych.

Secret Service również przejrzała kilka fałszywych tropów. W laboratorium w terenowym biurze w Pittsburghu agenci mieli tablicę pokrytą nickami i odpowiadającymi im nazwiskami, połączone łukami i liniami. Wiele nazwisk się krzyżowało. To był ich

nieustannie zmieniający się przewodnik po Icemanie i jego świecie.

Mularski wrócił do Pittsburgha i obie agencje wznowiły poszukiwania prawdziwego Keysera Söze cyberświata, nieuchwytnego króla hakerów - Icemana.

ROZDZIAŁ 30

Maksik

Max wiedział, co się święci. Z agentami FBI u steru DarkMarket będzie pułap-ką, w którą wpadnie wielu carderów, lądując w więzieniu. Niczym Kasandra z greckiej mitologii był skazany na poznanie przyszłości, ale nikt mu nie wierzył.

Między artykułem w „USA Today" a nieudaną próbą ujawnienia Master Splyntra Max wyczuwał, że wokół niego robi się gorąco. W listopadzie ogłosił, że Iceman przechodzi na emeryturę, i odstawił szopkę z przekazaniem władzy nad stroną Th3C0rrupted0ne. Wyłączył się do czasu, aż sprawy się uspokoją, i trzy tygodnie później powrócił na pokład z innym nickiem. Iceman umarł -

niech żyje Aphex.

Max był zmęczony ciasnym mieszkaniem w Post Street Towers, więc Chris sprowadził Nancy, jedną ze swych dziewczyn, do San Francisco, by wynajęła dla Maksa lokal z jedną sypialnią w kompleksie mieszkaniowym w strzelistym apartamentowcu Archstone Fox Plaza w dzielnicy finansowej. Występowała jako przedstawiciel handlowy z Capital Solutions, firmowej fasady, której Aragon używał do prania części swoich dochodów. Tea, po powrocie z Mongolii, została zwerbowana do siedzenia w tym mieszkaniu i odebrania dostarczonego 222

tam łóżka, za które zapłaciła własną legalną kartą American Express. Chris później zwrócił jej koszty.

W styczniu 2007 roku Max powrócił do interesu ze swojej nowej kryjówki, gęsto otulonej WiFi. Fox Plaza był wielkim krokiem, jeśli chodzi o luksus, w porównaniu z Post Street Towers, ale Maksa było na to stać. Mógł zarobić na czynsz w ciągu kilku dni dobrej sprzedaży zrzutów. Jako Digits był teraz uznawany przez niektórych carderów za drugiego najlepszego na świecie sprzedawcę danych z pasków magnetycznych.

Na pierwszym miejscu mocno trzymał się Ukrainiec znany jako Maksik.

Działał on poza forami cardingowymi, prowadząc własny sklep z kradzionymi kartami na stronie internetowej Maksik.cc. Kupujący zaczynali od wysłania Maksikowi zapłaty z góry przez e-gold, WebMoney, przelew internetowy lub Western Union. To dawało im dostęp do strony, gdzie mogli wybierać zrzuty, jakie chcieli, ułożone według BIN-ów i typów kart, oraz złożyć zamówienie.

Maksikowi pozostawało tylko kliknięcie, by zaakceptować transakcję, i klient dostawał maila ze zrzutami, które zamówił, prosto z wielkiej bazy danych Maksika.

Towar Ukraińca był wyśmienity, z dużym odsetkiem sukcesów przy kasie i gigantycznym wyborem BIN-ów. Podobnie jak w wypadku Maksa, karty Maksika pochodziły z transakcji w terminalach płatniczych. Jednak zamiast obierać za cel małe sklepy i restauracje, Maksik kradł karty z mniejszej liczby dużych sklepów: Polo Ralph Lauren w 2004, Office Max w 2005. W ciągu trzech miesięcy Discount Shoe Warehouse stracił 1,4 miliona kart zabranych ze 108 sklepów w 25 stanach - trafiły prosto do bazy danych Maksika. W lipcu 2005 roku został pobity rekord: 45,6 miliona zrzutów zostało

skradzionych z będących własnością TJX sieci sprzedaży detalicznej T.J. Maxx, Marshalls i HomeGo-ods.

Był czas, kiedy takie włamania mogły pozostać tajemnicą hakerów, firm i federalnej policji, a ofiary wśród klientów pozostawały w cieniu. Aby zachęcić firmy do zgłaszania włamań, niektórzy agenci FBI utrzymywali nazwy firm w 223

tajemnicy przed oskarżycielami i dziennikarzami, chroniąc je przed złą reklamą ich marnych zabezpieczeń. W 1997 roku, kiedy w sprawie Carlosa Salgado juniora - pierwszej kradzieży kart kredytowych online na wielką skalę - władze przekonały sędziego wydającego wyrok, aby na stałe utajnił zapisy sądowe, obawiając się że firmy, które padły ofiarą, ucierpiałyby z powodu „strat w interesach w wyniku wywołania wrażenia, że ich systemy komputerowe są podatne na ataki". W konsekwencji 80 000 ofiar nigdy nie dowiedziało się, że ich nazwiska, adresy i numery kart kredytowych zostały wystawione na sprzedaż na IRC-u.

W 2003 roku stan Kalifornia skutecznie zakończył z tego rodzaju tajemni-cami, kiedy legislatura powołała do życia SB1386, pierwsze w kraju prawo ujawniania notorycznych włamań. Prawo wymagało, by znakowane organiza-cje prowadzące interesy w Złotym Stanie natychmiast ostrzegały ofiary włamania o możliwej kradzieży ich tożsamości. W następnych latach 45 innych stanów wprowadziło podobne regulacje prawne. Obecnie żadna znacząca kradzież danych klientów nie pozostaje na długo tajemnicą, kiedy już zostanie wykryta przez firmy i banki. Nagłówki mówiące o włamaniach do sieci handlu detalicznego na niespotykaną dotąd skalę tylko dodały blasku produktom Maksika - nie starał się on wcale tego ukryć, sprzedawał zrzuty z sieci detalicznych.

Kiedy wiadomości o ataku na TJX pojawiły się w mediach w styczniu 2007

roku, szczegóły, które wypłynęły, również potwierdziły to, czego wielu carderów już się domyślało: Ukrainiec miał amerykańskiego hakera dostarczającego mu zrzutów. Maksik był pośrednikiem dla tajemniczego hakera w Stanach.

W połowie 2006 roku haker najwidoczniej był w Miami, gdzie zatrzymał

się przed dwoma należącymi do TJX outletami Marshalls i złamał szyfr WiFi sklepów. Stamtąd przeskoczył do lokalnej sieci i popłynął w górę do głównej siedziby korporacji, gdzie odpalił sniffer, by przechwycić na żywo transakcje kartami kredytowymi Marshalls, T.J. Maxx i sklepów Home-Goods w całym kraju. Ten sniffer, jak później wykazało śledztwo, działał niezauważony przez siedem miesięcy.

Max miał w Ameryce konkurenta, i to cholernie dobrego.

224

W dużej części dzięki hakerowi Maksika i Maksowi Visionowi powszechne przekonanie konsumentów, że transakcje internetowe są mniej bezpieczne niż zakupy w realnym życiu, okazało się teraz całkiem fałszywe. W 2007 roku większość przechwyconych kart została skradziona ze sklepów i restauracji.

Łupem wielkich włamań do sieci detalicznych padały wówczas miliony kart, ale ataki na mniejszych sprzedawców były znacznie bardziej powszechne -

badania Visy wykazały, że 83 procent kradzieży kart kredytowych miało miejsce w

placówkach pobierających płatności milionem lub mniejszą liczbą kart Visa rocznie, a większość z nich dokonywano w restauracjach.

Aby zmylić śledczych, Max starał się utrzymywać źródło swoich zrzutów w tajemnicy, twierdząc na swym forum niezgodnie z prawdą, że dane pochodzą z centrów przetwarzania kart kredytowych. Ale Visa wiedziała, że jednym z głównych celów były terminale płatnicze. W listopadzie 2006 roku firma wy-dała biuletyn dla branży gastronomicznej, w którym ostrzegano przed atakami hakerów przeprowadzanymi przez VNC i inne rodzaje oprogramowania do zdalnego dostępu do komputera. Mimo to Maksowi nadal nie brakowało podatnych na ataki lokali gastronomicznych.

Przestało mu to jednak wystarczać. Nie po to zaczął zajmować się kradzieżą danych, żeby być numerem dwa w tym biznesie. Maksik odbierał mu pienią-

dze. Nawet Chris kupował od obydwu: Maksika i Maksa, wybierając tego, który zaoferował mu dobrą cenę za najlepsze zrzuty.

Na prośbę Maksa Tea w ciągu kilku miesięcy zaprzyjaźniła się z Ukraińcem i nakłaniała go do sprzedawania na Carders Market. Maksik grzecznie odmówił

i zasugerował, by odwiedziła go kiedyś na Ukrainie. Odrzucony Max porzucił

dyplomatyczne metody i kazał Tei wysłać Maksikowi trojana, w nadziei że przejmie bazę danych ze zrzutami Ukraińca. Maksik wyśmiał tę próbę znakowania go.

Gdyby Max wiedział, mógłby pocieszać się tym, że nie był jedynym, które-go frustrowało świetne zabezpieczenie Maksika.

Służby federalne tropiły Maksika, odkąd zaczął cieszyć się złą sławą u za-rania operacji „Firewall”. Tajny agent Secret Service kupował od niego zrzuty.

225

Inspektor Greg Crabb współpracował z policją w Europie, by złapać carderów, którzy robili interesy z Maksikiem, i dzielił się zdobytymi informacjami z milicją ukraińską. Na początku 2006 roku Ukraińcy w końcu zidentyfikowali Maksika jako Maksyma Jastremskiego z Charkowa. Nie mieli jednak wystarczają-

cych dowodów, by go aresztować.

Amerykanie skoncentrowali się na zidentyfikowaniu hakerskiego źródła Maksika. E-gold raz jeszcze dostarczył klucza. Secret Service przeanalizowała konta Maksika w bazie danych tej firmy i stwierdziła, że między lutym a ma-jem 2006 roku Maksik przelał 410 750 dolarów ze swego konta do „Segveca”, sprzedawcy zrzutów z Mazafaka, powszechnie uważanego za człowieka z Europy Wschodniej. Zewnętrzny przelew wskazywał, że Segvec nie jest jednym z klientów Maksika, lecz dostawcą otrzymującym swoją działkę.

Federalni dostali szansę na bardziej bezpośrednie informacje w czerwcu 2006 roku, kiedy Maksik był na wakacjach w Dubaju. Agenci Secret Service z San Diego współpracowali z miejscową policją, by wśliznąć się do jego pokoju, gdzie potajemnie skopiowali twardy dysk Ukraińca do analizy. Ale to był

ślepy zaułek. Wrażliwy materiał na dysku został całkowicie zaszyfrowany przy użyciu

programu Pretty Good Privacy. Zabezpieczenie było na tyle dobre, że Secret Service nie mogła ruszyć dalej.

Carderzy tacy jak Maksik i Max mieli przewagę dzięki zastosowaniu jednego z niezapowiedzianych darów komputerowej rewolucji: oprogramowania krypto-graficznego tak silnego, że teoretycznie nawet NSA nie mogła go złamać.

W latach dziewięćdziesiątych Departament Sprawiedliwości i FBI pod kie-rownictwem Louisa Freeha starały się usilnie o zdelegalizowanie takiego szyfrowania w USA, obawiając się, że trafi ono w ręce przedstawicieli przestępczości zorganizowanej, pedofili, terrorystów i hakerów. Był to daremny wysi-

łek. Amerykańscy matematycy już dziesiątki lat wcześniej stworzyli i 226

opublikowali algorytmy szyfrowania o wysokim poziomie bezpieczeństwa, które konkurowały z rządowymi systemami utajniania danych - dżin już wyszedł z butelki. W1991 roku programista i aktywista z USA Phil Zimmerman wypuścił darmowe oprogramowanie Pretty Good Privacy, które było dostępne w sieci. Nie powstrzymało to jednak funkcjonariuszy policji i wywiadu przed podejmowaniem prób. W 1993 roku administracja Clintona zaczęła wypuszczać tak zwane Clipper Chips, rozwinięte przez NSA czipy szyfrujące przeznaczone do użytku w komputerach i telefonach i zaprojektowane z funkcją „odzyskiwania klucza", która pozwalała władzom na łamanie szyfrów na życzenie całkowicie zgodnie z prawem. Czip poniósł porażkę na rynku i projekt upadł

przed 1996 rokiem.

Potem ustawodawcy zaczęli zmierzać w przeciwnym kierunku, uchylając regulacje z okresu zimnej wojny - tajne mocne szyfrowanie było według nich

„uzbrojeniem", którego eksport generalnie został zakazany. Regulacje te zmu-szały firmy technologiczne do trzymania mocnych szyfrów z dala od kluczo-wego oprogramowania internetowego, osłabiając bezpieczeństwo online, podczas gdy po drugiej stronie oceanu firmy nie były skrępowane przepisami prawa i miały dobrą pozycję, by przejąć amerykański rynek szyfrowania.

Federalni odpowiedzieli drakońskimi kontrpropozycjami, mającymi uczynić sprzedaż na terenie USA jakiegokolwiek oprogramowania szyfrującego, do którego nie mogli mieć tajnego klucza szpiedzy policyjni i rządowi, przestępstwem zagrożonym karą do pięciu lat więzienia. W oświadczeniu dla podkomi-sji Izby Reprezentantów w 1997 roku prawnik z Departamentu Sprawiedliwo-

ści przestrzegał, że hakerzy będą pierwszymi nabywcami legalnego szyfrowania, i posłużył się przykładem zatrzymania Carlosa Salgado, by zilustrować swoje racje. Salgado zaszyfrował CD-ROM z 80 000 skradzionych numerów kart kredytowych. FBI potrafiło się do nich dostać tylko dlatego, że haker dał

swemu domniemanemu klientowi klucz.

„Mieliśmy szczęście w tej sprawie, ponieważ człowiek, który kupował od Salgado, był współpracownikiem FBI - stwierdził urzędnik. - Ale gdybyśmy trafili na tę sprawę w inny sposób, policja nie mogłaby uzyskać dostępu do 227

informacji na CD-ROM-ie Salgado. Przestępstwa takie jak to mają poważne konsekwencje dla zdolności policji do zabezpieczania danych handlowych, jak również osobistej prywatności".

Federalni przegrali szyfrową wojnę i w 2005 roku niemożliwe do złamania szyfry stały się szeroko dostępne dla każdego. Katastroficzne przewidywania w przeważającej mierze się nie sprawdziły - większość przestępców nie była na tyle inteligentna, aby używać szyfrowania.

Max jednak był. Gdyby jego cały proceder upadł i federalni weszliby do je-go kryjówki, znaleźliby wszystko, co zgromadził dzięki swej przestępczej dzia-

łalności: od numerów kart kredytowych po hakerski kod, zwinięte za pomocą stworzonego w Izraelu program szyfrującego DriveCrypt – tysiąctrzystutrzy-dziestoczterobitowego wojskowego szyfru, który kupił za około 60 dolarów.

Oczekiwał, że władze tak czy inaczej by go aresztowały i domagały się klucza do szyfru. On stwierdziłby, że go zapomniał. Sędzia federalny gdzieś tam nakazałby mu ujawnienie tajnego klucza, a on by odmówił. Potrzymano by go w areszcie za obrazę sądu może przez rok, a potem wypuszczono. Bez jego plików władze nie miałyby żadnych dowodów na jego prawdziwe przestępstwa.

Max nie pozostawił niczego na łaskę losu. Miał pewność - był nietykalny.

ROZDZIAŁ 31

Proces

Jonathan Giannone, carder z Long Island, którego Max i Chris odkryli, kiedy był nastolatkiem, miał pewną tajemnicę.

W tym samym dniu kiedy Max wessał swych konkurentów, agenci Secret Service aresztowali Giannonego w domu jego rodziców za sprzedaż zrzutów Maksa Brettowi Johnsonowi, informatorowi Secret Service, znanemu jako Gollumfun. Giannone został zwolniony za kaucją, ale nikomu nie powiedział o tym, że wpadł. Dla niego była to po prostu drobna stłuczka na drodze. Co wła-

ściwie mogli mu zrobić za sprzedaż 29 zrzutów?

Wrażenie, że miał do czynienia ledwie z klapsem, jeszcze wzrosło, kiedy sędzia z Południowej Karoliny zniósł mu ograniczenia w podróżowaniu miesiąc po wpadce. Giannone szybko znalazł się na lotnisku w Oakland w cardingowym biegu, a Tea odebrała go i wzięła na przejażdżkę. Jeździli tam i z powrotem Pacific Coast Highway, w Fat Slice na Berkeley's Telegraph Avenue kupiła mu kawałek pizzy. Giannone zawsze był według niej zabawny - cheł-

pliwy biały dzieciak o kręconych włosach z hiphopową wrażliwością, który kiedyś w miejscowym barze przechwalał się, że pobiłby zawodnika New York Jets. Teraz jednak coś ich łączyło:

Chris przestał rozmawiać z Giannonem mniej więcej w czasie, kiedy go aresztowano, podczas gdy Tea dostała rozkaz powrotu do Bay Area, by nie sprawiać już problemów ze związkami Chrisa. Wygnał ich oboje.

Chris zadzwonił do Tei, kiedy szwendała się z Giannonem, i był zaskoczony, gdy usłyszał, że chłopak jest w mieście. Kazał jej go dać do telefonu.

- Co, zabierasz teraz moje dziewczyny na imprezę? - dopytywał się zły, że Giannone umówił się z jedną z jego dziewczyn, być może wciągając ją do własnej ekipy.

- Nie, po prostu tak się złożyło, że tu byłem i spotkałem ją - powiedział

Giannone trochę przepraszająco.

To miała być ostatnia telefoniczna rozmowa Chrisa z Giannonem. Chłopak wrócił do domu. Utrzymywał kontakt z Teą i kilka miesięcy później ostrzegł ją, że może być osobą, do znajomości z którą lepiej się nie przyznawać. Był przekonany, że ktoś go śledził w czasie podróży do Bay Area.

- Wokół mnie robi się teraz gorąco - powiedział.

- Co masz na myśli? - zapytała Tea.

Giannone lubił tworzyć atmosferę zagrożenia.

- W przyszłym tygodniu będę miał proces.

Federalne procesy w sprawach kryminalnych należą do rzadkości. Mając przed sobą perspektywę długoletniej odsiadki, gwarantowanej przez surowe wytyczne wyroku, większość obrońców wybiera przyznanie się do winy w zamian za nieznaczne zmniejszenie wyroku lub ograniczenie ujawnienia dzięki zostaniu informatorem. Jakieś 87 procent śledztw zakończyło się w ten sposób w roku 2006, kiedy to odbył się proces Giannonego. W kolejnych 9 procentach przypadków oskarżenia zostały odrzucone, zanim doszło do procesu, ponieważ władze wolały raczej zrezygnować z drobnej sprawy, niż ryzykować porażkę.

Kiedy już ława przysięgłych się zgromadzi, szanse oskarżonego na uniewinnienie wynoszą około jednego do dziesięciu.

230

Ale Giannone lubił ryzyko. O większości spraw nie mogły decydować zeznania tajnego agenta, będącego aktywnym przestępcą komputerowym. Brett

„Gollumfun” Johnson, wkrótce po tym jak doniósł na Giannonego, ruszył w czteromiesięczny przestępczy rajd po kraju, dokonując swych oszustw na fikcyjny zwrot podatku w Teksasie, Arizonie, Nowym Meksyku, Las Vegas, Kalifornii i Florydzie, gdzie w końcu aresztowano go w Orlando z prawie 200 000

dolarów upchniętymi w plecakach w jego sypialni. Nie był zbyt dobrym świadkiem oskarżenia.

Urzędnik sądowy wręczył kartki i ołówki dwunastu ławnikom i prokurator zaczął wygłaszać swe wstępne oświadczenie, przyjmując ciepły, familiarny ton.

„Kocham Internet - powiedział. - Internet jest fascynującą rzeczą. To miejsce, gdzie możemy się rozerwać, znaleźć informacje, oglądać filmy, grać w gry, kupować różne rzeczy. eBay jest świetnym miejscem, możesz licytować różne rzeczy. Możesz tam kupić, co tylko przyjdzie ci do głowy.

Ale, drodzy państwo, Internet ma też drugą stronę, o której nie lubimy my-

śleć. Ciemną stronę - to ta jego część, gdzie nie handluje się czy wymienia błyskotkami czy pomponami, ale gdzie ludzie handlują bądź wymieniają się ludzkim życiem…

Zobaczycie tę stronę Internetu. I podejrzewam, że już nigdy nie będziecie patrzeć na Internet tak jak dawniej”.

Proces trwał trzy dni. Prokurator wysłał Bretta Johnsona prosto za kratki, stwierdzając, że Gollumfun jest kłamcą i złodziejem, który zdradził zaufanie swych opiekunów z Secret Service. Właśnie z tego powodu władze nie powoła-

ły go na świadka. „Głównym świadkiem” będą komputerowe zapisy rozmów Giannonego z informatorem. Przemówią same za siebie.

Adwokat Giannonego robił co mógł, by podważyć zapisy. „Komputery po-pełniają błędy”. Twierdził, że ponieważ kradzione karty kredytowe nie zostały 231

użyte, nie było ofiar. Przypominał ławnikom, że nikt nie umarł ani nie odniósł

obrażeń ciała.

Po całym dniu rozstrząsań wydano werdykt: winny. Pierwszy federalny proces cardingowego półświatka był zakończony. Sędzia zdecydował, że Giannone pójdzie do aresztu.

Tydzień później Giannone został wypuszczony ze swej celi w Lexington County Jail. Od razu rozpoznał agentów Secret Service czekających przy bra-mie wyjściowej, dwóch parach żelaznych drzwi dzielących go od wolności. Ci dwaj faceci byli opiekunami Johnsona i zeznawali na procesie Giannonego.

- Chcemy wiedzieć, kim jest ten Iceman - powiedział jeden z nich.

- A kto to jest Iceman? - odparł niewinnie Giannone.

Sytuacja jest poważna, powiedzieli agenci; dowiedzieli się, że Iceman groził, iż zabije prezydenta. Giannone poprosił o prawnika i agenci od razu do niego zadzwonili. Adwokat zgodził się na rozmowę w nadziei, że zdobędzie pobłażliwość dla swego klienta przy ogłaszaniu wyroku.

W serii spotkań w ciągu kolejnych trzech tygodni agenci wyciągali Giannonego z więzienia raz po raz, przewożąc go do tego samego biura terenowego, gdzie Gollumfun pracował nad swym upadkiem. W przeciwieństwie do większości carderów, Giannone trzymał swoje brudy w areszcie i stawił się na proces, zamiast przyjąć ofertę i zostać donosicielem. Ale teraz wisiał nad nim pię-

cioletni wyrok. Miał tylko 21 lat.

Giannone powiedział im wszystko, co wiedział: Iceman mieszka w San Francisco, prowadzi ożywiony handel zrzutami, czasem używa aliasów Digits i Generous, pod którymi sprzedaje swój towar. Hakuje przez WiFi, by zatrzeć ślady. Mongołka imieniem Tea jest jego tłumaczką z rosyjskiego.

Co ważniejsze, ma wspólnika nazwiskiem Christopher Aragon w Orange County w Kalifornii. Chcecie Icemana? Złapcie Chrisa Aragona.

Rewelacje zelektryzowały agentów tropiących Icemana. Kiedy Keith Mularski wstukał nazwisko Chrisa Aragona do systemu zarządzania śledztwami FBI, 232

znalazł zeznania Wernera Janera z 2006 roku, który podał imię dostawcy zrzutów Chrisa, opisując go jako wysokiego mężczyznę z włosami spiętymi w kucyk, którego znał jako „Maksa Hakera". Dalej było jeszcze lepiej. Wcześniej, w grudniu 2005 roku, Jeff Norminton został aresztowany za przejęcie przelewu Janera dla Aragona. Opowiedział FBI o przedstawieniu Aragonowi superhake-ra Maksa Butlera po jego wyjściu z Taft. Przesłuchujący Normintona agent był

zainteresowany tylko oszustwami na nieruchomościach i nie poszedł za tymi wskazówkami.

Teraz Mularski i jego odpowiednicy z Secret Service mieli nazwisko. Zeznania Giannonego potwierdziły to. Iceman powiedział Giannonemu, że kiedyś miał rewizję, bo podejrzewano go o kradzież kodu źródłowego *Half-Life 2*.

Mularski przeprowadził kolejne wyszukiwanie i zobaczył, że były tylko dwa amerykańskie nakazy rewizji przeprowadzone w tym śledztwie: jeden na nazwisko Chrisa

Toshoka, a drugi Maksa Raya Butlera.

Tożsamość Icemana przez cały czas pozostawała ukryta w rządowych komputerach. Giannone dał im hasło, by ją otworzyć.

Poznanie tożsamości Icemana nie było równoznaczne z jej dowiedzeniem.

Federalni mieli wystarczające powody, by wydać nakaz rewizji, ale nie znali adresu kryjówki Maksa. Co gorsza, Giannone powiedział im, że Iceman używa DriveCrypt. Oznaczało to, że nawet jeśli wytropią jego adres, nie mogą liczyć na znalezienie dowodów na jego twardym dysku. Mogli wyważyć drzwi w mieszkaniu Maksa, a potem patrzeć, jak wychodzi z sądu 24 godziny później za kaucją lub na pisemne zobowiązanie. Mając do dyspozycji sieć międzynarodowych sprzedawców fałszywych dokumentów tożsamości i złodziei tożsamo-

ści, do których wystarczyło tylko zadzwonić, Max mógł na zawsze zniknąć z pola widzenia.

Musieli się zabezpieczyć, zanim zrobią jakikolwiek ruch. Mularski uznał, że kluczową postacią jest Chris Aragon. Dzięki Normintonowi wiedzieli wszystko o przelewie i oszustwach w nieruchomościach, z których Chris czerpał zyski niemal pięć lat wcześniej. Gdyby mogli przymknąć Aragona za to, mogliby 233

przycisnąć go, by współpracował z nimi w sprawie przeciw Maksowi.

Nieświadomy pętli zaciskającej się wokół jego szyi Max kontynuował swoje całodobowe zarządzanie Carders Market jako Aphex. Nie żeby ktoś dał się nabrać na jego nowy nick. W swym nowym wcieleniu nie mógł powstrzymać się przed kontynuowaniem kampanii Icemana przeciw przywódcom DarkMarket, nazywając ich „niekompetentnymi idiotami”, i puszczaniem w obieg dowodów, które zebrał przeciw Master Splyntrowi. Był zaskoczony tym, że tak wielu ludzi mu nie wierzy. „DarkMarket został założony i jest prowadzony przez NCFTA/FBI na litość boską!”

Th3C0rrupted0ne wierzył Maksowi i zrezygnował ze swego statusu na DarkMarket, by pracować jako pełnoetatowy admin na forum Maksa, i teraz poświęcał stronie czternaście godzin dziennie. Ale Max nie ufał nawet jemu.

Dobrze wiedziano, że ten C0rrupted mieszka w Pittsburghu, gdzie znajduje się siedziba NCFTA.

Max stworzył nowy test dla możliwych informatorów i w marcu wypróbo-wał go na carderach, oznajmiając ni z tego, ni z owego, że współpracuje z organizacją terrorystyczną i proponując: „powinniśmy zastrzelić prezydenta Bus-ha w nadchodzący weekend”. Gdyby C0rrupted był federalnym, byłby zobowiązany do zniechęcenia do planowanego zabójstwa, myślał Max, lub spytałby o więcej szczegółów.

Corrupted odpowiedział krótko, rozwiewając wątpliwości Maksa. „Powodzenia z prezydentem. Nie zapomnijcie dorwać wiceprezydenta. On nie jest lepszy”.

Na forum było wiele pracy. Carders Market rozwijał się, mając kilkunastu wyspecjalizowanych sprzedawców: DataCorporation, Bolor, Tsar Boris, Perl i RevenantShadow sprzedawali numery kart kredytowych z CW2s, skradzione na różne sposoby w USA, Wielkiej Brytanii i Kanadzie; Jewin sprzedawał

kalifornijskie prawa jazdy; Notepad za niewielką opłatą testował ważność zrzutów; Snake Solid sprzedawał amerykańskie i kanadyjskie zrzuty. Woroszyłow 234

oferował złodziejom tożsamości usługi, dzięki którym mogli uzyskać numer ubezpieczenia społecznego ofiary i datę urodzenia; DelusionNFX sprzedawał

znakowane dane bankowości online; Illusionist był odpowiedzią Carders Market na JiLsiego, sprzedawał nowe szablony i obrazy kart kredytowych; Imagine konkurował z Easylivinem w handlu plastikiem.

Max próbował wprowadzić żelazną dyscyplinę. „Jak w wojsku” - skarżył

się jeden z krytycznie nastawionych carderów. Podobnie jak w czasach kiedy był białym kapeluszem, Max nagradzał intelektualną uczciwość, odmawiając specjalnych względów nawet najbliższym sprzymierzeńcom.

W kwietniu C0rrupted przygotował recenzję ostatniej generacji „nowych” dokumentów tożsamości i plastiku Chrisa. Stwierdził, że są wadliwe z jednego powodu - paski na podpisy były wydrukowane bezpośrednio na karcie - trzeba było je podpisywać pisakiem. Uważał, że produkty zasługiwały na pięć gwiaz-dek z dziesięciu, ale spytał Maksa, czy powinien trochę złagodzić swoją ocenę.

„Wiem, że ty i Easylivin przyjaźnicie się, więc chciałem wiedzieć, czy powi-nienem napisać w poście moją prawdziwą opinię o tych rzeczach, czy nie po-winienem być tak surowy”.

„Uważam, że zdecydowanie powinieneś napisać prawdę, a jeśli to możliwe, zilustrować to zdjęciami itd. - odpisał Max. - Przyjaźnię się z Easylivinem, ale uważam, że prawda jest ważniejsza. Poza tym, jeśli dostanie dobrą recenzję i będzie sprzedawał kiepski towar (cholera… czy to naprawdę jest aż tak złe?), odbije się to źle na tobie i na Carders Market”.

Negatywna recenzja oznaczała, że Chris straci pieniądze. Max jednak nie wahał się, kiedy w grę wchodziła spójność jego przestępczego forum.

ROZDZIAŁ 32

Centrum handlowe

Chris wjechał swym tahoe do garażu w Fashion Island Mall w Newport Beach, zaparkował

i

wysiadł

wraz

ze

swym

nowym

wspólnikiem

-

dwudziestotrzyletnim Guyem Shitritem. Ruszyli ku Bloomingdale’s z fałszywymi kartami kredytowymi w portfelach.

Pochodzący z Izraela Shitrit był przystojnym gitarzystą i kobieciarzem, któ-

rego Chris poznał na Carders Market. Shitrit prowadził operację skimmingową w Miami, rekrutując profesjonalne striptizerki i dając im bardzo małe skimmery, by kradły swoim stałym klientom dane z pasków magnetycznych. Kiedy menedżerowie klubów ze striptizem dowiedzieli się o tym, Shitrit musiał w pośpiechu uciekać z miasta. Wylądował w Orange County, gdzie Chris obdarzył go fałszywymi dokumentami tożsamości, wynajętym samochodem i mieszkaniem w Archstone. Potem zaczęli chodzić po sklepach.

Chris był teraz bliski, bardzo bliski wyjścia z interesu. Jego żona Clara wy-ciągnęła na eBayu w ciągu nieco ponad trzech lat 780 000 dolarów, sprzedając 2609 torebek Coacha, iPody, zegarki Michele i ciuchy z Juicy Couture. Miała pracownicę, która przez 20 godzin w tygodniu zajmowała się wyłącznie do-starczaniem klientom nieuczciwie zdobytych towarów. Chris dorabiał na 236

sprzedaży plastiku i nowości na Carders Market, przedsięwzięciu, któremu nie pomogła kąśliwa recenzja Th3C0rrupted0ne.

Czuł, że Max ignoruje Whiz List - ich plan na dokonanie jednego wielkiego skoku i wyjście z interesu. Chris w końcu to zrozumiał: Max nie chciał tego.

Lubił hakowanie; tylko to chciał robić. Pieprzyć więc go. Chris miał własną strategię wyjścia. Zainwestuje swe zyski w przedsiębiorstwo Clary - produkujące odzież dżinsową firmę Trendsetter USA, która już zatrudniała kilku pełno-etatowych pracowników w jasnym, przyjemnym biurze w Aliso Viejo. Był

przekonany, że kiedyś ten biznes zacznie przynosić zyski. I jest w stu procentach legalny.

Do tej chwili Chris nadal będzie zajęty.

Shitrit był modnisiem i roztrwonili już część skradzionych kart kredytowych na ciuchy dla siebie. Podczas tego wypadu byli skupieni. Weszli do kli-matyzowanego chłodu Bloomingdales, kierując się najkrótszą drogą do działu damskich torebek. Torebki Coacha spoczywały na najniższych półkach wzdłuż ściany, rozłożone każda osobno, jak muzealne eksponaty. Chris i Guy wzięli po kilka i podeszli do kasy. Po kilku przeciągnięciach przez terminal ruszyli ku wyjściu z wartymi 13 000 dolarów torebkami Coacha w rękach.

Chris złamał własne reguły, idąc na zakupy, ale jego ekipa nagle mocno schudła. Nancy, która pomogła zorganizować nową kryjówkę Maksa, przeniosła się do Atlanty i robiła tutaj tylko małe zakupy. Liz stała się chorobliwie podejrzliwa - nieustannie oskarżała Chrisa o oszukiwanie jej, wyrażając swoje niezadowolenie w drobiazgowych, ręcznie pisanych arkuszach kalkulacyjnych, w których wyliczała, jak wiele Chris jest jej winien za każde zakupy: 1918

dolarów z wyjazdu do Vegas; 674 za iPody i GPS-y; 525 za cztery torebki Coacha warte 1750. Kolumna „zapłacono mi” była z góry na dół wypełniona ze-rami. Tymczasem jego nowa pracownica Sarah unikała kupowania bardzo drogich rzeczy, jednak ciągle była użyteczna do załatwiania drobnych sprawun-ków. Na walentynki kupiła Chrisowi prezenty dla jego żony i kochanki.

237

Mając na głowie sprzedaż, rozkręcanie legalnego biznesu i odbudowywanie swojej ekipy, Chris stwierdził, że lepiej będzie zatrudnić teraz kogoś do robienia jego kart. Federika Vigo poznał w UBuyWe-Rush. Vigo szukał sposobu na spłacenie 100 000 dolarów długu meksykańskiej mafii, po tym jak przyjął tę sumę z góry, by ściągnąć paletę efedry z Chin, wyłącznie po to by jego towar został przechwycony na granicy. Chris wziął go do pracy. Sprzęt do podrabiania został przeniesiony z Tea House do biura Vigo w Northridge i jeden z pomagierów Chrisa wyruszał poza Valley kilka razy w tygodniu, zbierając świeże pliki kart kredytowych, gorących jeszcze i spod prasy, płacąc Vigo 10 dolarów za sztukę.

Chris i Guy wyszli z Bloomingdales i nie spiesząc się, wracali do SUV-a.

Chris otworzył tylne drzwi i znalazł miejsce na nowe zakupy między dziesiątkami ciasno poutykanych gładkich brązowych toreb z butików. Wszystkie były wypełnione torebkami, zegarkami i kilkoma męskimi ciuchami. Zamknął

drzwiczki; wsiedli do samochodu i zaczęli planować następny przystanek.

Ciągle jeszcze się zastanawiali, kiedy biały policyjny radiowóz wjechał do garażu. Zatrzymał się obok nich i wyrzucił dwóch umundurowanych funkcjonariuszy policji Newport Beach.

Chris zamarł. Kolejna wpadka.

Policjanci spisali Chrisa na posterunku w Newport Beach niedaleko od centrum handlowego, następnie przeszukali jego samochód, odkrywając siedemdziesiąt kart kredytowych oraz niewielkie ilości ecstasy i xanaksu. Kiedy zdjęto mu odciski palców, Chris został zaprowadzony do pokoju przesłuchań, gdzie detektyw Bob Watts wręczył mu formularz z Prawami Mirandy.

Chris podpisał i zaczął opowiadać tę samą historyjkę, dzięki której wykara-skał się z

poważnych kłopotów w San Francisco kilka lat wcześniej. Szybko podał swe prawdziwe nazwisko i wyraził skruchę z powodu używania podro-bionych kart kredytowych w Bloomingdales i w innych miejscach. To ze 238

względu na kryzys gospodarczy, powiedział. Pracował w branży kredytów mieszkaniowych i mocno ucierpiał, gdy zawalił się rynek nieruchomości. Wtedy właśnie boss cardingowego gangu z Orange County zwerbował go do robienia zakupów przy użyciu fałszywych kart za niewielki procent zysków. Był

tylko mułem.

Watts, który wcześniej złapał drobnych mułów, słyszał tę historyjkę nie pierwszy raz. To by nawet wyjaśniało amatorskie zachowanie Aragona w raj-dzie na Bloomingdales - zgarnięcie tylu wartych tysiące dolarów torebek Coacha naraz. Ochrona w Bloomingdale’s nie lubi niepokoić klientów sklepu, więc kiedy ktoś wyda im się podejrzany, zazwyczaj dzwoni do Wattsa lub jego partnera, a policjanci urządzają dyskretne zatrzymanie na drodze - za „naruszenie przepisów drogowych” - by sprawdzić podejrzanego z dala od sklepu. Jeśli klient był niewinny, nigdy się nie dowiedział, że to Bloomingdale’s zatelefo-nowało na policję w jego sprawie. Zachowanie Chrisa i Shitrita było jednak tak rażące, że kierownictwo sklepu nie miało wątpliwości, iż są winni. Ochrona zadzwoniła bezpośrednio do policyjnego centrum zgłoszeń, by mieć pewność, że mężczyźni nie ulotnią się z parkingu.

Watts nie kupił jednak historyjki o prześladującym Chrisa pechu. Był detektywem zaledwie od ośmiu miesięcy, ale gliniarzem od siedmiu lat. Pierwszą rzeczą, jaką zrobił, kiedy Aragon wpadł, było sprawdzenie go w NCIC. Poznał

przestępczą historię Chrisa sięgającą lat siedemdziesiątych i zorientował, że teoretycznie ciągle jeszcze był on na zwolnieniu warunkowym po ostatniej wpadce w San Francisco - za fałszowanie kart kredytowych.

Watts pojął, że ma w swej celi przywódcę gangu. W pośpiechu uzyskał nakaz rewizji i podążył wraz z ekipą detektywów i umundurowanych policjantów pod jedyny adres Chrisa, jaki udało mu się ustalić: Trendsetter USA. Jedno spojrzenie na zdumione twarze pracowników, gdy gliniarze jak burza weszli do środka, wystarczyło, by Watts był pewny, że są niewinni. Po kilku pytaniach jeden z pracowników wspomniał, że ich szefowa Clara prowadzi biznes zwią-

zany z handlem na eBayu w biurze z tyłu budynku.

239

Watts otworzył pomieszczenia magazynowe na zapleczu i zabrał całą zawartość: 31 torebek Coacha, 12 aparatów cyfrowych Canon Power-Shot, kilka nawigacji GPS TomTom, okulary przeciwsłoneczne Chanel, palmtopy i iPody, wszystko nowe, jeszcze w pudełkach.

Clara weszła do biura w trakcie rewizji i od razu została aresztowana. W jej torebce Watts znalazł rachunki za prąd, wodę, gaz itp. na adres w Capistrano Beach, każdy na inne nazwisko. Clara niechętnie przyznała, że tam mieszka, i zbladła, kiedy Watts powiedział, że to będzie kolejne miejsce, które odwiedzi.

Z jej kluczami i nowym nakazem rewizji w dłoni detektywi pojawili się w domu Aragona i zaczęli przeszukiwanie. W domowym biurze Chrisa znaleźli otwarty sejf w szafie. W środku były dwa plastikowe segregatory wypchane podrobionymi kartami. W sypialni znaleźli ich jeszcze więcej, związanych taśmą klejącą i schowanych w nocnej szafce. MSR206 spoczywał na półce w pokoju dziennym, a w sąsiadującym z nim garażu pudło pełne torebek stało na podłodze obok sprzętu do fitnessu.

Poza jadalnią i łazienkami jedynym miejscem, w którym nie znaleziono dowodów przestępczej działalności, była wygodna sypialnia chłopców. Tylko dwa takie same łóżka, jedno obok drugiego, pluszowe zwierzaki i zabawki.

W całej swojej gadce o fałszowaniu kart kredytowych jako przestępstwie bez ofiar Chris przeoczył dwie najbardziej wrażliwe ofiary swego postępowania. Jedna miała cztery lata, druga siedem, a ich tatuś nie wracał do domu.

ROZDZIAŁ 33

Strategia wyjścia

- To federalny - powiedział Max, wskazując mijającego ich sedana. Charity sceptycznie spojrzała na forda. Amerykańskie samochody były po prostu kolejną rzeczą, która ostatnio budziła niepokój Maksa.

Minęły tygodnie od aresztowania Chrisa i czytając poświęcone temu wyda-rzeniu artykuły w gazetach z Orange County, Max nie mógł sobie poradzić z tym, jak wiele dowodów policja znalazła w domu Aragona. Używając arkuszy z wypłatami, które sporządził Chris, jako przewodnika, gliniarze wytropili całą jego ekipę - nawet Marcusa, hodowcę marihuany i chłopca na posyłki, w któ-

rego mieszkaniu w Archstone odkryto domową hodowlę konopi. Po dwóch tygodniach polowań policja znalazła fabrykę kart kredytowych Chrisa w biurze Federika Vigo w Valley, aresztowała Vigo i zarekwirowała cały sprzęt. Za zwolnienie Chrisa wyznaczono kaucję w wysokości miliona dolarów.

Całe przedsiębiorstwo było rozbierane kawałek po kawałku. Nazwano je prawdopodobnie największym gangiem złodziei tożsamości w historii Orange County.

„Kurde, zastanawiam się, jakie dane miał na swoich komputerach - napisał

później Max do Th3C0rrupted0ne. - Jeśli był na tyle niedbały, by trzymać sprzęt w domu”.

Max już wyrzucił swoją komórkę na kartę i wprowadził „ban bezpieczeń-

stwa” na konto swojego dawnego wspólnika z Carders Market. To były rutynowe środki ostrożności - na początku nie był specjalnie zaniepokojony aresztowaniem; w końcu była to tylko sprawa stanowa. Chris został już złapany na gorącym uczynku w W i wtedy wywinął się, dostając jedynie dozór prokurator-ski.

Jednak gdy minęło kilka tygodni, a Chris ciągle pozostawał za kratami, Max zaczął się martwić. Zauważał dziwne samochody zaparkowane na jego ulicy -

furgonetka służby zajmującej się bezdomnymi zwierzętami wzbudziła jego podejrzenia

tak bardzo, że wyciągnął latarkę, by zajrzeć w jej okna. Potem agent FBI z San Francisco zadzwonił do niego ni z tego, ni z owego, pytając o dawno martwą bazę danych arachNIDS. Max postanowił zainwestować w sznurową drabinkę; trzymał ją w oknie wychodzącym na podwórko budynku, w którym mieszkał z Charity, w razie gdyby musiał szybko się ewakuować.

Co chwila zastanawiał się nad swoją wolnością - on był tu, cieszył się życiem, hakowaniem, podczas gdy w tym samym czasie Chris siedział w więziennej celi w Orange County.

Z żółtych stron wybrał na chybił trafił adwokata z San Francisco, poszedł do jego biura i wręczając plik banknotów, chciał, by prawnik pojechał do południowej Kalifornii i sprawdził, czy nie dałoby się czegoś zrobić dla Chrisa.

Adwokat odpowiedział, że przyjrzy się sprawie, ale nigdy się nie odezwał.

Wtedy właśnie Max w końcu dowiedział się o aresztowaniu Giannonego z artykułu prasowego na temat życia Bretta Johnsona jako informatora. Max zgubił ślad Giannonego i przy całym tym hakowaniu nigdy nie przyszło mu do głowy, by sprawdzić nazwiska swych znajomych na stronie internetowej sądu federalnego. Wiadomość, że Giannone został skazany w procesie kryminalnym, przestraszyła go.

„Ze wszystkich skurwysyńskich kabli Giannone jest najbliższy podania mnie federalnym na talerzu - wyznawał w prywatnym poście administratorów forum na Carders Market. - Ten mały gnojek może naprawdę być zdolny do ściągnięcia mi na głowę federalnych".

Max wyniósł się z Fox Plaza, ukrywając swój sprzęt w domu, do momentu kiedy znalazł nowe lokum. 7 czerwca odebrał klucze w Oakwood Geary, kolejnym apartamentowcu wykutym z błyszczącego marmuru w Tenderloin. Teraz nazywał się „Daniel Chance" i był po prostu kolejnym softwareo'wym trut-niem, który przeniósł się do Bay Area. Prawdziwy Chance miał pięćdziesiąt lat i brodę, podczas gdy Max był gładko wygodny i nosił długie włosy, ale fałszywe prawo jazdy i prawdziwy przekaz pieniężny wystarczyły, by mógł tam zamieszkać.

Następnego wieczoru Max wypożyczył czerwonego mustanga z sąsiedniego Zipcar i zapakował do niego sprzęt komputerowy. Przy całej swej paranoi nie zauważył agentów Secret Service śledzących go w drodze do Oakwood i wi-dzących z ulicy, jak wchodzi do nowej kryjówki.

Miesiąc później coś nagle wyrwało Maksa ze snu. Usiadł wyprostowany na łóżku, próbując dostrzec coś w ciemnym mieszkaniu. To była tylko Charity; wsunęła się do łóżka obok niego, bezskutecznie próbując go nie obudzić. Z każdym dniem stawał się coraz bardziej nerwowy.

- Kochanie, nie możesz tak żyć - wymruczała Charity. - Może ty sobie tego nie uświadamiasz, ale ja tak, ja to widzę. Stajesz się coraz bardziej opętany przez to. Przestajesz być sobą i nie wiesz, co robisz.

- Masz rację - powiedział. - Jestem skończony.

Minęło wiele czasu od ostatniego pobytu w więzieniu, myślał Max. Może mógłby znaleźć znowu uczciwą pracę. NightFox już zaoferował mu legalne zajęcie w Kanadzie, ale odmówił. Nie mógłby opuścić Charity. Zastanawiał się nad małżeństwem, bawiąc się pomysłem zwabienia jej do Las Vegas na wakacje, by tam się oświadczyć. Była bardzo niezależna, ale nie mogła się skarżyć, że nie daje jej dużo wolności.

243

Postanowił, że nadeszła pora na powrót Maksa Visiona, białego kapelusza.

To będzie oficjalny charakter. Odwiedził budynek sądu w San Francisco i wy-pełnił potrzebne papiery. 14 sierpnia sędzia zatwierdził legalną zmianę nazwiska z Max Butler na Max Ray Vision.

Miał już pomysł na nową stronę, dzięki której znowu mógłby się znaleźć w świecie białych kapeluszy: system służący wykrywaniu i radzeniu sobie z dziu-rami zero-day. Mógł zacząć od luk w systemie bezpieczeństwa, w które został

wtajemniczony w półświatku, przynosząc exploity do świata białych kapeluszy, niczym uciekinier przekraczający Checkpoint Charlie z walizką pełną państwowych sekretów.

Jednak po całej pracy, jaką włożył w zrobienie z Carders Market czołowego przestępczego forum w anglojęzycznym świecie, nie potrafił tak po prostu tego porzucić.

Powrócił do swej kryjówki. To był sierpień i znowu poczuł żar - temperatu-ra na zewnątrz przekraczała 32 stopnie, a w jego kawalerce była jeszcze wyż-

sza. Istniało zagrożenie, że jego procesor sam się usmaży. Włączył wentylato-ry, usiadł przed klawiaturą i zaczął pracować nad stopniowym wycofaniem swych tożsamości Digitsa i Apheksa.

Zalogował się na Carders Market i jako Digits napisał posta, w którym stwierdzał, że przekazuje sprzedaż zrzutów Unauthorized, jednemu ze swych adminów. Potem, jako Aphex, ogłosił, że odchodzi z cardingu i sprzedaje Carders Market. Zostawił ogłoszenie na kilka minut, a następnie zamknął stronę.

Kiedy przywrócił, przy władzy był Achilous, jeden z administratorów z Kanady. Max stworzył dla siebie nowy, neutralny nick „Admin”, by w okresie przejściowym pomóc nowemu bossowi Carders Market.

Max nadal pracował nad swą strategią wyjścia, kiedy na ekranie pojawiła się wiadomość. Przyszła od Sila, kanadyjskiego cardera, który ciągle bez powodzenia próbował go zhakować. Max wytropił go i zidentyfikował jako Lloyda Liskego z Kolumbii Brytyjskiej. Podejrzewał, że Liske jest informatorem.

244

Post był dziwny, składał się z długiego zdania na temat nowicjuszy popeł-

niających głupie błędy. Silo ukrył w nim jednak inny przekaz, strategicznie zapisując dziewięć liter kapitalikami.

Układały się one w słowa „MAX VISION”.

Zgaduje, pomyślał Max. *Silo najprawdopodobniej nic nie wie.*

To było tylko zgadywanie.

W dniu, w którym Max ogłosił swoje odejście, agentka Secret Service Melissa McKenzie i federalny prokurator z Pittsburgha polecieli do Kalifornii, aby po-

łączyć z sobą luźne wątki.

Śledztwo było na ukończeniu. Secret Service dostała maile Digitsa od swego kontaktu w policji z Vancouver, oficera prowadzącego Sila. Max używał

poczty mailowej, której dostawcą była kanadyjska firma Hushmail, oferująca bardzo bezpieczne szyfrowanie przy użyciu apletu Javy, który szyfruje wiadomości bezpośrednio na pececie klienta, a nie na serwerze firmy. Teoretycznie ustawienie to zapewnia, że nawet Hushmail nie może dostać tajnego klucza klienta ani przychodzących maili. Firma otwarcie oferowała usługę jako sposób na obejście inwigilacji FBI.

Jednak, podobnie jak e-gold, Hushmail stała się kolejną kiedyś przyjazną przestępcom firmą, która teraz była infiltrowana przez policję. Amerykańskie i kanadyjskie agencje uzyskały specjalne nakazy z Sądu Najwyższego Kolumbii Brytyjskiej, które zmusiły kierownictwo Hushmail do sabotowania własnego systemu i wydania kluczy do szyfrów osób będących przedmiotem inwigilacji.

Teraz federalni mieli maile Maksa.

W tym samym czasie agencja zlokalizowała Teę, która mieszkała w Berkeley i była na zwolnieniu warunkowym - okazało się, że wpadła w Emeryville Apple Store kilka miesięcy wcześniej, płacąc kartami podarowanymi jej przez Aragona. Miał to być treningowy wypad dla nowych pracownic Chrisa, ale Tea nigdy wcześniej tego nie robiła i gdy pod wpływem impulsu do iPoda, którego kupowała, dorzuciła jeszcze PowerBooka, została aresztowana razem ze swą 245

trenerką. Chcąc uniknąć większych problemów, powiedziała Secret Service wszystko, co wiedziała.

Tymczasem Secret Service rozpoczęła sporadyczne śledzenie Maksa w realnym życiu. Z zeznań Wernera Janera Mularski dowiedział się, że Max ma dziewczynę o nazwisku Charity Majors. Ogólnodostępne źródła danych osobowych dostarczyły adresu, a nakaz ujawnienia jej rachunków bankowych dowiódł, że ma wspólne konto z Maksem. Secret Service miała na oku dom, w którym mieszkała, i w końcu dotarła za Maksem do Oakwood Geary.

Elektroniczna inwigilacja potwierdziła, że Max działał w Oakwood. FBI uzyskało tajny nakaz sądowy, który pozwalał mu na elektroniczny monitoring adresów IP łączących się z fasadą Carders Market w amerykańskiej firmie hostującej - nowoczesny odpowiednik zdejmowania tablic rejestracyjnych poza terenem kontrolowanym przez mafię. Kilka z nich doprowadziło z powrotem do abonentów Internetu mieszkających w zespole apartamentowców i korzystających z WiFi. Dwa tygodnie wcześniej agentka Secret Service przebrana za pokojówkę jechała windą z Maksem i zobaczyła, że otwiera mieszkanie numer 409. To była ostatnia informacja, której potrzebowano.

Zanim tam weszli, musieli jeszcze odwiedzić tylko jedno miejsce: Orange County Central Men’s Jail, ponure więzienie w płaskim, spalonym słońcem centrum Santa Ana w

Kalifornii. McKenzie i federalny prokurator Luke Dembosky zostali skierowani do pokoju widzeń, by spotkać się z Chrisem Aragonem.

Chris jako jedyny z całego gangu z Orange County pozostawał za kratami.

Clara i sześć dziewczyn z ekipy zgodziło się przyznać do winy w zamian za złagodzenie kary. Dzięki temu ostatecznie otrzymały wyroki od sześciu miesięcy do siedmiu lat więzienia. Clara dostała dwa lata i osiem miesięcy.

Dziećmi zajęła się matka Chrisa.

Kiedy zostali sobie przedstawieni, McKenzie i Dembosky przeszli do interesów. Nie mogą nic dla Chrisa zrobić w stanowej sprawie, ale jeśli będzie współpracował, do jego akt trafi miły list od władz USA, stwierdzający, że pomógł w dużym federalnym śledztwie. To mogłoby pozytywnie nastawić 246

sędziego w czasie wydawania wyroku. To wszystko, co mogą zaoferować.

McKenzie ułożyła kilka zdjęć i kazała wybrać Chrisowi to, które wydawało mu się znane. Jego sytuacja wyglądała źle. Z wyrokami za napady na bank i przemyt narkotyków mógł odpowiadać jako recydywista. Oznaczało to pewną karę od 25 lat do dożywocia.

Chris wybrał zdjęcie Maksa z kartoteki policyjnej. Potem opowiedział federalnym historię o przejściu Maksa Visiona na ciemną stronę.

W środę 5 września 2007 roku Max zatrzymał się przy poczcie, gdzie Charity wysiadła, by coś załatwić, i kazał taksówkarzowi jechać do centrum pod sklep CompUSA na Market Street. Kupił nowy wentylator do chłodzenia procesora, wszedł do mieszkania, rozebrał się i rzucił na łóżko w plątaninę nieposkłada-nego prania. Zapadł w głęboki sen.

Max przestał hakować, ale ciągle jeszcze wyplątywał się ze swego podwójnego życia - po pięciu latach miał wiele różnych spółek i związków z ludźmi, których nie mógł zerwać z dnia na dzień.

Spał, nie słysząc pukania do drzwi około drugiej po południu. Nagle drzwi otworzyły się i do pokoju wbiegło sześciu agentów z pistoletami w dłoniach, wykrzykując komendy. Max usiadł wyprostowany jak struna i krzyknął.

- Połóż ręce tak, bym mógł je widzieć! - krzyknął agent. - Połóż się!

Agent stanął pomiędzy Maksem a jego komputerami. Max często myślał, że w razie nalotu, będzie w stanie wyciągnąć wtyczkę od kabla zasilającego serwer, sprawiając, że już i tak dostatecznie mocna cyberobrona stanie się całkowicie nieprzenikniona. Teraz, kiedy działo się to naprawdę, uświadomił sobie, że zanurkowanie do komputerów jest niemożliwe, chyba że chce dostać kulkę.

Odzyskał spokój. Odłączone czy nie, jego komputery są zabezpieczone, a szyfr twardy jak kamień. Udało mu się trochę odprężyć, kiedy agenci pozwolili mu się ubrać, a potem prowadzili go na dół w kajdankach.

247

Po drodze minęli trzyosobową grupę, która czekała, aż Secret Service zabezpieczy kryjówkę. Nie byli to federalni, ale ludzie z Carnegie Mellon University’s Computer Emergency Response Team, i przyszli, by złamać szyfr Maksa.

To był pierwszy przypadek, kiedy CERT został zaproszony do wzięcia udziału w policyjnym nalocie - ale okoliczności były szczególne. Chris Aragon używał tego samego szyfru, zabezpieczającego cały dysk oprogramowania DriveCrypt, co Max i ani Secret Service, ani CERT nie były w stanie niczego z dysku wyciągnąć. DriveCrypt utrzymuje cały twardy dysk zaszyfrowany przez cały czas: wszystkie pliki, wszystkie nazwiska, system operacyjny, oprogramowanie, strukturę katalogu - każdą wskazówkę, która mogłaby powiedzieć, co robił użytkownik. Bez klucza do szyfru dysk równie dobrze mógłby służyć za frisbee.

Kluczem do złamania programu pełnego zaszyfrowania dysku jest dostanie się do niego, kiedy jeszcze działa na komputerze. W tym momencie dysk ciągle jest w pełni zaszyfrowany, ale klucz jest przechowywany w pamięci RAM, aby umożliwić oprogramowaniu szyfrowanie i deszyfrowanie danych z twardego dysku w locie.

Pukanie do drzwi było obliczone na oderwanie Maksa od komputerów, bo gdyby je wyłączył, zanim agenci Secret Service założą mu kajdanki, nawet CERT nie mógłby wiele zdziałać - zawartość pamięci RAM wyparowałaby.

Ale Max został zaskoczony w czasie drzemki i jego serwery ciągle chodziły.

CERT spędził ostatnie dwa tygodnie, analizując różne scenariusze tego, co można znaleźć w kryjówce Maksa. Teraz szef ekipy popatrzył na ustawienia: serwer był podłączony do sześciu twardych dysków. Dwa straciły zasilanie, kiedy agent wyrwał kabel wijący się po podłodze, ale sam serwer ciągle działał

i to się liczyło.

Kiedy lampy błyskowe Secret Service skakały po ścianach zagraconego mieszkania Maksa, eksperci sądowi ruszyli do komputerów i zaczęli pracę, używając oprogramowania memory-acquisition, które przynieśli z sobą, by wyciągnąć żywe dane z pamięci RAM na przenośny dysk.

Na dole, w mieszkaniu federalnych, Max czekał na dalszy rozwój wypadków.

Pilnowało go dwóch agentów. Miał być przesłuchany później - na razie agenci po prostu przy nim siedzieli, gadając. Agent z Secret Service pracował

w miejscowym biurze w San Francisco; zapytał swego kolegę z FBI, skąd przyjechał.

- Jestem z Pittsburgha - odpowiedział Keith Mularski.

Max odwrócił głowę, by spojrzeć na Master Splyntra. Nie było wątpliwości, kto wygrał wojnę carderów.

Agenci Secret Service cieszyli się z aresztowania.

- Marzyłam o tobie - powiedziała agentka Melissa McKenzie, kiedy wiozła Maksa do biura terenowego. Widząc jego podniesione brwi, dodała: - To znaczy o Icemanie. Nie o tobie osobiście.

Dwóch miejscowych agentów zostało wysłanych do domu Charity. Powiedzieli jej, co się stało, i zabrali ją do centrum, by pożegnała się z Maksem.

- Przepraszam - powiedział, kiedy weszła. - Miałaś rację.

Max przez chwilę rozmawiał z agentami z biura terenowego, próbując wyczuć, co wiedzą, i ocenić, w jak wielkich kłopotach się znalazł. Niektórzy z nich wydawali się zaskoczeni jego grzecznością, tym, że po prostu dał się lu-bić. Max nie pasował do ich wyobrażeń o zimnym, wyrachowanym bossie, którego tropili przez rok.

W drodze do więzienia McKenzie w końcu wyraziła swoje zaskoczenie.

- Wyglądasz na miłego faceta - powiedziała - i to ci pomoże. Ale mam do ciebie jedno pytanie… Dlaczego nas nienawidzisz?

Maksowi odjęło mowę. Nigdy nie czuł nienawiści do Secret Service ani FBI, ani nawet do konfidentów na Carders Market. Iceman tak. Ale Iceman nigdy naprawdę nie istniał; był przebraniem, osobowością, którą Max wkładał

jak garnitur, kiedy był w cyberprzestrzeni.

Max Vision nigdy w życiu nikogo nie nienawidził.

Głodni Programiści jako pierwsi dowiedzieli się, że Max znowu został aresztowany. Tim Spencer zaoferował podpisanie zobowiązania, by Max mógł

wyjść za kaucją. Jako zabezpieczenie miał prawie sto hektarów ziemi w Idaho, które kupił jako swą wymarzoną posiadłość z myślą o emeryturze. Kiedy Tim poznał szczegółowe zarzuty przeciw staremu przyjacielowi, zawahał się. Co jeśli naprawdę wcale nie zna Maksa? Moment zwątpienia minął i Tim podpisał

formularz. Matka Maksa zaoferowała jako zabezpieczenie swój dom, by jej syn mógł zostać zwolniony. Ostatecznie to jednak i tak nie miało znaczenia. Kiedy Max przyjechał do San Jose, gdzie został postawiony w stan oskarżenia, federalny magistrat odmówił mu prawa do wyjścia za kaucją i nakazał przewiezie-nie go do Pittsburgha.

Władze ogłosiły aresztowanie Icemana 11 września 2007 roku. Wiadomość pojawiła się na Carders Market, wywołując gwałtowny wybuch aktywności.

Achilous błyskawicznie skasował całą bazę danych z postami i prywatnymi wiadomościami, nie wiedząc, że federalni już ją mają. „Myślę, że baza danych SQL niemal dostała ataku serca, kiedy to robiłem, ale teraz już po wszystkim.

Myślę, że Aphex by tego chciał - napisał. - To forum jest otwarte na posty, więc ludzie mogą pisać i zastanawiać się, gdzie stąd pójść. Bądźcie tylko bardzo ostrożni, szczególnie jeśli chodzi o poniższe linki. Proszę, ograniczcie teo-rie spiskowe do minimum.

Powodzenia, Uważajcie na siebie”.

Silo pojawił się pod innym aliasem, niesłusznie nazywając swego dawnego rywala kablem, opierając się na informacjach z mediów, które źle zrozumiały współpracę Maksa z FBI, w czasach kiedy był białym kapeluszem. „To smutny widok, kiedy wspaniały facet odchodzi - napisał. - Wniósł wiele do tego forum i całego carderskiego światka jako sprzedawca i administrator. Wielu ludzi zarobiło dzięki niemu sporo kasy”.

Ale „kapuś zawsze będzie kapusiem” - napisał bez śladu ironii. „Całe to forum powstało

dlatego, że lata temu FBI i Aphex nie zgadzali się co do tego, na kogo miał donosić… Wniosek: on jest największym hipokrytą, jaki kiedykolwiek pojawił się w tym światku".

Kiedy już Mularski zasiadł z powrotem przy swoim biurku, założył czarny kapelusz Master Splyntra, by włączyć się w dyskusję na temat tego, co się 250

zdarzyło. Agent FBI doskonale wiedział, że Iceman nie był informatorem, ale po jego *alter ego* wszyscy będę oczekiwać, że podchwyci wiadomość o tym, że Max kiedyś współpracował z federalnymi. „No i gdzie ja jestem? - triumfował

na DarkMarket, ciesząc się tą chwilą. - Patrzcie… patrzcie… Co z tym nagłówkiem z SFGate.com? I cytatem, »Były konfident FBI w SF oskarżony o hakowanie instytucji finansowych«.

Czy ktoś inny coś w tym nagłówku dostrzegł? O taaak, konfident FBI. Okazało się, że był po prostu taki jak Gollumfun i El. Nic dziwnego, że Iceman zawsze się z nimi ścierał, ponieważ był taki jak oni i konkurował o względy swych mocodawców".

Kiedy Max pojawił się w Pittsburghu, nowy obrońca z urzędu próbował

uzyskać dla niego wyjście za kaucją, ale sędzia odmówił, po tym jak śledczy stwierdzili, że Max ma sporą ilość ukrytej gotówki i mógłby łatwo zniknąć z nowym nazwiskiem. Aby dowieść, że próbował wymknąć się federalnym, za-grali swoją atutową kartą: prywatnym wiadomościami Maksa, w których opisywał on, jak korzystał z fałszywych dokumentów tożsamości, kiedy podróżo-wał, i jak „wymknął się" do swej ostatniej kryjówki. Max wysłał te wiadomo-

ści do informatora Secret Service z Pittsburgha, który przez cały rok był adminem Carders Market.

Nie zdziwił się zbytnio, kiedy zobaczył, że wtyką był Th3C0rruptedOne.

ROZDZIAŁ 34

DarkMarket

Mężczyzna siedzi sztywno na gładkim drewnianym krześle i złowrogo patrzy w kamerę. Przed nim na ziemi leżą pomalowane kawałki popękanego gipsu.

Został rozebrany do majtek i trzyma tabliczkę pokrytą odręcznym pismem nad swym zwisającym brzuchem. JESTEM KIER, jest tam napisane dużymi po-grubionymi literami. MOJE PRAWDZIWE NAZWISKO MERT ORTAC…

JESTEM KABLEM. JESTEM ŚWINIĄ. JESTEM GNOJONY PRZEZ CHA0.

Pojawienie się tego zdjęcia na DarkMarket w maju 2008 roku sprawiło, że Mularski pospieszył z powrotem do centrum komunikacyjnego NCFTA. Jego szefowie będą chcieli wiedzieć, że jeden z adminów Master Splyntra właśnie uprowadził i torturował informatora.

Cha0 był inżynierem w Istambule, który sprzedawał wysokiej klasy skimmery do bankomatów i PIN-pady oszustom z całego świata. Potajemnie przy-mocowany do bankomatu skimmer zapisywał dane z pasków magnetycznych każdej karty debetowej czy kredytowej włożonej do bankomatu, a nakładka PIN-pad gromadziła tajne kody użytkowników.

Cha0 był bardzo wyrazistą postacią w półświatku. Jego robione we fleszu animowane reklamy na DarkMarket stały się klasyką. Zaczynały się od 252

rysunkowego ludzika brodzącego przez dom pełen pieniędzy. „Czy to ty? -

pytał tekst. - Tak. Jeśli kupiłeś skimmer i PIN-pad od Cha0”. W utrzymanym w podobnym stylu poradniku wideo dla nowych klientów jako narrator występo-wała uśmiechnięta karykatura samego Cha0. „Cześć, jestem Cha0. Sprzedaję urządzenia do skimmingu. Pracuję dla ciebie przez 24 godziny na dobę i robię najlepszy sprzęt skimmingowy.

Dzięki mnie i mojej grupie będziesz mógł zarabiać na tym interesie. Robimy te urządzenia dla początkujących - są tak łatwe w użyciu!” Potem animo-wany Cha0 udziela praktycznych rad: nie instaluj swojego skimmera rano, ponieważ przechodnie są o tej porze bardziej czujni. Nie wybieraj miejsc, przez które dziennie przechodzi 250 osób lub więcej. Unikaj miejscowości mniejszych niż 15 000 mieszkańców - ludzie dobrze tam wiedzą, jak powinien wy-glądać bankomat, i mogą zauważyć produkt Cha0.

Mimo żartobliwego marketingu Cha0 zawsze jasno dawał do zrozumienia swemu przyjacielowi Master Splyntrowi, że jest poważnym przestępcą, nie-obawiającym się używać przemocy w realnym świecie, aby bronić swego war-tego wiele milionów dolarów biznesu. Teraz tego dowiódł. Mert „Kier” Ortac należał do jego organizacji Crime Enforcers, do momentu kiedy poszedł do tureckiej telewizji, by wygadać się na temat działalności Cha0. Po kilku wywiadach zniknął. Kiedy trochę później znowu się pojawił, opowiedział wstrzą-

sającą historię o uprowadzeniu i pobiciu go przez Cha0 i jego pomagierów.

Teraz Cha0 potwierdził opowieść, zamieszczając zdjęcie porwanego na DarkMarket jako

ostrzeżenie dla innych.

Zdjęcie dostarczyło dowodu na żywione od dawna podejrzenie FBI, że komputerowy półświatek przestępczy opanowuje przemoc. Biorąc pod uwagę wpływające co rok do półświatka setki milionów dolarów, wydawało się nie-uniknione, że carderzy sięgną po brutalne metody tradycyjnej przestępczości zorganizowanej, aby powiększyć lub zabezpieczyć swe nielegalne dochody.

Gdy Max siedział bezpiecznie zamknięty w izbie zatrzymań w Ohio, DarkMarket mógł się swobodnie rozwijać, a Mularski osaczać grube ryby 253

z forum - wśród nich także Cha0. Nad przygwożdżeniem producenta skimmerów pracował z Mularskim turecki detektyw zajmujący się cyberprzestępczo-

ścią, który spędził trzy miesiące na stypendium w NCFTA.

W zeszłym roku agent wysłał Cha0 dwa lekkie pecety jako prezent, stawiając pierwszy krok w śledztwie. Cha0 skierował przesyłkę do pomagierów ze swej organizacji, którzy zostali szybko wzięci pod nadzór tureckiej policji.

Dzięki temu dotarli do Cagataya Evyapana, inżyniera elektronika posiadające-go już bogatą kryminalną przeszłość - jej szczegóły zgadzały się z biografią Cha0, którą prywatnie opowiedział on Mularskiemu.

Policja zgłosiła się do kilku międzynarodowych firm kurierskich i przedstawiła im w ogólnych zarysach przedsięwzięcia Cha0. Jedna z nich zidentyfikowała pewną przesyłkę ze skimmerami z Istambułu do Europy, wskazując znanego członka organizacji Cha0 jako nadawcę.

W ten sposób policja uzyskała dowód, którego potrzebowała. 5 września pięciu policjantów w kamizelkach kuloodpornych weszło do domu Cha0 na obrzeżach Istambułu. Wpadli jak burza z wycelowanymi karabinami i po chwili rzucili na ziemię Cha0 i jego wspólników.

Znaleźli u niego dobrze wyposażone elektroniczne laboratorium i linię produkcyjną ze składnikami pieczołowicie porozkładanymi na podstawkach i w pojemnikach. Jakieś dziesięć włączonych komputerów stało na biurkach. Cha0

miał zupełnie te same urządzenia do podrabiania kart, którymi szczyciła się fabryka Chrisa Aragona, a także wielkie kartonowe pudła, gdzie znajdowało się około 1000 skimmerów i 2000 PIN-padów - wszystkie oczekiwały na wysyłkę.

Z notatek Cha0 wynikało, że cztery kartony już dotarły do Stanów.

Policjanci wyprowadzili Evyapana w kajdankach - ten wysoki, dobrze zbudowany mężczyzna z krótko przyciętymi włosami, ubrany w czarny T-shirt z kostuchą był twarzą zorganizowanej przestępczości w epoce Internetu.

Cha0 był ostatnim celem tajnej operacji Mularskiego; inni kluczowi gracze z DarkMarket już zostali zdjęci. Markus Kellerer, Matrix001, został aresztowany 254

w Niemczech w maju 2007 roku i spędził już cztery miesiące w więzieniu o zaostrzonym rygorze. Renukanth „JiLsi” Subramaniam, pochodzący ze Sri Lanki obywatel brytyjski, wpadł w Londynie w czerwcu 2007 roku, po tym jak detektywi z Serious Organised

Crime Agency in Britain wyśledzili kafejkę internetową Java Bean, którą wykorzystywał jako biuro, dopasowując jego pojawianie się tam z postami JiLsiego na DarkMarket i jego rozmowami z Master Splyntrem. Wspólnik JiLsiego, sześćdziesięciosiedmioletni John

„Devilman" McHugh, został złapany w tym samym czasie. W domu starszego obywatela policja znalazła fabrykę podrabianych kart kredytowych.

W Turcji sześciu członków gangu Cha0 zostało oskarżonych wraz z nim. Z

pomocą Mularskiego w obławie wpadł także Erkan „Seagate" Findikoglu, członek DarkMarket, który zajmował się wielkimi operacjami wyciągania pieniędzy w stylu Kinga Arthura. Findikoglu był odpowiedzialny za kradzież co najmniej dwóch milionów dolarów z amerykańskich banków i kas pożyczkowych - z czego udało się odzyskać milion w gotówce podczas jego aresztowania. 27 członków gangu Seagatea zostało oskarżonych w Turcji, a FBI schwytało w Stanach sześciu pracujących dla niego mułów.

Kiedy Cha0 i Seagate trafili za kratki, praca Mularskiego była skończona -

dwa lata prowadzenia przez niego DarkMarket zaowocowały teraz 56 areszto-waniami w czterech krajach. We wtorek 16 września 2008 roku napisał post formalnie ogłaszający zamknięcie tej strony. Jako hołd dla historii i kultury cardingowego świata agent FBI nawiązał do legendarnego oświadczenia Kinga Arthura zamykającego CarderPlanet kilka lat wcześniej. „Dobrego dnia, sza-nowni i drodzy członkowie forum" - zaczął.

Nadeszła pora, by przekazać wam złą wiadomość – forum powinno zostać zamknięte. Tak, naprawdę to mam na myśli.

W ciągu ostatniego roku straciliśmy kilku adminów z różnych forów: Icemana z Carders Market; JiLsi i Matrix001 zniknęli, a teraz Cha0

z DM. Widać wyraźnie, że to forum za bardzo przyciąga uwagę światowych służb…

Ja sam wolę wyjść jak King Arthur niż jak Iceman. Podczas gdy Iceman postanowił, że jedyne, co zrobi, to zmieni swój nick na Aphex i będzie nadal prowadził CM, King Arthur zamknął CarderPlanet i zniknął

w mroku. Historia pokazała, że Iceman popełnił fatalny błąd. Ja nie mam zamiaru go powtórzyć.

Mularski planował zachować tożsamość Master Splyntra uśpioną, ale żywą: miał dobrze ugruntowaną podziemną legendę, po którą mógł sięgnąć, jeśli kiedykolwiek będzie jej potrzebował w przyszłych śledztwach. Tak się jednak nie stało. Tydzień po tym jak DarkMarket pogrążył się w mroku, reporter z Südwestrundfunk, publicznego radia z południowych Niemiec, dotarł do dokumentów procesowych ze sprawy Matriksa, które ujawniły podwójne życie Mularskiego. Prasa amerykańska podchwyciła tę historię. Teraz 2500 człon-ków DarkMarket dowiedziało się, że prowadzili interesy na stronie-pułapce i że Iceman miał we wszystkim rację.

Trzy dni po pojawieniu się historii w Stanach Mularski znalazł na ICQ wiadomość do Master Splyntra czekającą na jego komputerze. Wysłał ją TheUnknown, cel z Wielkiej Brytanii, któremu udało się uciec po nalocie brytyjskiej policji. „Ty pierdolona kupo

gówna. Skurwysynu. Myślałeś, że potrafisz mnie złapać. Ha, ha, ha. Jebany żółtodziób. Nie masz pojęcia, gdzie jestem”.

„Jeśli chcesz się ujawnić, daj mi znać - odpisał Mularski. - To będzie lepsze niż oglądanie się za siebie przez resztę życia”.

TheUnknown ujawnił się tydzień później.

Mularski niemal poczuł ulgę, po tym jak jego tajna tożsamość została od-kryta; przez dwa lata laptop był jego nieodłącznym towarzyszem - nawet na wakacjach ciągle rozmawiał przez Internet z carderami. Część tych kontaktów sprawiała mu radość - budowanie przyjaźni online z niektórymi ze swych ce-lów, drażnienie innych i kpienie z nich. Master Splyntr mógł powiedzieć 256

przestępcom to, na co szanowany agent FBI nigdy by sobie nie pozwolił.

Nawet jeśli Mularski chciał powrócić do swego życia, wymagało to jeszcze czasu. Prawie miesiąc po zamknięciu DarkMarket ciągle walczył z nieokreślonym niepokojem. Stało przed nim jeszcze jedno wyzwanie, któremu musiał

sprostać. Nauczyć się, jak nie być Master Splyntrem.

ROZDZIAŁ 35

Wyrok

Max górował nad strażnikami sądowymi, kiedy wprowadzili go do sali sądowej w Pittsburghu na odczytanie wyroku. Miał na sobie luźny pomarańczowy więzienny uniform, włosy przycięte krótko i starannie.

Strażnicy zdjęli mu kajdanki z rąk, po czym usiadł obok swego adwokata z urzędu. Kilku reporterów rozmawiało po jednej stronie galerii, a po drugiej dyskutowało dokładnie tylu federalnych. Za nimi stały długie drewniane ławy, w większości puste: żadnych przyjaciół ani krewnych, nie było też Charity; powiedziała już Maksowi, że nie ma zamiaru na niego czekać.

Był 12 lutego 2010 roku, od chwili gdy Max został aresztowany w swej kryjówce, minęło dwa i pół roku. Pierwszy miesiąc spędził w okręgowym więzieniu w Santa Clara, codziennie prowadząc z Charity długie rozmowy telefoniczne bardziej intymne niż jakakolwiek z tych, które mieli, kiedy był zaanga-

żowany w przestępczą działalność. Strażnicy w końcu wsadzili go do samolotu i zabrali do izby zatrzymań w Ohio, gdzie Max pogodził się ze swym uwięzieniem, wyzbyty teraz gniewu, jaki towarzyszył mu podczas poprzednich odsia-dek, biorącego się z poczucia własnej wyższości i przekonania o tym, że 258

słuszność jest po jego stronie. W więzieniu znalazł nowych przyjaciół: geeków takich jak on. Zaczęli grać w Dungeons and Dragons.

Do końca roku wszystkie tajemnice Maksa zostały ujawnione. Śledczym z CERT-u wystarczyły dwa tygodnie na znalezienie klucza do szyfru w obrazie pamięci RAM jego komputera. W czasie jednego z jego pobytów w sądzie prokurator Luke Dembosky wręczył obrońcy Maksa świstek papieru z jego hasłem: „Jeden człowiek może robić różnicę!”.

Przez całe lata Max używał swego zaszyfrowanego twardego dysku jako rozszerzenia własnego mózgu, przechowując tam wszystko, co znalazł, i wszystko, co robił. Ujawnienie tego przez federalnych miało katastrofalne skutki dla jego prawnej przyszłości, ale poza tym odczuł to jak pogwałcenie intymności. Przedstawiciele władzy byli w jego głowie, czytali w jego myślach i wspomnieniach. Kiedy wrócił do celi, płakał w poduszkę.

Mieli wszystko: pięć terabajtów narzędzi hakerskich, phishingowe maile, *dossier,* które zebrał na temat swych internetowych przyjaciół i wrogów, zapi-ski dotyczące jego zainteresowań i działań i 1,8 miliona kont kart kredytowych z ponad tysiąca banków. Władze dotarły do tego: Max ukradł 1,1 miliona kart z terminali. Reszta pochodziła w większości od carderów, których zhakował.

To dawało 13 kilometrów danych z pasków magnetycznych i federalni byli przygotowani do pociągnięcia Maksa do odpowiedzialności za każdy milimetr.

Władze w tajemnicy przetransportowały Chrisa do Pittsburgha, gdzie całymi tygodniami go przesłuchiwano, podczas gdy firmy wydające karty kredytowe obliczały oszukańcze

obciążenia kart Maksa, dochodzące do zdumiewającej sumy 86,4 miliona dolarów strat.

Zyski hakera były o wiele mniejsze: Max powiedział władzom, że na swych przestępstwach zarobił poniżej 1 miliona, z czego większość przepuścił na opłaty za wynajem mieszkania, jedzenie, taksówki i gadżety. Władze znalazły około 80 000 dolarów na koncie Maksa w WebMoney. Ale federalne wytyczne wyroku w wypadkach kradzieży opierają się na szkodach ofiar, a nie zyskach przestępców, więc Max mógłby zostać oskarżony za przestępstwa popełnione 259

przez Chrisa, carderów, którzy kupowali zrzuty od Digitsa i Generousa, i potencjalnie także te popełnione przez carderów, których Max zhakował. Jeśli dodać do tego kryminalną kartotekę Maksa, 86 milionów przełoży się na wyrok od trzydziestu lat do dożywocia, bez możliwości starania się o wcześniejsze zwolnienie.

Zagrożony spędzeniem kilku dziesięcioleci w więzieniu Max zaczął współ-

pracować. Mularski zabierał go na długie sesje przesłuchań dotyczących przestępstw hakerskich. W czasie jednej z nich, po tym jak informacje, jakoby DarkMarket był policyjną pułapką, dostały się do prasy, Max przeprosił Mularskiego za swe próby obnażenia Master Splyntra. Mularski usłyszał nutkę szcze-rości w głosie dawnego wroga i przyjął przeprosiny.

Po trwających rok negocjacjach adwokat Maksa dogadał się z władzami -

będą rekomendować sędziemu trzynaście lat więzienia. W lipcu 2009 roku oskarżony przyznał się do winy.

Umowa nie była wiążąca dla sądu; teoretycznie Max mógłby z miejsca zostać uniewinniony, skazany na dożywocie lub dostać jakikolwiek wyrok po-między tymi dwiema możliwościami. Dzień przed ogłoszeniem wyroku Max napisał czterostronicowy list do mianowanego przez prezydenta Forda 70-letniego wówczas sędziego Maurice'a Cohilla juniora, który został prawnikiem, zanim jeszcze Max się urodził.

„Nie wierzę w to, że kolejne lata spędzone przeze mnie w więzieniu komukolwiek pomogą - napisał Max. - Nie sądzę, aby to było konieczne, ponieważ chcę tylko pomóc. Nie zgadzam się z powszechnymi szacunkami wytycznych wyroku. Tak się nieszczęśliwie składa, że grozi mi przerażający wyrok, w po-równaniu z którym nawet 13 lat wydaje się »dobre«. Ale zapewniam pana, że to jest gruba przesada, jestem przysłowiowym leżącym, którego się kopie. To oznacza, że planuję jak najlepiej przeżyć czas, który mi jeszcze pozostał na tej ziemi, czy to w więzieniu czy gdzie indziej".

Kontynuował: „Żałuję wielu rzeczy, ale myślę, że moim podstawowym błę-

dem było to, że straciłem poczucie odpowiedzialności, które wiąże się z by-ciem członkiem społeczeństwa. Mój przyjaciel powiedział mi kiedyś, żebym 260

zachowywał się tak, jak gdyby każdy przez cały czas widział, co robię. To pewny sposób na uniknięcie angażowania się w nielegalne postępowanie, ale myślę, że w to nie uwierzyłem, ponieważ kiedy byłem niewidzialny, całkiem zapomniałem o tej radzie. Teraz wiem, że nie można być niewidzialnym i że takie myślenie jest niebezpieczne". Max patrzył z wystudiowanym spokojem, kiedy jego adwokat wstał, aby omówić z oskarżeniem ostatnie szczegóły, a personel sądowy zajął się przygotowaniami do

odczytania wyroku, testując mikrofony i przekładając dokumenty. O 10.30 drzwi się otworzyły. „Proszę wstać!”

Sędzia Cohill o pomarszczonej twarzy z gładko przyciętą śnieżnobiałą bródką zasiadł w ławie, patrzył na salę sądową przez okrągłe okulary, zapowiadając ogłoszenie wyroku Maksa Butlera (pod tym nazwiskiem Max został

oskarżony). Przeczytał Maksowi wytyczne wyroku, trzynaście lat do dożywocia, a następnie słuchał, kiedy prokurator Dembosky wystąpił o złagodzenie wyroku. Max znacząco pomógł władzom, powiedział, i zasługuje na wyrok niższy, niż przewidują wytyczne.

To, co nastąpiło później, mogłoby być ogłoszeniem nagrody, a nie wyroku.

Adwokat, prokurator i sędzia na zmianę wychwalali komputerowe zdolności Maksa i jego oczywistą skruchę. „Jest niezwykle bystrym komputerowym ekspertem samoukiem” - powiedział federalny publiczny obrońca Michael Novara, choć także człowiekiem, który zorganizował „złamanie komputerowych zabezpieczeń na wielką skalę”.

Dembosky, specjalista od przestępstw komputerowych i siedmioletni weteran pracy w biurze prokuratora krajowego, nazwał Maksa „niezwykle inteli-gentnym, elokwentnym i utalentowanym”. Uczestniczył w kilku przesłucha-niach Maksa i jak niemal każdy, kto znał go w realnym życiu, polubił hakera.

„Jest niemal naiwny i optymistyczny w swym widzeniu świata” - stwierdził.

Współpraca Maksa, dodał, jest powodem tego, że żądają tylko trzynastu lat, zamiast „astronomicznego” wyroku. „Wierzę w to, że jest mu bardzo przykro”.

Max nie miał wiele do dodania. „Zmieniłem się”, powiedział. Hakowanie już go nie pociągało. Poprosił sędziego Cohilla, by zadał mu kilka pytań. Sę-

dzia nie musiał tego robić. Oznajmił, że jest pod wrażeniem listu Maksa oraz 261

listów, które dostał od Charity, Tima Spencera, matki, ojca i siostry Maksa. Był

zadowolony z tego, że oskarżony wyraził skruchę. „Nie sądzę, bym musiał

dawać ci wykład na temat problemów, których przysporzyłeś swoim ofiarom”.

Cohill już napisał sentencję wyroku. Czytał ją głośno. Trzynaście lat wię-

zienia. Max zostanie również obciążony kosztami zadośćuczynienia w wysokości 27,5 miliona dolarów, obliczonymi na podstawie strat, jakie banki poniosły w związku z ponownym wydaniem 1,1 miliona kart, których dane Max ukradł z terminali płatniczych. Po zwolnieniu z więzienia przez pięć lat będzie pod dozorem sądowym i w tym czasie będzie mógł korzystać z Internetu jedynie w pracy i w celach edukacyjnych.

- Powodzenia - powiedział do Maksa.

Skazany wstał, na jego twarzy nie było widać żadnych uczuć, i pozwolił, by straż sądowa założyła mu kajdanki na ręce, które trzymał za sobą, a potem wyprowadziła go do drzwi na tyłach sali sądowej, wiodących do aresztu. Wraz z zaliczonym czasem odsiadki i przy dobrym sprawowaniu Max wyjdzie na wolność tuż przed Bożym Narodzeniem w 2018 roku.

Nadal pozostawało mu jeszcze prawie dziewięć lat za kratami. W tym czasie był to najwyższy wyrok kiedykolwiek wydany w sprawie przeciw hakerowi.

ROZDZIAŁ 36

Pokłosie

Zanim Max usłyszał wyrok, Secret Service zidentyfikowała tajemniczego amerykańskiego hakera, który wprowadził Maksika do kręgu czołowych światowych carderów. Groziła mu kara, przy której wyrok Maksa wyglądał jak man-dat drogowy.

Wielki przełom w sprawie nastąpił w Turcji. W lipcu 2007 roku tamtejsza policja dowiedziała się od Secret Service, że Maksik, dwudziestopięcioletni Maksym Jastremski, przyjechał nad Bosfor na wakacje. Tajna agentka Secret Service ściągnęła go do nocnego klubu w Kemer, gdzie policja aresztowała Jastremskiego i skonfiskowała jego laptop.

Niestety, twardy dysk tego komputera był zaszyfrowany w sposób niemoż-

liwy do złamania, tak jak wtedy gdy Secret Service próbowała się do niego włamać rok wcześniej w Dubaju. Ale po kilku dniach w tureckim więzieniu Maksik wydał siedemnastoliterowe hasło. Policja przekazała je wraz z kopią twardego dysku Secret Service, która zaczęła zgłębiać jego zawartość, szczególnym zainteresowaniem obdarzając logowania Maksika zapisane w jego rozmowach na ICQ.

Jeden z rozmówców zdecydowanie się wyróżniał: użytkownik ICQ

201679996 mógł być widziany, jak pomagał Ukraińcowi w hakerskich atakach na sieć restauracji Dave & Busters i omawiał z nim wcześniejsze wielkie włamania, dzięki którym Maksik pojawił się na mapie. Agenci sprawdzili numer ICQ i uzyskali adres mailowy używany przy pierwszej rejestracji konta: soup-nazi@efnet.ru.

SoupNazi było imieniem, które agenci już wcześniej słyszeli - w 2003 roku, kiedy aresztowali Alberta Gonzaleza.

Gonzalez był informatorem, który zwabił carderów z Shadowcrew do inwi-gilowanego VPN, co doprowadziło do 21 aresztowań w ramach operacji „Firewall” - legendarnej klęski zadanej cardingowemu półświatkowi przez Secret Service. Ale kilka lat przed tym jak dał się poznać na Shadowcrew jako Cumbajohnny, Gonzalez używał zainspirowanego serialem *Kroniki Seinfelda* nicka SoupNazi na IRC-u.

Carder zdrajca, który umożliwił przeprowadzenie operacji „Firewall”, kontynuował przestępczą działalność, dokonując największej kradzieży tożsamości w historii Stanów Zjednoczonych.

Miesiąc po „Firewallu” pozwolono Gonzalezowi na opuszczenie New Jersey i powrót do domu, do Miami, gdzie rozpoczął drugi etap swej hakerskiej kariery. Przybrał pseudonim Segvec i podawał się za Ukraińca, zakotwiczając się na wschodnioeuropejskim forum Mazafaka. Pod nagłówkiem „Operacja Get Rich or Die Tryin”’ (Zdobądź bogactwo lub zgiń, próbując) - tytuł płyty 50

Centa i motto Maksika na Shadowcrew - pracował nad stworzeniem obracają-

cego milionami dolarów gangu cyberzłodziei, który przysporzył strat dziesiąt-kom

milionów Amerykanów.

8 maja 2008 roku federalni zrobili obławę na Gonzaleza i jego amerykań-

skich wspólników. Licząc na złagodzenie wyroku, Gonzalez ponownie zgodził

się na współpracę, ujawniając agentom klucz do szyfru na swym twardym dysku i dając im informacje o całym swym gangu. Przyznał się do włamań do TJX, OfficeMax, DSW, Forever 21 i Dave & Buster's, a także do pomocy hakerom z Europy Wschodniej we wniknięciu do sieci sklepów spożywczych 264

Hannaford Bros., sieci bankomatów 7-Eleverís, Boston Market i firmy produkującej karty kredytowe Heartland Payment Systems, z której wyciekło blisko 130 milionów kart. Był to bardzo dochodowy biznes dla tego hakera. Gonzalez narysował Secret Service plan kryjówki na podwórku za domem swoich rodziców, gdzie schował ponad milion dolarów w gotówce. Władze zarządziły kon-fiskatę pieniędzy, bmw 2006 i pistoletu Glock 27 z amunicją.

Gonzalez zbudował swój gang, werbując niewykorzystane hakerskie talenty

- niegdysiejszych nastoletnich hakerów, którzy mieli problemy ze znalezieniem sobie miejsca w świecie białych kapeluszy. Wśród nich był Jonathan

„C0mrade" James, który zhakował NASA jako nastolatek i otrzymał przełomowy wyrok sześciu miesięcy poprawczaka w tym samym tygodniu, kiedy Max Vision przyznał się do zhakowania Pentagonu w 2000 roku. Po krótkim podmuchu sławy - i wywiadzie we „Frontline" w PBS - James odszedł w cień, żyjąc spokojnie w Miami, w domu odziedziczonym po matce.

Potem, prawdopodobnie w 2004 roku, zaczął pracować z Gonzalezem i wspólnikiem Christopherem Scottem. Władze są przekonane, że James i Scott, by dostać się do gangu Maksika, dokonali jednych z najwcześniejszych kradzieży pasków magnetycznych, włamując się do WiFi OfficeMaxs z parkingu przed sklepem i kradnąc tysiące danych z kart i zaszyfrowanych PIN-ów. Ci dwaj prawdopodobnie dostarczyli dane Gonzalezowi, który wraz z innym hakerem zajął się odszyfrowaniem kodów PIN. Firmy oferujące karty kredytowe wydały później ponownie, w odpowiedzi na atak, jakieś 200 000 kart kredytowych.

Ze wszystkich hakerów to Jonathan James zapłacił najwyższą cenę w po-gromie carderów po Shadowcrew. Po nalocie w maju 2008 roku James był

przekonany, że Secret Service będzie próbowała zwalić wszystkie włamania Gonzaleza na niego, wykorzystując jego niesławną przeszłość informatora. 18

maja dwudziestoczterolatek wszedł pod prysznic z pistoletem i zastrzelił się.

„Nie wierzę w system »sprawiedliwości« - napisał w liczącym pięć stron li-

ście samobójczym. - Być może to, co zrobię dzisiaj, i ten list będą mocniejszym 265

przekazem dla opinii publicznej. Całkowicie straciłem kontrolę nad tą sytuacją i to jest jedyny sposób na jej odzyskanie".

W marcu 2010 roku Gonzalez został skazany na dwadzieścia lat więzienia.

Jego amerykańscy wspólnicy dostali wyroki od dwóch do siedmiu lat. W Turcji Maksik został oskarżony o zhakowanie tureckich banków i skazany na trzydzieści lat.

Od momentu aresztowania Maksa w półświatku pojawiły się nowe sposoby oszukiwania. Najbardziej niebezpieczne wykorzystywały wyspecjalizowane trojany stworzone po to, by kraść hasła bankowości internetowej i przeprowadzać przelewy bankowe z konta ofiary prosto przez swój komputer. Złodzieje znaleźli genialne rozwiązanie problemu, który dręczył Chrisa Aragona: jak dostać się do pieniędzy. Werbują zwykłych konsumentów jako nieświadomych praczy pieniędzy, kusząc fałszywymi możliwościami pracy w domu, która polega na przyjmowaniu przelewów i depozytów pieniężnych, a potem wysy-

łaniu gotówki do Europy Wschodniej za pośrednictwem Western Union. Sza-cuje się, że w 2009 roku, kiedy ten rodzaj oszustwa się rozpowszechnił, banki i ich klienci stracili 120 milionów dolarów z powodu tych ataków, których najczęstszymi celami były małe firmy.

Tymczasem ciągle trwającą sprzedażą zrzutów zajął się nowy krąg sprzedawców, nieróżniący się od starego - Mr BIN, Prada, Vitrium, The Thief.

Jednak policja odniosła pewne trwałe zwycięstwa. Dotychczas nie pojawiło się żadne znaczące anglojęzyczne forum, które zastąpiłoby Carders Market i DarkMarket, a carderzy ze wschodniej Europy stali się bardziej zamknięci i czuli na punkcie bezpieczeństwa. Wielcy gracze przenieśli się do zaszyfrowanych serwerów czatowych, do których można się dostać tylko na zaproszenie.

Rynek istnieje, ale poczucie bezkarności carderów zostało zburzone, a ich handel jest okupiony paranoicznym lękiem i brakiem zaufania, w dużej mierze dzięki FBI, Secret Service, ich międzynarodowym partnerom i cichej pracy poczty.

Zasłona tajemnicy, która kiedyś chroniła zarówno hakerów, jak i korporacje, w większej części zniknęła, kiedy policja przestała ulgowo traktować firmy, by chronić je przed odpowiedzialnością za ich słabe zabezpieczenia. Wię-

cej niż jeden z celów zhakowanych przez Gonzaleza został upubliczniony po raz pierwszy w czasie jego procesu.

Ostatecznie pułapka Mularskiego na DarkMarket dowiodła, że federalni nie muszą iść z przestępcami do łóżka, by ich aresztować.

Wszystkie najgorsze momenty w wojnie z komputerowym półświatkiem pojawiły się na skutek działań informatorów. Brett „Gollumfun” Johnson, konfident, który przez krótki czas był administratorem Carders Market, zmienił

operację „Anglerphish” prowadzoną przez Secret Service w cyrk, robiąc na boku oszustwa na zwrotach podatku. Albert Gonzalez dostarcza najbardziej jaskrawego przykładu. Po operacji „Firewall” Secret Service płaciła mu roczną pensję w wysokości 75 000 dolarów, nawet kiedy przeprowadzał jedne z największych w historii hakerskich ataków mających na celu zdobycie danych kart kredytowych.

Kradzieże danych z pasków magnetycznych, które nastąpiły po upadku Shadowcrew, doprowadziły do procesów cywilnych. TJX zapłaciło 10 milionów dolarów w wyniku pozwu złożonego przez prokuratorów generalnych 41 stanów i kolejne 40 milionów

wydającym karty Visa bankom, które ucierpiały z powodu kradzie-

ży. Banki i kasy pożyczkowe złożyły pozwy przeciw Heartland Payment Systems w związku z wielkim włamaniem do firmy przeprowadzającej transakcje.

Ataki Gonzaleza zrobiły także wyłom w podstawowych zabezpieczeniach przeciw włamaniom, które stosowała cała branża kart kredytowych: tak zwany Payment Card Industry lub PCI Data Security Standard (Standard Bezpieczeństwa Danych Przemysłu Kart Płatniczych), dyktujący kroki, jakie kupcy i ci, co wydają karty, muszą podjąć, aby zabezpieczyć systemy operujące danymi kart kredytowych. Heartland otrzymał certyfikat PCI, zanim padł ofiarą włamań, a Hannaford Brothers uzyskali certyfikat bezpieczeństwa, nawet kiedy hakerzy byli 267

w ich systemach, kradnąc dane kart kredytowych.

Kiedy zaczął opadać kurz po atakach Gonzaleza na wielką skalę, zaczęły wychodzić na jaw mniejsze, lecz o wiele liczniejsze ataki na terminale płatnicze w restauracjach. Siedem restauracji w Missisipi i Luizjanie, które zostały zaatakowane, zorientowało się, że używały tych samych terminali - Aloha POS

- które kiedyś były ulubionymi celami Maksa. Restauracje złożyły pozew przeciw producentowi i firmie Computer World z Luizjany, która sprzedawała terminale przypuszczalnie instalujące oprogramowanie do zdalnego dostępu pcAnywhere, na wszystkich maszynach, a potem ustawiała na nich hasło „komputer”.

U źródła wszystkich tych włamań tkwi jeden systemowy błąd bezpieczeń-

stwa, dokładnie o długości 8,57 centymetra. Paski magnetyczne kart kredytowych są technologicznym anachronizmem, reliktem z epoki ośmiościeżkowej taśmy, i dzisiaj Stany Zjednoczone są niemal osamotnione w podtrzymywaniu tej dziury z zabezpieczeniach. Ponad sto innych krajów na całym świecie, głównie w Europie i Azji, a także Kanada i Meksyk, wprowadziły lub zaczyna-ją wprowadzać bezpieczniejszy system zwany EMV lub „czip-i-PIN”.

Zamiast polegać na biernym przechowywaniu paska magnetycznego, karty czip-i-PIN mają wmontowany w plastik mikroczip, używający zaszyfrowanego uzgodnienia parametrów transmisji danych, aby uwierzytelnić się w terminalu, a potem w serwerze przeprowadzania transakcji. System nie pozostawia nic, co haker mógłby ukraść - włamywacz siedzący na kablu może śledzić całą transakcję i mimo to nie być w stanie sklonować karty, ponieważ sekwencja uzgodnienia parametrów transmisji danych zmienia się za każdym razem.

Białe kapelusze opracowały ataki przeciw kartom czip-i-PIN, ale nie pojawiło się nic, co trafiłoby na masowy rynek zrzutów, który nadal dzisiaj istnieje.

Jak do tej pory największą słabością systemu jest to, że umożliwia on transakcje z użyciem paska magnetycznego. Dla Amerykanów podróżujących za granicę lub turystów odwiedzających USA jest to krok wstecz. Amerykańskie banki i firmy oferujące karty kredytowe odrzuciły czip-i-PIN z powodu 268

gigantycznych kosztów wymiany setek tysięcy terminali sprzedaży na nowe urządzenia. Ostatecznie instytucje finansowe zdecydowały, że straty, które ponoszą z tytułu oszustw,

są do przyjęcia, nawet jeśli tacy hakerzy jak Iceman będą grasowali w ich sieciach.

Epilog

W męskim więzieniu w Orange County Chris Aragon jest samotny, czuje się porzucony przez swych przyjaciół i rozdzierany zmartwieniem, że jego dzieci dorastają bez niego. W listopadzie 2009 roku Clara wystąpiła o rozwód, pragnąc uzyskać opiekę na dwojgiem dzieci. Kochanka Chrisa wystąpiła o alimen-ty.

Chris studiuje *Bhagawadgitę* i ma pełnoetatową pracę jako pełnomocnik więźniów, pomagając kilkuset osadzonym w sprawach prywatnych, zajmując się skargami medycznymi i problemami z więziennym personelem. Jego obrońca gra na czas, nieustannie przedłużając proces, który w wypadku prze-granej nadal grozi Chrisowi wyrokiem od 25 lat do dożywocia. Po tym jak historia Chrisa została opisana w magazynie „Wired" w artykule o Maksie, do Chrisa zwrócili się scenarzysta i producent z Hollywood, ale osadzony nie odpowiedział. Jego matka zasugerowała, by wziął agenta.

Max został skierowany do FCI Lompoc, więzienia o niskim rygorze, godzinę drogi na północ od Santa Barbara w Kalifornii. Chciałby wykorzystać ten czas na zdobycie dyplomu z fizyki lub matematyki - i dokończyć swą uniwersytecką edukację przerwaną dekadę wcześniej w Boise.

271

Zrobił myślowy remanent i jest skonsternowany tym, że mimo wszystko ciągle tkwią w nim te same impulsy, które zaprowadziły go do hakerskiego życia. „Nie wiem, jak się ich pozbyć; jedyne, co przychodzi mi do głowy, to ignorować je - powiedział w wywiadzie udzielonym w więzieniu. - Naprawdę wierzę, że się poprawiłem. Ale nie wiem, co się zdarzy później".

To wyznanie może się wydawać dziwne - przyznanie się, że cząstki jego osobowości, które sprawiły, że wylądował za kratkami, ciągle głęboko w nim tkwią. Ale nowa samoświadomość Maksa daje nadzieję na prawdziwą przemianę. Jeśli ktoś urodził się hakerem, nawet całe lata spędzone w więzieniu tego nie zmienią. Żadna terapia, nadzór sądowy ani warsztaty więzienne nie mogą tu pomóc. Max musi zmienić się sam - nauczyć się panować na swym postępowaniem i skierować pożyteczne elementy swej natury na coś produk-tywnego.

W tym celu Max zgłosił się jako wolontariusz, by pomagać władzom w czasie odbywania kary, broniąc amerykańskich sieci i być może przeprowadzając kontrataki na zagranicznych wrogów. W piśmie zatytułowanym „Dlaczego USA potrzebują Maksa" spisał cały zestaw oferowanych usług. „Mógłbym przeniknąć do chińskich sieci wojskowych i ich sprzymierzeńców - zasugerował. - Mógłbym zhakować Al-Kaidę". Jest pełen nadziei, że mógłby się przysłużyć rządowi na tyle, by uzyskać skrócenie wyroku od swego sędziego.

To długa droga i jak na razie federalni nie skorzystali z jego oferty. Ale miesiąc po ogłoszeniu wyroku Max zrobił malutki krok w tym kierunku. Keith Mularski załatwił mu wykład w NCFTA dla chętnego audytorium składającego się z wysokich rangą policjantów, studentów, ekspertów od bezpieczeństwa z instytucji finansowych i

korporacji oraz pracowników naukowych z Carnegie Mellon.

Mularski załatwił mu przepustkę z więzienia, by mógł przyjechać. I przez godzinę lub dwie Max Vision znowu był białym kapeluszem.

Przypisy

Prolog

s. 11 *Taksówka zatrzymała się…:* wywiad z Maksem Visionem.

l. Klucz

s. 15 *Kiedy tylko pikap wtoczył się na krawężnik:* wywiad z przyjacielem Maksa Timem Spencerem. Konfrontacja została również opisana mniej szczegółowo przez Kimi Mack, byłą żonę Maksa. Mimo że Max mógł odstraszać napastników, nigdy nie był zmuszony do fizycznej konfrontacji z nimi.

s. 16 *Rodzice Maksa pobrali się w młodym wieku: Stan Idaho przeciw Maksowi Butlerowi*, 1991. District Court of the Fourth Judicial District, Ada County, sprawa nr 17519.

s. 16 *Robert Butler był weteranem wojny w Wietnamie: Stan Idaho przeciw Maksowi Butlerowi* i wywiady z Maksem.

s. 16 *Weather Channel i filmy przyrodnicze:* wywiady z Kimi Winters i Maksem. Rodzice Maksa nie zgodzili się na rozmowę.

s. 16 *relaksu i napadów szału:* wywiady z Timem Spencerem i „Amy" byłą dziewczyną Maksa. Problemy emocjonalne Maksa z tego okresu znajdują również odbicie w aktach sądowych sprawy *Stan Idaho przeciw Maksowi Butlerowi.* Max przyznaje, że głęboko przeżył rozwód rodziców.

s. 17 *Pewnego dnia wynurzył się ze swego domu:* wywiad z Timem Spencerem. Max przyznaje, że takie wydarzenie miało miejsce, ale twierdzi, że rozpalił ogień na polu sąsiadującym z domem Spencerów.

s. 17 *Geekowie z Meridian znaleźli pęk kluczy:* relacja o incydencie z głównym kluczem pochodzi z wywiadów z Timem Spencerem. Zapisy sądowe potwierdzają wyrok sądu dla 273

nieletnich. Max przyznał się do wejścia do szkoły i kradzieży chemikaliów, nie chciał jednak ujawnić szczegółów dotyczących tego, co wydarzyło się w budynku. John, który towarzyszył

Maksowi w czasie włamania, ale nie został oskarżony, odmówił komentarza.

s. 18 *Max stał się „Lordem Maksem":* Max opowiedział o swojej nieprzyjemnej rozmowie z Secret Service w wywiadzie. Odwołanie do niej znajduje się także w napisanym przez Maksa liście, który został dołączony do akt procesu *Stan Idaho przeciw Maksowi Butlerowi.*

2, Śmiercionośna broń

s. 21 *To jest pokój rekreacyjny!!!!:* Don Mitchell, *From MUDs to Virtual Worlds*, Microsoft Social Computing Group, 23 marca 1995.

s. 21 *300 000 hostujacych komputerów,* wiele źródeł, m.in. Colin Barras, *Illuminating the net's Dark Ages,* BBC News, 23 sierpnia 2007.

s. 22 Na *skutek nalegań:* wydarzenia związane z wyrokiem Maksa za napaść zostały zaczerpnięte ze stenogramów i innych akt sprawy *Stan Idaho przeciw Maksowi Butlerowi,* a także z wywiadów z Maksem i „Amy". Jeżeli istnieją znaczące różnice zdań co do zaistniałych faktów, to zostały one tutaj odnotowane.

s. 23 *Upiorna prawda:* Michael Moorcock, *The Dreaming City,* „Science Fantasy", t. 47, czerwiec 1961.

s. 25 *jak kilku z nich od razu zaczął hakować:* hakowanie w BSU zostało opisane przez Maksa i Davida w wywiadach. David wspominał szybkość i niecierpliwość Maksa. Alexander Feld-man, profesor z BSU, mówił w wywiadzie o wydanym Maksowi zakazie korzystania z komputera, dodając również, że Max sondował inne komputery.

s. 25 *Szeryf zadzwonił do administratora uniwersyteckiej sieci o drugiej nad ranem:* wywiad z Gregiem Jahnem, byłym administratorem sieci na BSU odpowiedzialnym za zamknięcie konta Maksa i przechowywanie jego plików.

3. Głodni Programiści

s. 30 *Sad Najwyższy Stanu Idaho zdecydował w podobnym przypadku: Państwo przeciw Townsendowi,* 124 Idaho 881, 865 P.2d 972 (1993).

s. 31 *Znalazł niezabezpieczony serwer plików FTP: Cinco Network Inc. przeciw Maksowi Butlerowi,* 2:96-cv-1146, US District Court, Western District of Washington. Max potwierdza tę relację, ale twierdzi, że w pierwszym rzędzie był zainteresowany rozpowszechnianiem plików muzycznych, a nie nielegalnego oprogramowania.

s. 33 *Chris Beeson, młody agent:* szczegóły współpracy Maksa z FBI pochodzą z akt sądowych i zostały przedstawione przez obrońcę Maksa w jego późniejszym procesie kryminalnym, *USA przeciw Maksowi Rayowi Butlerowi,* 5:00-cr-20096, US District Court, Northern District of California. Szczegóły dotyczące zwerbowania Maksa i jego relacji z agentami pochodzą z wywiadów z Maksem i tekstów, które zamieścił on w Internecie zaraz po przyznaniu się do winy.

Zob. http://www.securityfocus.com/comments/articles/ 203/5729/threaded (24 maja 2001). Max twierdzi, że nie uważał się za konfidenta i dostarczał jedynie informacji o charakterze technicz-nym.

4. Biały kapelusz

s. 35 *Pierwszymi ludźmi, którzy uznawali siebie za hakerów,* prekursorskim opracowaniem na temat pierwszych hakerów jest książka Stevena Levy'ego, *Hackers. Heroes of the Computer Revolution,* New York: Anchor Press/Doubleday, 1984. Zob. również: Steve Wozniak, Gina Smith, *iWoz. Od komputerowego geeka do kultowej ikony,* tłum. Anna i Olga Wojtaszczykowe, Warszawa 2009.

s. 37 *Pewnego dnia, kiedy Tim był w pracy:* ta anegdota została zapamiętana przez Tima Spencera. Max później przypomniał radę Spencera w liście do sędziego, który wydawał

wyrok w jego sprawie w Pittsburghu.

s. 38 *Jeśli było coś, za czym Max tęsknił:* szczegóły na temat związku Maksa i Kimi pochodzą przede wszystkim z wywiadów z Kimi.

s. 39 *Pojechał do miasta, żeby odwiedzić Matta Harrigana:* relacja na temat firmy Harrigana i jego pracy z Maksem pochodzi w przeważającej części od Harrigana, Max potwierdził niektóre szczegóły.

5. Cyberwojna!

s. 42 *W1998 roku eksperci od bezpieczeństwa odkryli najnowszy błąd w kodzie:* ta relacja na temat ataku Maksa na BIND opiera się przede wszystkim na zapisach sądowych, w tym także na pisemnym zeznaniu Maksa, wywiadach z Kimi i z byłym śledczym sił powietrznych Erikiem Smithem. Fragmenty korespondencji mailowej Maksa z FBI pochodzą z zapisów sądowych.

Szczegóły techniczne zostały zaczerpnięte głównie ze współczesnych analiz kodu Maksa, które można znaleźć na http://www.mail-archive.com/redhat-list@redhat.com/msg01857.html (dostęp: 20 lipca 2011).

s. 43 *podniosła alarm:* „Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases”, CERT Advisory CA-98.05.

s. 47 *Wysłał Paxsonowi anonimowa notę:* nota została dostarczona autorowi przez Verna Paxsona. Max potwierdził, że ją wysłał.

6. Tęsknię za przestępstwem

s. 50 *Kimi wróciła ze szkoły:* Kimi opisała tę część przeszukania przeprowadzonego przez FBI i jego skutki.

s. 51 *Agenci FBI dostrzegli szansę w przestępstwie Maksa:* szczegóły pochodzą z akt sądowych obrony w sprawie *USA przeciw Maksowi Rayowi Butlerowi,* 5:00-cr-20096, US District Court, Northern District of California.

s. 52 *Max był w siódmym niebie:* wywiady z Maksem i Kimi.

s. 54 *Carlosa Salgado juniora, trzydziestosześcioletniego fachowca od naprawiania komputerów,* szczegóły dotyczące przestępstwa Salgado pochodzą z wywiadu z nim samym, jego nie-doszłym klientem, a także z byłym administratorem sieci dostawcy Internetu, którego zhakował, i zapisów sądowych w sprawie *USA przeciw Carlosowi Felipe Salgado juniorowi,* 3:97-cr-00197, US District Court, Northern District of California. FBI odmówiło komentarza na temat tego przypadku, jak również zidentyfikowania ofiar kradzieży danych kart kredytowych.

s. 57 *Następnego dnia bez pluskwy FBI spotkał się z Harriganem w małej restauracji u Denny’ego:* wywiady z Mattem Harriganem i Maksem.

7. Max Vision

s. 60 *Pod koniec 1998 roku były pracownik cyberbezpieczeństwa w NSA:* wywiad z Martym Roeschem.

s. 63 *Podpisałem zeznania:* wywiady z Kimi. W rozmowie z autorem Max wyraził przekonanie, że przywiązanie do Kimi pogarszało jego sytuację prawną.

s.

65

To

jego

sprawa:

list

mailingowa

Snort

IDS,

3

kwietnia

2000,

http://archives.neohapsis.com/archives/snort/2000-04/0021.html (dostęp: 20 lipca 2011).

s. 65 *Patrick „MostHateD" Gregory. Computer Hacker Sentenced*, nota prasowa Departamentu Sprawiedliwości USA, 6 września 2000, http://www.justice.gov/criminal/cybercrime/

gregorysen.htm (dostęp: 20 lipca 2011).

276

s. 65 *Jasona „Shadow Knight" Diekmana: Orange County Man in Federal Custody for Hacking into Government Computers,* nota prasowa Departamentu Sprawiedliwości USA, 21

września 2000, http://www.justice.gov/criminal/cybercrime/diekman.htm (dostęp: 20 lipca 2011).

s. 65 *szesnastolatek Jonathan James: Juvenile Computer Hacker Sentenced to Six Months in Detention Facility,* nota prasowa Departamentu Sprawiedliwości USA, 21 września 2000, http://www.justice.gov/criminal/cybercrime/comrade.htm (dostęp: 20 lipca 2011).

8. Witamy w Ameryce

s. 67 *Dwaj Rosjanie:* szczegóły pułapki w Invicie i historii rosyjskich oskarżonych pochodzą przede wszystkim z akt sądowych, szczególnie *USA przeciw Wasilijowi Gorszkowowi*, 2:00:mj:00561, US District Court, Western District of Washington, a także wywiadu z byłym agentem FBI, który brał udział w operacji. Opis ubioru Rosjan i odniesienia do Grupy Ekspertów zostały zaczerpnięte ze świetnego artykułu Ariany Eunjung Cha w „The Washington Post" *A Tempting Offer for Russian Pair,* 19 maja 2003. Cytaty z rozmów, które miały miejsce w biurze Invity, pochodzą z transkrypcji taśmy z podsłuchu, z drobnymi gramatycznymi zmianami, które uczyniły je bardziej czytelnymi.

9. Okazje

s. 72 *Max włożył blezer i wymięte bojówki:* autor był obecny przy ogłoszeniu wyroku Maksa: zob. *As the Worm Turns*, „SecurityFocus", „Businessweek" online, 21 maja 2001, http://

www.businessweek.com/technology/content/jul2001/tc20010726_443.htm (dostęp: 20 lipca 2011). Listy napisane w obronie Maksa zostały dołączone do akt *USA przeciw Maksowi Rayowi Butlerowi*, 5:00-cr-20096, US District Court, Northern District of California.

s. 75 *Kimi rozmawiała z nim przez telefon:* wywiad z Kimi.

s. 75 *Max przyjął nowinę z niesamowitym spokojem:* wywiad z Maksem.

s. 75 *„Rozmawiałem z kilkoma ludźmi":* wywiad z Kimi.

s.75 *Jeffrey James Norminton:* trzej z bliskich znajomych Normintona, Chris Aragon, Werner Janer i anonimowy informator, wspominali o jego alkoholizmie, a Aragon mówił o wpływie nałogu na przestępczą produktywność Normintona. W aktach sądu federalnego znajduje się skierowanie Normintona do centrum odwykowego dla alkoholików i narkomanów, a w aktach lokalnego sądu świadectwo dwóch aresztowań za prowadzenie samochodu w stanie nietrzeźwo-

ści w 1990 roku (Orange County Superior Court, sprawy SM90577 i SM99355).

s. 76 *Ostatnie przestępstwo: USA przeciw Jeffreyowi Jamesowi Normintonowi*, 2:98-cr-01260, US District Court, Central District of California.

s. 76 *Norminton nie krył, że dostrzegł prawdziwy potencjał Maksa:* wywiady z Maksem, Chrisem Aragonem, Wernerem Janerem i innym informatorem zaznajomionym z więziennymi planami Maksa i Normintona.

s. 77 *On nie chciał jednak podpisać dokumentu:* Kimi i Max zgadzają się co do tego. Max twierdzi, że odmówił, ponieważ Kimi wydawała się niezdecydowana w kwestii rozwodu.

s. 77 *„Pokazywałem sie w miejscach (…)":* prośba Maksa do społeczności zajmującej się bezpieczeństwem jest zarchiwizowana http://seclists.org/fulldisclosure/2002/Aug/257.

s. 78 *Nawet Projekt Miodowej Sieci:* Max stwierdził, że ludzie prowadzący projekt odrzucili go. Założyciel Miodowej Sieci Lance Spitzner nie odpowiedział na pytanie autora.

s. 80 *Światowe badania:* prowadzone przez belgijską firmę Scanit, zajmującą się bezpieczeń-

stwem komputerowym. Polegały na udostępnieniu darmowego narzędzia online do oceny słabych punktów, 9 lipca 2003.

10. Chris Aragon

s. 83 *Max spotkał swego przyszłego przyjaciela i wspólnika w przestępczym procederze:* Chris Aragon przedstawił tę relację o swym pierwszym spotkaniu z Maksem. Max nie pamięta, gdzie po raz pierwszy się spotkali.

s. 84 *Pierwszy napad:* pierwsza próba napadu na bank i ostatni napad zakończony sukcesem zostały opisane w aktach sądowych sprawy *USA przeciw Christopherowi Johnowi Aragonowi i Albertowi Dwayne'owi See,* 81-cr-133, US District Court for the District of Colorado. Dodatkowe szczegóły, m.in. na temat incydentu ze śmietnikiem i stylu życia Aragona w tamtym czasie, pochodzą z wywiadu autora z Albertem See, byłym przestępczym wspólnikiem Aragona. W

wywiadzie Aragon zasadniczo przyznał się do wyroku za napad na bank i do brania kokainy w tym czasie.

s. 85 *zajął się oszustwami z użyciem kart kredytowych:* według Aragona, potwierdzone także przez jego byłego wspólnika Wernera Janera i Maksa.

s. 85 *by wpaść w zakrojonej na skalę całego kraju tajnej operacji DEA:* Kathryn Sosbe, *13*

arrested in marijuana bust/Colombian cartel used Springs as distribution point, „Colorado Springs Gazette-Telegraph", 13 września 1991. The Federal Bureau of Prisons potwierdziło skazanie Aragona, któremu postawiono m.in. zarzut rozprowadzania marihuany.

s. 87 *Wylądowali w dwudziestosiedmiopiętrowym Holiday Inn:* relacje te pochodzą od Maksa i Aragona i w całej książce zostały zaczerpnięte przede wszystkim z wywiadów z Maksem i Aragonem, jak również z ich wspólnikami Wernerem Janerem, Jonathanem Giannonem, Tsengeltsetseg Tsetsendelger oraz z innymi ludźmi zaangażowanymi w ich działalność przestępczą.

Oświadczenia złożone FBI przez Jeffreya Normintona streszczone w dokumentach sądowych także potwierdzają wiele z tych szczegółów.

s. 88 *haker w białym kapeluszu wynalazł sport zwany „wardrivingiem":* był to „Evil" Pete Shipley. Zob. Kevin Poulsen, *War Driving by the Bay,* Securityfocus.com, 12 kwietnia 2001, http://www.securityfocus.com/news/192 (dostęp: 20 lipca 2011).

s. 89 *Zaoferował on Maksowi 5000 dolarów za wejście do komputera osobistego wroga:* we-dług Aragona, Maksa i innych źródeł. Janer twierdzi, że pieniądze stanowiły pożyczkę. Charity potwierdza, że przyjęła czek w imieniu Maksa.

s. 89 *Charity miała tylko ogólne wyobrażenie o tym, czym zajmował się Max:* wywiad z Charity Majors.

s. 91 *Przy okazji włamał się do komputera Kimi:* wywiad z Maksem.

11. Dwudziestodolarowe zrzuty Scripta

s. 92 *Wiosną 2001 roku około 150 rosyjskojęzycznych przestępców komputerowych:* Greg Crabb z US Postal Inspection Service. Roman Vega, obecnie uwięziony w USA, odmówił komentarza, podobnie jak Ukrainiec powszechnie podejrzewany o bycie Scriptem.

s. 92 *Zarzewiem dyskusji był:* ta historia forów cardingowych pochodzi z wywiadów z kilkoma weteranami półświatka, akt sądowych, rozmów z przedstawicielami organów ścigania i szczegółowych badań archiwów Counterfeit Library, CarderPlanet i Shadowcrew.

s. 96 *Kiedy CW został wprowadzony przez Visę w 1992 roku, natychmiast wpłynął na zmniejszenie strat:* dane liczbowe dotyczące oszustw pochodzą z prezentacji Stevena Johnsona, dyrektora USA Public Sector Sales, przedstawionej na 9. dorocznej GSA SmartPay Conference w Filadelfii 23 sierpnia 2007.

s. 98 *Chris zdecydował, że sam spróbuje cardingu:* Aragon opowiedział o swoich kontaktach ze Scriptem i o pierwszym nielegalnym zakupie.

12. Darmowy Amex!

s. 100 *Max podzielił się swym planem z Charity,* wywiad z Charity Majors.

279

s. 102 *Internet Explorer może obsługiwać więcej niż tylko strony WWW:* Drew Copley i eEye Digital Security, *Internet Explorer Object Data Remote Execution Vulnerability,* 20 sierpnia 2003. Zob. CERT Vulnerability Note VU#865940. Autor niniejszej książki zlokalizował kod ataku Maksa w 2003 roku w poście opublikowanym na hakerskim forum, a badacz bezpieczeń-

stwa komputerowego i kierownik w eEye Marc Maiffret potwierdził, że atak wykorzystywał tego robaka. Max pamięta, że znał ten słaby punkt, zanim został on upubliczniony, ale nie jest pewien, skąd go miał. Twierdzi, że eEye i jego badacze nigdy nie wypuszczali informacji o robakach z wyprzedzeniem.

s. 104 *było tam pełno raportów FBI:* Aragon, Max i Werner Janer potwierdzają historię o włamaniu się przez Maksa do komputera agenta FBI. Max, Janer i inne źródła potwierdzają jego nazwisko. Sam agent, EJ. Hilbert, upiera się, że nigdy nie został znakowany, a Max najprawdopodobniej dostał się do miodowego punktu FBI wypełnionego fałszywymi informacjami.

13. Villa Siena

s. 106 *Chris włożył prostokątny kawałek PCW:* Aragon przyznaje się do fałszowania kart kredytowych i w wywiadzie podał niektóre szczegóły tego procederu. Autor zapoznał się z fał-

szerskim sprzętem Aragona i z dziesiątkami zrobionych przez niego kart w Newport Beach Police Department. Opis działania urządzeń krok po kroku pochodzi z wywiadu z innym do-

świadczonym fałszerzem kart, który używał tego samego sprzętu.

s. 108 *zebrał swoje dziewczyny:* Nancy Diaz Silva i Elizabeth Ann Esquere przyznały się do winy, potwierdzając rolę, jaką odgrywały w przedsięwzięciu Aragona. Informacji o innych oso-bach robiących dla niego zakupy podrabianymi kartami dostarczyli przy różnych okazjach byli współpracownicy Aragona: Werner Janer, Jonathan Giannone i Tsengeltsetseg Tsetsendelger.

s. 109 *„uderzała wyłącznie w system":* The Newport Beach Police Department przesłuchał

jedną z ostatnich dziewczyn z gangu Aragona Sarah Jean Gunderson w 2007 roku. Według raportu policyjnego: „Aragon stwierdził, że «uderzała wyłącznie w system«.

Gunderson powiedziała, że zdawała sobie sprawę z tego, że to było złe, jednak dzięki temu mogła zapłacić wszystkie rachunki" Gunderson przyznała się do winy.

14. Nalot

s. 112 *Chrisa Toshoka obudził dźwięk dzwonka przy drzwiach:* szczegóły policyjnego nalotu zostały zaczerpnięte przede wszystkim z posta *The whole surreal story* na blogu Toshoka / *am Pleased Precariously,* 15 stycznia 2004.

280

s. 115 *FBI próbowało ściągnąć Gembego do Ameryki:* Cassell Bryan-Low, *Hacker Hitmen,*

„The Wall Street Journal", 6 października 2003. Zob. też Kevin Poulsen, *Valve Tried to Trick* Half-Life 2 *Hacker into Fake Job Interview,* Wired.com, 12 listopada 2008, http://www.

wired.com/threatlevel/2008/ll/valve-tricked-h/ (dostęp: 20 lipca 2011).

s. 117 *„Oddzwoń, kiedy nie będziesz naćpany":* zarówno Aragon, jak i Max przyznają, że kłócili się o pieniądze. Ten cytat został przywołany przez Aragona.

s. 117 *wysyłał je do Meksyku, by dopasować do nich czyste VIN-y.* wywiad z Wernerem Janerem i Jonathanem Giannonem. Akta sądowe dotyczące aresztowania Aragona w San Francisco pokazują, że jego samochód miał fałszywy numer identyfikacyjny VIN i Aragon zgodził się na przepadek samochodu jako jeden z warunków zwolnienia. W wywiadach odmawiał podania dalszych szczegółów na temat tego aspektu swojej działalności.

15. UBuyWeRush

s. 120 *Cesar dotarł do podziemia okrężną drogą:* wywiad z Carranza.

s. 122 *Sam sprzęt nie był nielegalny.* Carranza przyznał się do prania pieniędzy w grudniu 2009 roku w związku z prowadzeniem usług wymiany e-gold dla carderów pod szyldem UBuyWeRush. *USA przeciw Cesarowi Carranzie,* l:08-cr-0026 US District Court for the Eastern District of New York. 16 września 2010 roku został skazany na sześć lat więzienia.

s. 123 *Średniej wielkości Commerce Bank w Kansas City, Missouri, mógł być pierwszym:* wywiad z Markiem J. Tomasikiem, byłym wiceprezesem Commerce Banku. Patrz również *Hey, banks, earn your stripes and fight ATM fraud scams,* „The Kansas City Star", 1 czerwca 2008.

s. 124 *Citibank, największy pod względem liczby klientów amerykański holding bankowy, stal się główną ofiarą:* Ataki CW były szeroko znane w cardingowych kręgach jako „wyciąganie gotówki z Citibanku". Jeden z mułów Kinga Arthura Kenneth Flury został oskarżony w Stanach Zjednoczonych, po tym jak przyznał się do kradzieży, wybierając 384 000 dolarów w bankomatach Citibanku w ciągu dziesięciu dni wiosną 2004 roku: *USA przeciw Kennethowi J. Flury emu,* l:05-cr-00515, US District Court for the Northern District of Ohio. Citibank odmówił komentarza. Aby zniechęcić konkurencję, spece od „wyciągania gotówki" często utrzymywali, że są w posiadaniu tajnych algorytmów, dzięki

którym mogą tworzyć działające dane pasków magnetycznych. Max i inni carderzy potwierdzili, że był to mit, to samo stwierdził też agent FBI J.

Keith Mularski. Dowolne dane mogły zadziałać.

281

s. 124 *wymknęło się kiedyś przy koledze, że King zarabiał milion dolarów tygodniowo na swych operacjach na całym świecie:* Joseph Menn, *Fatal System Error,* New York: Public Affa-irs, 2010.

s. 125 *Max przekazał je Chrisowi, który rzucił się na nie jak dziki:* wywiad z Maksem. Werner Janer potwierdził, że Chris pracował z Maksem nad „wyciąganiem gotówki z Citibanku", ale Janer nie znał szczegółów. Aragon odmówił komentarza na ten temat.

s. 126 *Tylko w ciągu roku:* Avitan Litan, *Criminals Exploit Consumer Bank Account and ATM System Weaknesses,* Gartner report G00129989, 28 lipca 2005. Szacowane straty obejmują dwa typy „uznaniowych" danych pasków magnetycznych, które nie zostały właściwie zweryfi-kowane: CW i opcjonalny offset PIN-u używany przez niektóre banki.

16. Operacja „Firewall"

s. 128 *Na górze strony pojawił się baner:* Ta i inne informacje na temat zawartości Shadowcrew pochodzą z kopii publicznie dostępnej części strony, zdobytej w październiku 2004 roku, tuż przed jej skasowaniem.

s. 129 *Te posty błyskawicznie zniknęły,* wywiady z Maksem. Aragon niezależnie stwierdził, że on sam i Max próbowali ostrzec członków Shadowcrew przed nalotami policji w ramach operacji „Firewall"

s. 130 *Transakcje, zarówno drobne, jak i gigantyczne:* szczegóły dotyczące transakcji pochodzą z: operacja „Firewall", CSA *przeciw Mantovaniemu i innym,* 2:04-cr-00786, US District Court for the District of New Jersey.

s. 131 *siły specjalne zauważyły, że Ethics oferował:* o znakowaniu agenta Secret Service przez Ethicsa po raz pierwszy poinformował Kevin Poulsen: *Hacker Penetrates T-Mobile Systems,* Securityfocus.com, 11 stycznia 2005. Informacje o używaniu przez Ethicsa exploitu BEA Systems pochodzą od informatorów zaznajomionych ze sprawą i po raz pierwszy zostały upublicznione przez autora książki: *Known Hole Aided T-Mobile Breach,* Wired.com, 28 lutego 2005, http://www.wired.com/politics/security/news/2005/02/66735 (dostęp: 20 lipca 2011). Zob.

też *USA przeciw Nicolasowi Lee Jacobsenowi,* 2:04-mj-02550, US District Court for the Central District of California.

s. 133 *David Thomas był długoletnim oszustem, który odkrył forum przestępcze:* na temat historii związków Thomasa z forami i szczegółach jego pracy dla FBI, zob. Kim Zetter, / *Was a Cybercrookfor the FBI,* Wired.com, 20 stycznia 2007. Ze źródeł zbliżonych do władz USA 282

autor otrzymał potwierdzenie, że Thomas pracował dla FBI, kiedy prowadził swoje forum The Grifters.

s. 133 *„Nie wiecie, z kim macie do czynienia":* z policyjnego raportu z aresztowania

Thomasa. „Problem z FBI i Secret Service polega na tym, że przyglądają się tylko największym przekrętom, które mogą ujawnić - powiedział Thomas w 2005 roku w wywiadzie z autorem tej książki. - Chcą wielkiej zdobyczy".

s. 135 *Ich cele zostały zaznaczone na mapie USA:* Brian Grow, *Hacker Hunters,* Businessweek, 30 maja 2005, http://www.businessweek.com/magazine/content/05_22/b3935001_

mz001.htm (dostęp: 20 lipca 2011). Identyfikacja broni agentów Secret Service również pochodzi z tej historii.

s. 136 *przechwalał się w prasie prokurator generalny ¡ohnAshcroft. Nineteen Individuals In-dicted in Internet „Carding" Conspiracy,* 28 października 2004 http://www.justice.gov/usao/nj/

press/files/pdffiles/firel028rel.pdf.

17. Pizza i plastik

s. 139 *Skanowanie doprowadziło go do wnętrza komputera z Windowsem:* Max, Jonathan Giannone i Brett Johnson - każdy z nich niezależnie zidentyfikował Pizzę Schmizzę w Vancouver w stanie Waszyngton jako źródło zrzutów Maksa w tym okresie. Menedżerka lokalu stwierdziła, że restauracja od tamtej pory zmieniła właściciela, a ona nie posiada żadnej wiedzy na temat włamań.

s. 140 *Max nie mógł znieść tego, że znowu ktoś go oszukuje:* wywiady z Maksem.

s. 141 *Giannone był bystrym dzieciakiem z klasy średniej lubiącym kokainę:* Giannone potwierdził branie kokainy i wszystkie szczegóły swych związków z Maksem i Aragonem. O przy-ciskaniu guzików w windzie i kawale z „obrabowaniem banku" powiedział na czacie z innym carderem. Zapis tej rozmowy otrzymał autor. Giannone przyznał w wywiadzie, że rozmawiał o kawale z „obrabowaniem banku", stwierdził jednak, że były to czcze przechwałki i tak naprawdę tego nie zrobił. Powiedział też, że nie przypomina sobie sprawy z windą.

s. 141 *Giannone dołączył do Shadowcrew i CarderPIanet pod nickiem MarkRich:* używanie przez Giannonego różnych pseudonimów zostało przez niego potwierdzone w wywiadzie. Posty na forum, przejrzane przez autora książki, dowodzą, że Giannone porzucił swój oryginalny nick, po tym jak zaczęto go podejrzewać o donoszenie na wspólnika, gdy przebywał w poprawczaku.

s. 141 *dokonał ataku DDoS na JetBlue:* Giannone mówił również o tym ataku we wspomnianych wyżej zapisach czatów. Potwierdził to też w rozmowie z autorem.

s. 141 *nastolatek hakował, korzystając z komputera w sypialni swej matki:* wywiady z Maksem.

18. Odprawa

s. 144 *chciał być agentem już od pierwszego roku studiów:* szczegóły z życia Mularskiego i jego wczesnej pracy w NCFTA pochodzą z wywiadów z nim.

s. 146 *Odprawa dla sześciu agentów:* wywiady z J. Keithem Mularskim oraz z

inspektorem Gregiem Crabbem.

19. Carders Market

s. 148 *„Sherwood Forest" nie przyjąłby się na przestępczym rynku:* informacja o odrzuceniu nazwy przez Aragona pochodzi z wywiadów z Maksem i z listów, które pisał do sędziego wydającego wyrok w jego sprawie.

s. 149 *Janer, zapalony kolekcjoner zegarków, ruszył prosto do Richard's of Greenwich:* Janer ujawnił motywy swego nieudanego zakupu zegarków w wywiadach, a Aragon potwierdził, że dostarczył Janerowi podrabiane karty w ramach przysługi. Policyjne akta sprawy opisują jego aresztowanie i późniejszą współpracę. Informacje te zostały potwierdzone przez Janera. *USA przeciwko Wernerowi Williamowi Janerowi*, 3:06-cr-00003, US District Court for the District of Connecticut.

s. 151 *Znakował centrum informacji na Florydzie prowadzone przez Affinity Internet:* akta sądowe potwierdzają, że Carders Market był wówczas hostowany w Affinity i że Affinity dostarczyła później FBI kopii systemu plików. Max opisał dokładnie znakowanie serwera w wywiadach i jako „Iceman" w postach na internetowym forum dyskusyjnym.

s. 152 *„ Widzę, że razem będziemy robić dobre interesy w przyszłości":* zapisy czatów uznane za dowód w sprawie *USA przeciw Jonathanowi Giannonemu,* 3:06-cr-01011, US District Court for the District of South Carolina. Posty z czatów i forów dyskusyjnych są w tej książce przytaczane dosłownie, kiedy pojawiają się jako cytaty, z wyjątkiem drobnych zmian gramatyki, interpunkcji lub pisowni, które uczyniły je bardziej czytelnymi.

20. Starlight Room

s. 154 *Tsengeltsetseg Tsetsendelger właśnie została pocałowana:* Aragon, Max i inne źródła potwierdzają, że Tsetsendelger została zwerbowana w Starlight Room i zaprowadzona do hotelu, w którym zatrzymał się Aragon. Szczegóły pochodzą z wywiadu z Tsetsendelger. Liz i Michelle Esquere odmówiły komentarza.

22. Wrogowie

s. 164 *wymagał od techników zrestartowania komputera co 49,7 dnia:* jedno ze źródeł: Linda Geppert, *Lost Radio Contact Leaves Pilots on Their Own*, „IEEE Spectrum" listopad 2004, http://spectrum.ieee.org/aerospace/aviation/lost-radio-contact-leaves-pilots-on-their-own (dostęp: 20 lipca 2011).

s. 165 *Giannone był mocno przekonany, że nie będzie w stanie zhakować maca:* wywiad z Giannonem. Max przyznał, że często hakował Giannonego i śledził jego ruchy, miał również skłonność do wysyłania do Giannonego i do innych długich wiadomości, w których opisywał

swe myśli. Wyjaśnił również, że hakowanie maców nie stanowi dla niego problemu.

s. 166 *Dotarł więc do Thomasa przez ICQ, aby spróbować rozwiązać probłem:* Max i Aragon dyskutowali na temat bieżący konfliktu z Thomasem, który szczegółowo przedstawił swe podejrzenia wobec Carders Market i Johnsona na swej własnej stronie,

the Grifters. Dodatkowo Kevin Poulsen otrzymał przytoczony w książce zapis czatu między Aragonem i Thomasem.

23. Anglerphish

s. 170 *Po prostu potrzebował pieniędzy:* szczegóły z osobistego życia Johnsona pochodzą z zeznania pod przysięgą, które złożył w swej sprawie kryminalnej 13 kwietnia 2007 roku, i z listu, który napisał 1 marca 2007 roku do sędziego wydającego wyrok w jego sprawie. Zob. *USA przeciw Brettowi Shannonowi Johnsonowi,* 3:06-cr-0U29, US District Court for the District of South Carolina.

s. 170 *równocześnie pokazywane na czterdziestodwucałowym ekranie plazmowym powieszonym na ścianie biura:* stenogram procesu *USA przeciw Jonathanowi Giannonemu,* 3:06-cr-01011, US District Court for the District of South Carolina.

s. 171 *Podejrzany zrobił wszystko z wyjątkiem dokładnego wyczyszczenia dywanów i pomalowania ścian:* wywiad z Justinem Fefferem, starszym śledczym, High Technology Crime Division, Los Angeles County District Attorney's Office. Zob. też: *Obywatele Stanu Kalifornia przeciw Shawnowi Mimbsowi,* BA300469, Superior Court of California, County of Los Angeles.

Mimbs odmówił komentarza.

s. 171 *Pisaki nie poruszyły się, kiedy Johnson odpowiadał na pierwsze dwa pytania:* tak twierdzi Johnson. Secret Service odmówiła rozmów na temat operacji „Anglerphish".

s. 173 *nie dam ci spokoju do końca życia:* z listu Johnsona do sędziego, który wydawał wyrok w jego sprawie.

285

24. Ujawnienie

s. 174 *„Tea, te dziewczyny to blachary":* wywiad z Tsengeltsetseg Tsetsendelger. Aragon wspomniał o swej skłonności do Tsetsendelger w wywiadach i listach do autora.

s. 175 *Stwierdziła, że Iceman jest naprawdę spoko:* wywiad z Tsetsendelger. Max powiedział, że był dla niej miły na czacie, ale prywatnie jej nie lubił.

s. 176 *„Spadajcie stąd":* opis zdarzenia pochodzi z wywiadu z Tsetsendelger i Giannonem.

s. 177 *Robak był w krótkiej sekwencji uzgodnienia parametrów transmisji danych:* Zob.

CERT Vulnerability Note VU#117929. Robak został odkryty przypadkowo przez Stevea Wise-mana z Intelliadmin.com, kiedy pisał on program klienta VNC i testował go. Szczegóły techniczne

pochodzą

z

analizy

Jamesa

Evansa;

zob.

http://marc.info/?l=bugtraq&m=

114771408013890&w=2.

s. 181 *popularnym blogu poświęconym bezpieczeństwu:* blog Bruce'a Schneiera *Schneier on Security,* http://www.schneier.com/blog/archives/2006/06/interview_with_l.html.

s.

182

przypadkowego

bloga

pod

nazwą

„Life

on

the

Road":

zob.

http://afterlife.wordpress.com/2006/06/19/cardersmarket-shadowcrew-and-credit-card-theft/i http://afterlife. wordpress.com/2006/07/12/carding-web-sites/.

25. Wrogie przejęcie

s. 188 *Carders Market miał teraz 6000 członków.* Max, były administrator jego forum Th3C0rruptedOne i inni carderzy twierdzą, że po wrogim przejęciu liczba użytkowników prze-kroczyła 6000. Departament Sprawiedliwości określił jednak tę liczbę na 4500.

s. 191 *w tajemnicy nawet przed swoja matką:* tak utrzymuje jego matka Marlene Aragon.

26. Co masz w portfelu?

s. 196 *finansowany przez branżę raport Javelin Strategy and Research:* Javelin Strategy and Research, *2007 Identity Fraud Survey Report,* luty 2007. Raport był sponsorowany przez Visa USA, Wells Fargo i CheckFree, a potem nieustannie cytowany przez Visa USA w prezentacji w PowerPoincie na szkoleniu w Federalnej Komisji Handlu: „50 procent zidentyfikowanych złodziei to *osoby znane ofiarami"* (podkreślenie autorów raportu). Zob. też Kevin Poulsen, *Stolen Wallets, Not Hacks, Cause the Most ID Theft? Debunked,* Wired.com, 12 lutego 2009, http://www.wired.com/threatlevel /2009/02/stolen-wallets/ (dostęp: 20 lipca 2011).

s. 196 *Prywatne obliczenia Visy pokazywały prawdę:* wystąpienie dyrektora Stevena Johnsona, Visa USA Public Sector Sales, na 9. dorocznej konferencji GSA SmartPay w Filadelfii, 23

sierpnia 2007. Slajdy z prezentacji zostały oznaczone jako „Visa Confidential".

s. 197 C0rr *upted odkrył świat warez na osiągalnych przez połączenie telefoniczne bulletin board systemach:* informacje biograficzne pochodzą z wywiadów telefonicznych i online z Th3C0rrupted0ne, który zgodził się mówić, pod warunkiem że jego prawdziwe nazwisko nie zostanie ujawnione.

s. 198 *„Nie mogę uwierzyć, jak wiele o mnie wiesz":* wywiad z Aragonem.

s. 199 „Me *klikajcie na niesprawdzone linki":* US-CERT Technical Cyber Security Alert TA06-262A, http://www.kb.cert.org/vuls/id/416092 (dostęp: 20 lipca 2011).

s. 201 *Każda kopia wiadomości została dostosowana:* tekst phishingowego maila Maksa pochodzi ze złożonego FBI pisemnego oświadczenia pod przysięgą, dołączonego do akt sprawy *USA przeciw Maksowi Rayowi Butlerowi,* 3:07-mj-00438, US District Court for the Eastern District of Virginia. „Mary Rheingold" nie jest prawdziwym nazwiskiem i zostało podane przez autora zamiast „[imię i nazwisko odbiorcy]" w oryginalnym dokumencie sądowym.

27. Pierwsza wojna sieciowa

s. 206 *„Secret Service i FBI odmówiły komentarzy na temat kemana lub przejęć":* Byron Acohido i Jon Swartz, *Cybercrime flourishes in online hacker forums,* „USA Today", 11 paź-

dziernika 2006.

s. 207 *Kurwa, straciłeś rozum:* wywiad z Chrisem Aragonem.

s. 207 *„szczególnie Bank of America i Capital One":* za swój harpunniczy atak phishingowy Max został oskarżony tylko w wypadku włamania do Capital One. Inne ofiary ujawnił Max.

28. Cardingowy sąd

s. 211 *To tylko Siło próbował zdobyć dla policji informacje o członkach DarkMarket* Max, Mularski i Th3C0rrupted0ne zidentyfikowali Liskego jako Silo. W długich wywiadach Liske unikał kwestii swej działalności na forach, w pokrętny sposób mówiąc o pracy informatora i swych relacjach z Maksem. „Max był dobrym przypadkiem. Wiesz, stanowił wyzwanie". Na temat trojana w NCFTA powiedział: „Czy nie należy przyznać, że ktokolwiek wysyłał trojany, robił to tak naprawdę wszystkim w półświatku?" Później: „Jeśli byłby złośliwy, ja mógłbym -

ktoś mógłby, spowodować prawdziwą szkodę". Detektyw Mark Fenton z policji w Vancouver powiedział, że kanadyjskie prawo zakazuje mu ujawnienia bądź potwierdzenia tożsamości 287

konfidenta. Na pytanie, czy otrzymał znakowane dowody od informatorów, odpowiedział:

„Wiem, że w Stanach branie pod uwagę jakiejś podejrzanej informacji jest niedopuszczalne.

Tutaj, gdy ktoś coś mi powie, pytam: «Gdzie to słyszałeś?«. On odpowiada: »Od jednego faceta«„. Podobało mu się rozwiązanie zastosowane w programie ostrzegania Crime Stoppers (STOP

Przestępczości): „Czy należy odrzucić Crime Stoppers, ponieważ dzwonią przestępcy, dając cynk na temat innych przestępców?". Pozostaje pytanie, w jakim stopniu, jeśli w ogóle, Secret Service wykorzystała zhakowane informacje, dostarczone przez policję z Vancouver, w śledztwach prowadzonych w USA. Secret Service odmówiła autorowi zgody na rozmowę z agentami:

„Mimo że podjęliśmy decyzję, by nie brać udziału w rym konkretnym projekcie, nie ma przeszkód, by się pan do nas zgłosił z innymi propozycjami w przyszłości".

s. 215 *tego samego użytkownika, który kiedyś zarejestrował w firmie inny adres:* Max twierdzi, że NightFox odpowiadał za zarejestrowanie strony internetowej Financial Edge News, i to on popełnił ten błąd.

29. Jedna platyna i sześć klasyków

s. 219 *„ za 150 klasyków":* oświadczenie pod przysięgą agenta specjalnego Secret Service Roya Dotsona, 24 lipca 2007, w aktach sprawy *USA przeciw E-Gold,* LTD, l:07-cr-0019, US

District Court for the District of Columbia. Cała historia e-gold została opisana przez Kim Zetter, *Bullion and Bandits. The Improbable Rise and Fall ofE-Gold,* Wired.com, 9 czerwca 2007.

s. 221 *Współpracowali ściśle z oficerem prowadzącym Siła z policji w Vancouver,* wieść o spotkaniu dotarła do Liskego. „Pojawiły się oskarżenia, że to ja jestem Icemanem - powiedział w wywiadzie. - Zrobiono też wielką prezentację, by pokazać, że ten facet to Iceman. Ludzie, któ-

rym ją przedstawiono, doskonale wiedzieli, że nim nie jestem".

30. Maksik

s. 223 *dostawał maila ze zrzutami, które zamówił, prosto z wielkiej bazy danych Maksika: USA przeciw Maksymowi ¡astremskiemu,* 3:06-cr-01989, US District Court for the Southern District of California.

s. 226 *Na początku 2006 roku Ukraińcy w końcu zidentyfikowali Maksika jako Maksyma Jastremskiego:* wywiad z Gregiem Crabbem.

s. 226 *potajemnie skopiowali twardy dysk Ukraińca do analizy,* dokument z 24 lipca 2009 w sprawie *USA przeciw Albertowi Gonzalezowi,* 2:08-cr-00160, US District Court for the Eastern District of New York.

s. 227 *„Mieliśmy szczęście w tej sprawie, ponieważ człowiek, który kupował od Salgado, był*

współpracownikiem FBI": pisemne zeznanie Roberta S. Litta, zastępcy prokuratora generalnego, przed Podkomisją Telekomunikacji, Handlu i Ochrony Konsumenta, Komisja Handlu Izby Reprezentantów, 4 września 1997, http://www.justice.gov/criminal/cybercrime/daag9_97.htm (dostęp: 20 lipca 2011).

s. 228 *Federalni przegrali szyfrową wojnę:* szczegóły historii w: Steven Levy, *Crypto. How the Code Rebels Beat the Government - Saving Privacy in the Digitai Age,* New

York: Penguin Books, 2002.

31. Proces

s. 230 *„Co, zabierasz teraz moje dziewczyny na imprezę?”:* wywiad z Giannonem.

s. 230 *Kiedy już ława przysięgłych się zgromadzi, szanse oskarżonego na uniewinnienie wynoszą około jednego do dziesięciu:* Rok podatkowy 2006. Obliczenia z „Federal Justice Statistics, 2006 - Statistical Tables”, US Department of Justice, Bureau of Justice Statistics, 1 maja 2009 (http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=98b).

s. 231 *„/ podejrzewam, że już nigdy nie będziecie patrzeć na Internet tak jak dawniej”:* stenogram procesu *USA przeciw Jonathanowi Giannonemu,* 3:06-cr-01011, US District Court for the District of South Carolina. Do tekstu wprowadzono drobne gramatyczne zmiany, by uczynić go bardziej czytelnym.

s. 232 *„A kto to jest lcemani”:* wywiad z Giannonem.

32. Centrum handlowe

s. 236 *swym nowym wspólnikiem - dwudziestotrzyletnim Guyem Shitritem:* informacje o problemach Shitrita w Miami pochodzą od Aragona. Detektyw Robert Watts z policji w Newport Beach potwierdził, że słyszał tę samą relację. Shitrit, obecnie przebywający w więzieniu, nie odpowiedział na list autora książki.

s. 236 *Jego żona Clara wyciągnęła na eBayu w ciągu nieco ponad trzech lat 780 000 dolarów.* na podstawie obliczeń sprzedaży z konta Clary Aragon na eBayu uzyskanych przez policję z Newport Beach. Aragon odmówił rozmowy na temat swych zysków.

s. 237 *Czuł, że Max ignoruje Whiz List - ich plan na dokonanie jednego wielkiego skoku i wyjście z interesu:* wywiad z Aragonem. Kiedy policja przejrzała zawartość jego telefonu ko-mórkowego, znaleźli wpis na jego elektronicznej liście spraw do załatwienia: „załatwić whiz list”.

s. 237 *w drobiazgowych, ręcznie pisanych arkuszach kalkulacyjnych, w których wyliczała, jak wiele Chris jest jej winien za każde zakupy:* Jeden z takich arkuszy został przejęty przez policje z Newport Beach i autor książki mógł go zobaczyć.

s. 238 *Vigo szukał sposobu na spłacenie 100 000 dolarów długu meksykańskiej mafii:* według zeznań Vigo złożonych po aresztowaniu. Policja z Newport Beach znalazła kopię listu przewozowego w biurze Vigo.

s. 239 *Ochrona w Bloomingdale’s nie lubi niepokoić klientów sklepu:* wywiad z detektywem Robertem Wattsem.

s. 240 *31 torebek Coacha, 12 aparatów cyfrowych Canon PowerShot:* według raportu sporządzonego w czasie rewizji.

33. Strategia wyjścia

s. 242 *Max postanowił zainwestować w sznurową drabinkę:* wywiad z Maksem.

s. 242 *Wtedy właśnie Max w końcu dowiedział się o aresztowaniu Giannonego z artykułu prasowego:* Kim Zetter, Secref Service *Operative Moonlights as Identity Thief,*

Wired.com, 6

czerwca 2007, http://www.wired.com/politics/law/news/2007/06/secret_service (dostęp: 20 lipca 2011).

s. 243 *Z każdym dniem stawał się coraz bardziej nerwowy:* według wywiadu z Charity Majors. Max twierdzi, że był zaniepokojony, ale nie nerwowy.

s. 244 *sędzia zatwierdził legalną zmianę nazwiska z Max Butler na Max Ray Vision:* w: *Re: Max Ray Butler,* CNC-07-543988, County of San Francisco, Superior Court of California.

s. 245 *Silo ukrył w nim jednak inny przekaz:* wywiad z Maksem. Lloyd Liske ani nie potwierdził, ani nie *zaprzeczył* tej relacji.

s. 245 *Firma otwarcie oferowała usługę jako sposób na obejście inwigilacji FBI:* „W niektó-

rych krajach wprowadzono w życie finansowane przez rząd projekty, których celem jest gromadzenie wielkich ilości danych z Internetu, łącznie z mailami, i przechowywanie ich do przyszłych analiz. […] Za przykład takich działań może służyć projekt FBI pod kryptonimem »Car-nivore«. Korzystając z Hushmail, możesz być pewien, że twoje dane zostaną zabezpieczone przed

tego

rodzaju

szeroką

rządową

inwigilacją”,

http://www.

hushma-

il.com/about/technology/security/ (dostęp: 20 lipca 2011).

s. 245 *zmusiły kierownictwo Hushmail do sabotowania własnego systemu i wydania kluczy do szyfrów osób będących przedmiotem inwigilacji:* Ryan Singel, *Encrypted E-Mail Company* 290

Hushmail Spills to Feds, Wired.com, 7 listopada 2007. Detektyw Mark Fenton z policji w Vancouver przyznał, że ujawnił Secret Service mail Maksa z Hushmail.

s. 245 *Miał to być treningowy wypad dla nowych pracownic Chrisa:* wywiady z Tsengeltsetseg Tsetsendelger i Chrisem Aragonem.

s. 246 *agentka Secret Service przebrana za pokojówkę:* inwigilacja prowadzona przez Secret Service, w tym jazda windą z Maksem, została opisana w zeznaniach pod przysięgą w sprawie *USA przeciw Maksowi Rayowi Butlerowi,* 2:07-cr-00332, US District Court for the Western District of Pennsylvania. Max powiedział w wywiadzie, że agentka była ubrana jak pokojówka.

Agent FBI Mularski twierdzi, że inwigilacja była zawieszana i wznawiana w ciągu kilku

miesię-

cy.

s. 247 *Chris wybrał zdjęcie Maksa z kartoteki policyjnej: USA przeciw Maksowi Rayowi Butlerowi,* 2:07-cr-00332, US District Court for the Western District of Pennsylvania. Aragon twierdzi, że władze użyły wobec niego podstępu, mówiąc mu, że Max już został aresztowany, ale Aragon udzielił im również informacji na temat środków bezpieczeństwa, które przedsięwziął

Max, co podważa to stwierdzenie. Akta sądowe z procesu Aragona w Orange County zawierają zapieczętowany list od Dembosky'ego. *Obywatele Stanu Kalifornia przeciw Christopherowi Johnowi Aragonowi i innym,* 07HF0992, Superior Court of California, County of Orange.

s. 248 *Dwa straciły zasilanie, kiedy agent wyrwał kabel wijący się po podłodze:* tak twierdzi Max.

s. 249 *Max odwrócił głowę, by spojrzeć na Master Splyntra:* wywiad z Mularskim.

s. 249 *Miałaś rację:* wywiad z Charity Majors.

s. 249 *Dlaczego nas nienawidzisz?:* wywiad z Maksem.

34. DarkMarket

s. 253 *opowiedział wstrząsającą historię: Son bilgiyi verecekken yok oldu!,* „Haber", nr 71,12 sierpnia 2008, http://www.haber7.com/haber/20080812/Son-bilgiyi-verecekken-yok-oldu.php (dostęp: 20 lipca 2011).

s. 254 *wskazując znanego członka organizacji Cha0 jako nadawcę:* Mularski opisał genezę tego śledztwa. Rola, jaką odegrała w nim firma kurierska, została opisana w szczegółach przez Uri Rivnera z RSA w poście na blogu: http://www.rsa.com/blog/blog_entry.aspx?id=1451 (do-stęp: 20 lipca 2011). Turecka policja przekazała prośby do ambasady w Waszyngtonie, która odmówiła udzielenia zgody na przeprowadzenie z nimi wywiadu.

s. 254 *wysoki, dobrze zbudowany mężczyzna z krótko przyciętymi włosami, ubrany w czarny T-shirt z kostuchą:* na podstawie policyjnego nagrania wideo z aresztowania i rewizji. Zob. również: *Enselenen Chao sanai emayi anlatti,* „Haber", nr 7,12 września 2008, •

http://www.haber7.com/haber/s20080912/Enselenen-Chao-sanal-semayi-anlatti.php (dostęp: 20

lipca 2011).

s. 255 *dopasowując jego pojawianie się tam z postami JiLsiego:* wywiad z Mularskim. Zob.

również Caroline Davies, *Welcome to DarkMarket - global one-stop shop for cybercrime and banking*

fraud,

„The

Guardian”,

4

stycznia

2010,

http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley (dostęp: 20 lipca 2011).

s. 255 *Wspólnik JiLsiego, sześćdziesięciosiedmioletni John „Devilman” McHugh,* tamże.

s. 255 *Erkan „Seagate” Findikoglu:* wywiad z Mularskim. Zob też Fusun S. Nebil, *FBI Siber Suçlarla, ABD tçinde ve Dtsinda tsbirlikleri ile Miicadele,* Turk.Internet.com, 15 czerwca 2010, http://www.turk.Internet.com/portal/yazigoster.php?yaziid=28171 (dostęp: 20 lipca 2011).

s. 255 *27 członków gangu Seagatea zostało oskarżonych w Turcji:* wywiad z Mularskim.

s. 256 *reporter z Südwestrundfunk, publicznego radia z południowych Niemiec:* tym reporterem

był

Kai

Laufen.

Zob.

http://www.swr.de/swr2/programm/sendungen/wissen/-/

id=660374/nid=660374/did=3904422/p6601i/index.html (dostęp: 20 lipca 2011).

s. 256 *Prasa amerykańska podchwyciła tę historię:* autor niniejszej książki jako pierwszy zidentyfikował z nazwiska J. Keith Mularskiego jako agenta FBI występującego pod nickiem Master Splyntr, *Cybercrime Supersite „DarkMarket” Was FBI Sting, Documents Confirm,* Wired.com, 13 października 2008, http://www.wired.com/threatlevel/2008/10/darkmarket-post/

(dostęp: 20 lipca 2011).

35. Wyrok

s. 259 *Śledczym z CERT-u wystarczyły dwa tygodnie na znalezienie klucza do szyfru:* Max dobrze wiedział, że klucz był łatwy do odkrycia, kiedy znajdował się w pamięci RAM, ale był

przekonany, że zabezpieczenia na jego serwerze uniemożliwią komukolwiek uzyskanie dostępu do pamięci. Matt Geiger z CERT-u, który kierował ekipą dochodzeniową, odmówił komentarza na temat tego, jak ominął zabezpieczenia, ale powiedział, że był w stanie uruchomić na komputerze Maksa oprogramowanie do odzyskiwania pamięci.

s. 259 *Max ukradł 1,1 miliona kart z terminali:* Max nie zakwestionował tej liczby w czasie procesu, ale w wywiadzie wyraził wątpliwość, by mogła być aż tak duża.

36. Pokłosie

s. 263 *Tajna agentka Secret Service ściągnęła go do nocnego klubu: 2010 Data Breach Investigations Report,* Verizon RISK Team we współpracy z Secret Service USA, 28 lipca 2010.

s. 264 *użytkownik ICQ 201679996: Affidavit in Support of Arrest Warrant,* 8 maja 2007, *USA przeciw Albertowi Gonzalezowi,* 2:08-mj-00444, US District Court for the Eastern District of New York.

s. 265 *Ze wszystkich hakerów to Jonathan James zapłacił najwyższą cenę:* zobacz Kevin Poulsen, *Former Teen Hacker's Suicide Linked to TJX Probe,* Wired.com, 9 lipca 2009, http://

www.wired.com/threatlevel/2009/07/hacker/ (dostęp: 20 lipca 2011).

s. 266 *Werbują zwykłych konsumentów jako nieświadomych praczy pieniędzy:* więcej szczegółów na temat tzw. oszustw na muła na blogu byłego reportera Washingtonpost.com Briana Krebsa, który obszernie pisał na temat tych przestępstw: http://krebsonsecurity.com/.

s. 267 *Secret Service płaciła mu roczną pensję w wysokości* 75 *000 dolarów:* po raz pierwszy opisane przez Kim Zetter, *Secret Service Paid TJX Hacker $75,000 a Year,* Wired.com, 22

marca 2010.

s. 267 *złożonego przez prokuratorów generalnych 41 stanów,* jedno ze źródeł: Dan Kaplan, *TJX settles over breach with 41 states for $9.75 million,* „ SC Magazine", 23 czerwca 2009, http://www.scmagazineus.com/tjx-settles-over-breach-with-41-states-for-975-million/

artic-

le/138930/ (dostęp: 20 lipca 2011)..

s. 267 *kolejne 40 milionów wydającym karty Visa bankom:* Mark Jewell, *TJX to pay up to $40.9 million in settlement with Visa over data breach,* Associated Press, 30 listopada 2007.

s. 267-268 *Heartland otrzymał certyfikat PCI:* jedno ze źródeł Ellen Messmer, *Heartland breach raises questions about PCI standard's effectiveness,* „Network World", 22 stycznia 2009, http://www.networkworld.com/news/2009/012209-heartland-breach.html (dostęp: 20

lipca

2011).

s. 268 *Hannaford Brothers uzyskali certyfikat bezpieczeństwa, nawet kiedy hakerzy byli w ich systemach:* jedno ze źródeł: Andrew Conry-Murray, *Supermarket Breach Calls PCI Compliance into Question,* „InformationWeek", 22 marca 2008.

s.

268

Restauracje

złożyły

pozew:

http://www.prlog.org/10425165-secret-service-

investigation-lawsuit-cast-shadow-over-radiant-systems-and-distributo.html (dostęp: 20 lipca 2011). Także: *Radiant Systems and Computer World responsible for breach affecting restaurant* 293

lawsuit, Databreaches.net, 24 listopada 2010, http://www.databreaches.net/?p=8408 (dostęp: 20

lipca 2011), i Kim Zetter, *Restaurants Sue Vendor for Unsecured Card Processor,* Wired.com, 30 listopda 2009, http://www.wired.com/threatlevel/2009/ll/pos (dostęp: 20 lipca 2011).

s. 268 *Białe kapelusze opracowały ataki przeciw kartom czip-i-PIN:* Zobacz Steven J. Mur-doch, Saar Drimer, Ross Anderson, Mike Bond, *Chip and PIN Is Broken,* University of Cambridge Computer Laboratory, Cambridge, UK. Przedstawione na 2010 IEEE Symposium on Security and Privacy, maj 2010, http://www.cl.cam.ac.uk/research/security/banking/ nopin/

(dostęp: 20 lipca 2011). Odpowiedź UK Card Association znajduje się na http://

www.theukcardsassociation.org.uk/view_point_and_publications/what_we_think/ -/page/906/.

s. 269 *wymiany setek tysięcy terminali sprzedaży na nowe urządzenia:* same karty są również droższe. Bardziej wnikliwe omówienie czynników, które wstrzymują przyjęcie kart czip-

-i-PIN w USA, w Clases Bell, *Are chip and PIN credit cards coming?,* Bankrate.com, 18 lutego 2010, http://www.foxbusiness.com/story/personal-finance/financial-planning/ chip-pin-credit-cards-coming/). Zobacz również Allie Johnson, *US credit cards becoming outdated, less usable abroad,* Creditcards.com, http://www.creditcards.com/credit-

-card-news/outdated-smart-card-chip-pin-1273.php (dostęp: 20 lipca 2011).

Epilog

s. 271 *Jego matka zasugerowała, by wziął agenta: z* listu Aragona do autora.

Podziękowania

Maksa Visiona spotkałem po raz pierwszy jakieś dziesięć lat temu, kiedy by-

łem początkującym reporterem pracującym dla SecurityFocus.com, strony po-

święconej bezpieczeństwu komputerowemu. Max został wówczas oskarżony w związku z dobrze przygotowanym atakiem na tysiące systemów Pentagonu, a ja byłem zafascynowany spektaklem, który rozgrywał się w budynku sądowym w Dolinie Krzemowej, gdzie federalny system sprawiedliwości pastwił się nad niegdyś szanowanym

ekspertem od bezpieczeństwa komputerowego, który za sprawą jednego romantycznego hakerskiego porywu przewrócił swe życie do góry nogami.

Wiele lat później, gdy opisałem już setki przestępstw komputerowych, słabych punktów i usterek w oprogramowaniu, Max znowu został aresztowany, a nowe federalne śledztwo ujawniło ukryte życie, które prowadził, po tym jak wypadł z łask. W miarę kontynuowania moich dociekań umocniłem się w przekonaniu, że Max, bardziej niż ktokolwiek inny, ucieleśnia wielką zmianę w świecie hakingu, której świadkiem byłem, a jego przypadek mógłby służyć za doskonałą soczewkę umożliwiającą zbadanie współczesnego komputerowego półświatka.

295

Na szczęście inni podzielali moją opinię. Mam dług wdzięczności wobec mojego agenta Davida Fugatea, który przeprowadził mnie przez proces rozwi-jania mojego pomysłu do postaci książki, a także wobec mojego redaktora z wydawnictwie Crown Juliana Pavii, który przez cały rok pracował niestrudze-nie, bym nie zbaczał z kursu i nie spóźnił się zbytnio, zbierając materiały, pi-sząc i poprawiając tekst.

Równie ważne było też wielkie wsparcie ze strony mojego szefa Evana Hansena, redaktora naczelnego Wired.com. Jestem też wdzięczny moim kole-

żankom i kolegom z bloga Threat Level na Wired.com: Kim Zetter, Ryanowi Singlowi i Davidowi Kravtsowi, którzy zbiorowo nieśli brzemię mojej dwu-miesięcznej nieobecności, kiedy kończyłem książkę, a po wszystkim poradzili sobie z moim nerwowym i nieprzytomnym powrotem.

Dziękuję również Joelowi Deanebwi i Toddowi Lapinowi, którzy wprowadzili mnie w arkana dziennikarstwa, kiedy zaczynałem w 1998 roku, a także Alowi Hugerowi i Deanowi Turnerowi z SecurityFocus.com. Jason Tanz z czasopisma „Wired" włożył wiele pracy w mój artykuł o Maksie *Catch Me If You Can,* opublikowany w styczniowym numerze z 2009 roku.

Wśród moich przewodników w pisaniu tej książki byli policjanci, agenci federalni, hakerzy i carderzy, którzy bezinteresownie poświęcili wiele czasu na rozmowy ze mną. Szczególnie hojny pod tym względem był starszy agent specjalny FBI J. Keith Mularski; także Max Vision spędził wiele godzin przy wię-

ziennym telefonie, jak również pisząc długie maile i listy, w których opowiedział mi swą historię.

Dziękuję inspektorowi Gregowi Crabbowi z US Postal Inspection Service, detektywowi Bobowi Wattsowi z policji w Newport Beach, byłemu agentowi FBI EJ. Hilbertowi i prokuratorowi federalnemu Lukebwi Demboskyemu, któ-

ry nie powiedział mi zbyt wiele, ale zawsze był miły. Jestem również wdzięcz-ny Lordowi Cyrkowi, Lloydowi Liskemu, Th3C0rrupted0ne, Chrisowi Aragonowi, Jonathanowi Giannonemu, Tsengeltsetseg Tsetsendelger, Wernerowi 296

Janerowi, Cesarowi Carranzy i innym weteranom cardingowego półświatka, którzy prosili o zachowanie anonimowości.

Historia Maksa Visiona byłaby bardziej ograniczona do jego przestępczej działalności,

gdyby nie Tim Spencer i Marty Roesch, którzy opowiedzieli mi o swoich doświadczeniach z Maksem jako białym kapeluszem, i Kimi Mack, która mówiła otwarcie o swoim małżeństwie z Maksem. Dziękuję również cudownemu dziecku bezpieczeństwa komputerowego Markowi Maiffretowi, który wyodrębnił niektóre z exploitów Maksa.

Półświatek, w którym zanurzył się Król Hakerów, był opisywany przez wielu doskonałych dziennikarzy, takich jak Bob Sullivan, Brian Krebs, Joseph Menn, Byron Acohido, Jon Swartz i moja koleżanka z „Wired” Kim Zetter.

Na końcu chciałbym podziękować mojej żonie Lauren Gelman, bez której kochającego wsparcia i poświęcenia ta książka pie mogłaby powstać, oraz Sa-delle i Asherowi, którzy będą pod ścisłym nadzorem w czasie korzystania z komputera, dopóki nie ukończą osiemnastu lat.

Spis treści