Bezpieczny Internet - Zadanie

Oprac. Dawid Polowczyk

„Na przestrzeni ostatnich kilkunastu, a nawet kilkudziesięciu lat, powstało kilka szczególnie groźnych wirusów i programów, które określa się dzisiaj jako najniebezpieczniejsze wirusy w historii. O ich złej sławie nie zawsze świadczyły straty finansowe, jakie spowodowały. Czasami była to łatwość i szybkość ich rozprzestrzeniania lub problemy z ich detekcją i usunięciem."

1.Co to jest robak komputerowy?

Samoreplikujący się złośliwy program komputerowy, nie potrzebuje żadnego pliku wykonywalnego. Rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie

2. Co to jest wirus komputerowy?

Złośliwe oprogramowanie posiadające zdolność powielania się przez pliki tzn. potrzebuje i wykorzystuje sam system operacyjny lub inne aplikacje do przenoszenia się i duplikacji

3. Co to jest rootkit?

Rootkit to swego rodzaju narzędzie używane we włamaniach do systemów informatycznych i sieciowych. Ukrywa swoje pliki i procesy, które umożliwiają uzyskanie kontroli nad systemem. Może zostać użyty do np. ukrycia własnych procesów oraz procesów tzw. Trojana lub innego złośliwego oprogramowania.

4. Co to jest backdoor?

Jest to luka w zabezpieczeniach danego systemu, zostawiona celowo, aby można było ją wykorzystać w późniejszym czasie.

5. Co to jest torjan?

Jest to określenie na oprogramowanie, które podszywając się pod inne programy instaluje do systemu niepożądane złośliwe oprogramowanie. Trojan może posłużyć jako nosiciel innego złośliwego oprogramowania np.: Koń trojański, który instaluje oprogramowanie typu rootkit do systemu. Konie trojańskie nie są ściśle rzecz biorąc wirusami, bo nie replikują się.

6. Jaka jest różnica między robakiem a wirusem?

Wirus potrzebuje nosiciela do rozprzestrzeniania się czyli pliku, natomiast robak do rozprzestrzeniania wykorzystuje luki w systemie lub błędy użytkownika

6. Co to jest ransomware?

Oprogramowanie wymuszające okup blokuje komputery i urządzenia przenośne lub szyfruje dokumenty, obrazy i inne istotne pliki. Podobnie jak wirusy, oprogramowanie wymuszające okup często udaje gry i inne rodzaje legalnego oprogramowania. Gdy oprogramowanie wymuszające okup zaszyfruje dane, żąda zwykle pieniędzy.

7. Co to jest podatność (vulnerabilities) ?

Jest to pewnego rodzaju słabość. Odnosi się do braku odporności (systemu lub jednostki)na skutki wrogiego środowiska. Zjawisko podatności wykorzystywane jest przez zagrożenia i prowadzi do strat.

8. Podaj dwa przykłady konkretnego wirusa komputerowego – nazwa, data wykrycia, działanie?

ILOVEYOU *(4 maja 2000) - robak komputerowy napisany w języku VBScript. Robak ma postać skryptu, przez co hakerzy są w stanie łatwo tworzyć jego mutacje. Wirus dotarł do skrzynek e-mailowych z tematem „ILOVEYOU" i załącznikiem „LOVE-LETTER-FOR-YOU.TXT.vbs". Po otwarciu załącznika, wirus wysyłał swoje kopie do każdego z książki adresowej ofiary podszywając się pod nią. Cztery elementy uczyniły wirusa tak niebezpiecznym:*

- *wykorzystywał prostą inżynierię społeczną, aby skłonić użytkowników do otwarcia załączników (ukrywał się pod wieloma rodzajami nazw załączników, jak np. „sprawdź uprzejmie mój list miłosny", czy też „możesz wygrać milion dolarów");*
- *wykorzystywał niedoskonałość programów e-mail, które pozwalały na uruchamianie plików odbieranych w załącznikach przez proste kliknięcie;*
- *wykorzystany mechanizm — VBScript — nie był wcześniej wykorzystywany na taką skalę, żeby zwrócić uwagę na swój potencjał, więc odpowiednie warstwy zabezpieczeń nie były jeszcze stworzone.*
- *W większości komputerów ukryte były nazwy faktycznych rozszerzeń plików, tak więc, na przykład, plik „LOVE-LETTER-FOR-YOU.TXT.vbs" widoczny był jako „LOVE-LETTER-FOR-YOU.TXT*

Większość „strat" było kosztem pozbycia się wirusa z poszczególnych systemów. Pentagon, CIA i Parlament Brytyjski musieli wyłączyć serwery e-mail, żeby pozbyć się robaka, co uczyniło również większość wielkich korporacji. Wirus nadpisywał pliki ważne, ale również muzyczne, graficzne, multimedialne i inne, swoją kopią, którą również wysyłał do wszystkich z listy kontaktów użytkownika.

Narinnat Suksawat, 25-letni tajski informatyk, jako pierwszy na świecie napisał program naprawiający zniszczenia powodowane przez robaka i opublikował go 5 maja 2000 roku, 24 godziny po pierwszych infekcjach. Usuwał on pliki wirusa i odzyskiwał skasowane przez niego pliki systemowe

MELISSA *(około 26 marca 1999) - program rozprzestrzeniał się poprzez wiadomości elektroniczne; do maila dołączany był dokument o zachęcającej do otwarcia nazwie. Po aktywacji, wirus replikował się i wysyłał samoczynnie do 50 kolejnych osób z książki adresowej. „Melissa siała spustoszenie w sieciach rządowych i prywatnych" - takie oświadczenie wydała nie prasa, ale samo FBI. Poza klasycznymi mailami, Melissa rozprzestrzeniała się również za pomocą Usenetu (ogólnoświatowy system grup dyskusyjnych). Melissa, natomiast, stała się znana jako jeden z pierwszych wirusów komputerowych, który w tak szerokim stopniu zaistniał w opinii publicznej.*

9. Podaj dwa przykłady konkretnego robaka komputerowego – nazwa, data wykrycia, działanie?

CODE RED I *(13 lipca 2001) oraz* ***CODE RED II*** *(4 sierpnia 2001) - Robak wykorzystywał błąd w module indeksowania, będącym częścią pakietu IIS i wykonywał następujące działania:*

- *zamieniał treść wszystkich stron pobieranych z danego serwera WWW wyświetlając tekst: „HELLO! Welcome to http://www.worm.com! Hacked By Chinese!",*
- *próbował się kopiować na inne komputery, na których działało oprogramowanie IIS,*
- *czekał 20–27 dni, po których uruchamiał atak typu denial of service (DoS) na kilka wybranych adresów IP (w tym m.in. na komputery Białego Domu),*

Code Red II, działał według dokładnie takiego samego schematu, oprócz tego, że zamiast rozprzestrzeniać się na losowo wybieranych komputerach w internecie, kopiował się na wszystkie dostępne maszyny w intranecie, do którego przyłączony był pierwszy zainfekowany komputer.

Microsoft opublikował 18 lipca 2001 łatę na IIS, która zabezpieczała serwery IIS przed atakiem tego wirusa.

Stuxnet *(czerwiec 2010) - Jest pierwszym znanym robakiem używanym do szpiegowania i przeprogramowywania instalacji przemysłowych. Zawierał rootkit na system Windows. Wykorzystywał też wiele luk 0-day. Wirus miał zdolność aktualizacji metodą peer-to-peer. Podstawową formą rozpowszechniania się robaka są zainfekowane podręczne pamięci USB. Po zainstalowaniu się w systemie operacyjnym Windows robak zaczyna przeszukiwać sieć lokalną w poszukiwaniu podłączonych sterowników PLC, które są często używane w różnego rodzaju fabrykach, rafineriach czy elektrowniach. To absolutnie wyjątkowy wirus. Choćby już tylko dlatego, że to produkt wojskowych. Stany Zjednoczone użyły go jako broni w operacji militarnej wymierzonej w program nuklearny Iranu. Nośnikiem wirusa był pendrive jednego z pracowników. Po instalacji Stuxnet wyszukiwał konkretny sterownik i zmieniał jego ustawienia, doprowadzając np. do przyspieszenia pracy wirówek w zakładzie wzbogacania uranu w Natanz i ich zniszczenia. Czasowo unieruchomił niemal 1000 z 5000 wirówek i opóźnił irański proces wzbogacania uranu o około 1,5 roku.*

10. Podaj dwa przykłady luki/podatności – nazwa, data wykrycia, na czym polega?

Riple20 *(2020) - zestaw 19 nowych podatności w bibliotece TCP/IP stworzonej i dostarczanej przez firmę Treck Inc. oraz implementowanej w szerokiej gamie urządzeń. Za odkryciem podatności stoi izraelska firma JSOF. W dokumencie opisującym szczegółowo Ripple20 możemy przeczytać, że luki różnią się od siebie nie tylko poziomem krytyczności w skali CVSS, ale także trudnością ich realizacji. Cztery zostały sklasyfikowane jako krytyczne (ocena >= 9 w skali CVSS), jedna jako poważna (ocena >= 7 w skali CVSS).*

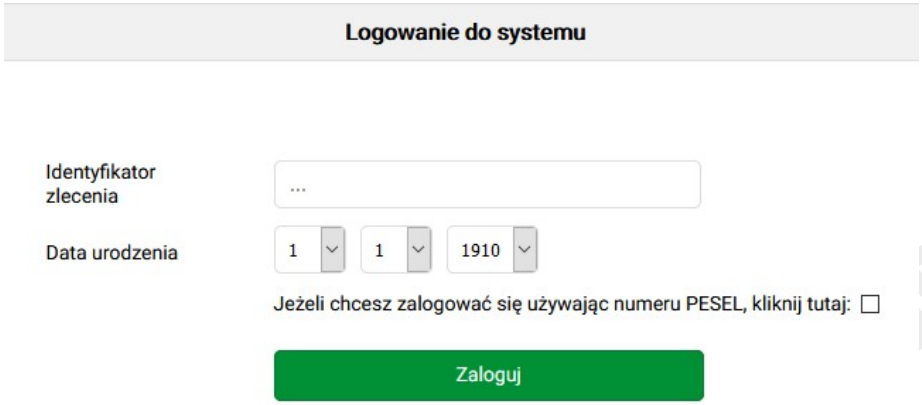
Autorzy dokumentu twierdzą także, że podatności zostały zgłoszone w bieżącym roku i przypuszczają, że mogły znajdować się w kodzie dostarczonym przez Treck Inc od momentu istnienia firmy czyli 20 lat (stąd nazwa Ripple20). Wedle informacji od JSOF, podatne mogą być urządzenia z przeróżnych branż, które wpięte (i nie) do sieci, są podatne na np. możliwość ataku poprzez nieautoryzowane zdalne wykonanie kodu (tzw. Remote Code Execution). Biorąc pod uwagę takie podatne urządzenia jak drukarki, zasilacze UPS czy pompy infuzyjne (por. Rozruszniki serca można zhackować. Także zdalnie).

Można sobie wyobrazić wiele różnych ataków. Poniżej prezentacja ataku ukierunkowanego na podpięty do sieci zasilacz UPS oraz efektu jaki można osiągnąć na innych, podłączonych przez niego do zasilania urządzeń.

https://www.youtube.com/embed/jkfNE_Twa1s?feature=oembed

Publicznie dostępne wyniki badań na koronawirusa (2020)

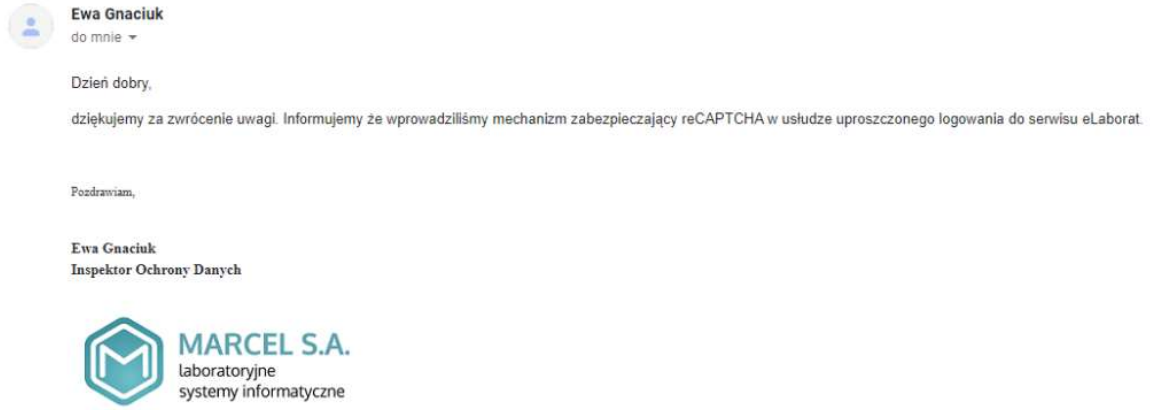
Logowanie do systemu zawierającego wyniki testów na koronawirusa:



Jak widać na powyższych grafikach – aby uzyskać dostęp do swojego wyniku poprzez funkcjonalność „uproszczonego logowania" potrzebne są dwie informacje:

- ***identyfikator zlecenia, gdzie kolejne numery zleceń są rosnące;***
- ***datę urodzenia osoby zlecającej [day=X&month=X&year=X]***

Przy pewnych założeniach ilość kombinacji dat urodzeń możliwych do przypisania do identyfikatora zlecenia, wynosi jedynie około 19 tys. kombinacji. Nie trudno się domyślić, że nie stanowi większego problemu wygenerowanie wszystkich takich kombinacji i sprawdzeniu, czy pasują one do numeru zlecenia. Lepszym zabezpieczeniem jest uzyskiwanie dostępu do wyników zlecenia poprzez odpowiednio długie, losowe hasło, które będzie przychodzić na numer telefonu zleceniodawcy. Błąd na szczęście został dosyć szybko naprawiony, poprzez wdrożenie mechanizmu reCAPTCHA od google:



Pozwoliło to na uzyskanie informacji wrażliwych pacjenta takich jak:

- ***imię;***
- ***nazwisko;***
- ***pesel;***
- ***data urodzenia;***
- ***adres zamieszkania;***
- ***wynik badań;***

Po zgłoszeniu przez badacza firma szybko odpowiedziała oraz skorygowała problem wprowadzając mechanizm CAPTCHA. Niestety bezpieczeństwo tego typu systemów, pisanych często „na szybko" jest prawdopodobnie często bardzo słabe. Niedawno zgłaszana była podatność SQL injection na „ekranie logowania" w innym labie realizującym testy na koronawirusa. Po otrzymaniu zgłoszenie, podatność została szybko naprawiona. Oto przykład jednek z wielu wyników do których można było uzyskać dostęp:

[redacted]

VITO-MED sp. z o.o.
Pracownia Wirusologii
44-100 Gliwice
ul. Radiowa 2
tel. 793-600-112
wirusologia@vitomed.pl
nr.ks.rej. 000000021381

vito-med Sp. z o.o. SZPITAL RADIOWA 2

Identyfikator dokumentu zlecenia:	nie podano
Nr/data w centralnej księdze:	[redacted]
Nr w księdze SARS COV-2:	
Data i godz. rejestracji zlecenia:	

Sprawozdanie z badania laboratoryjnego

Lekarz zlecający: Nie Podano — Typ zlecenia: DT-01 Gliwice

Jednostka kierująca: **Lekarz Podstawowej Opieki Zdrowotnej**
Płatnik: **Narodowy Fundusz Zdrowia**
Miejsce odesłania wyniku: **Zleceniodawca**

[redacted]

PESEL: [redacted] Data urodze[redacted]19[redacted] Wiek: [redacted] **lat** Płeć: [redacted]
Adres: [redacted]
Nr historii choroby: **nie podano** Ident. pacjenta: **nie podano**

WIRUSOLOGIA

Nazwa badania	Wynik badania	Wykonanie
	Materiał: Wymaz z nosogardzieli, pobrany: [redacted] *(Nieczytelny), przyjęty:* [redacted]	
COVID-19 (SARS-CoV-2) -RNA met.RT-PCR	**Pozytywny**	[redacted]

Wynik ujemny (negatywny) nie wyklucza zakażenia SARS-CoV-2.
W przypadku pogorszenia stanu klinicznego pacjenta lub potwierdzenia wysokiego narażenia na zakażenie należy pobrać do badania kolejną próbkę materiału.
Badanie wykonano testem jakościowym Novel Coronavirus (2019-nCoV) Real-time PCR Kit, aparatem Bioer Quant Gene 9600.
Metodologia testu zgodna z zaleceniami Światowej Organizacji Zdrowia (WHO).

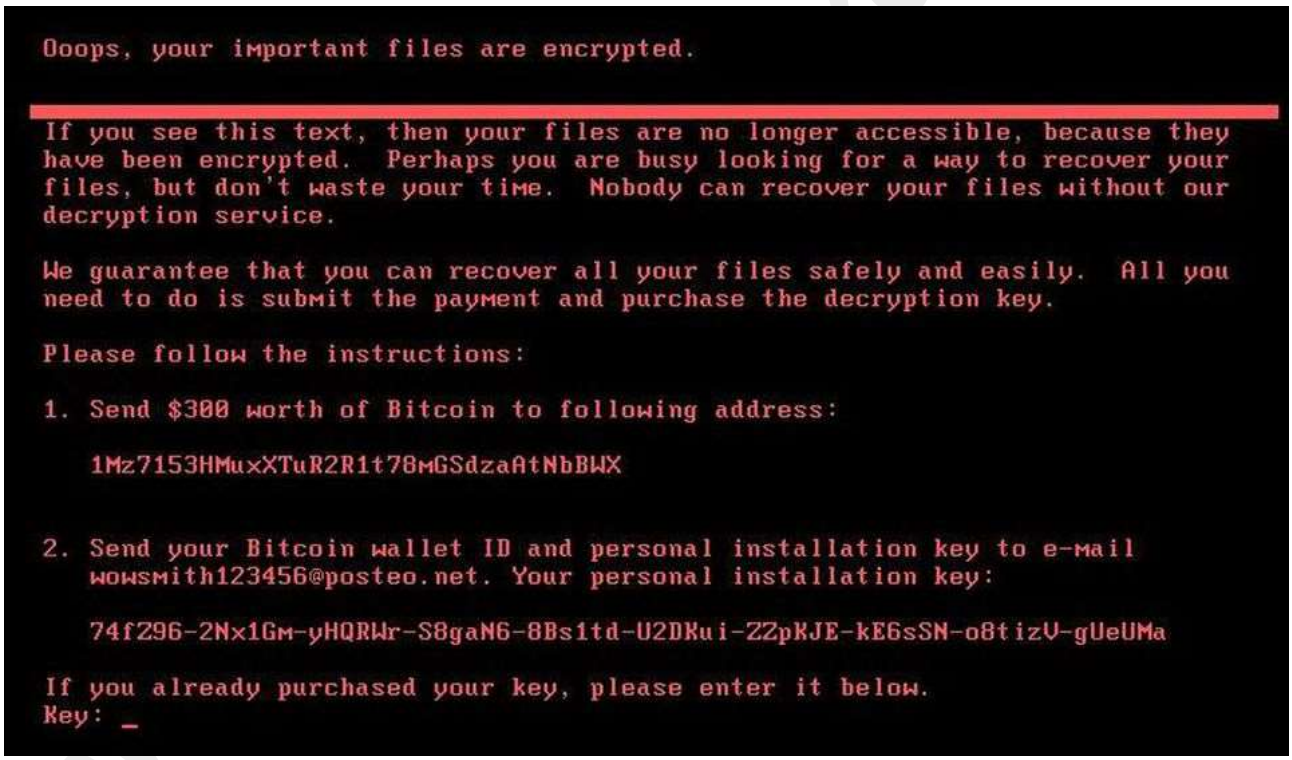
Badanie wykonano z materiału powierzonego.
Makroskopowy stan próbki bez zastrzeżeń.

koniec wyników

11. Podaj dwa przykłady konkretnego ransomware'u – nazwa, data wykrycia, działanie?

WannaCry (2017) *- Ogólnoświatowy cyberatak, który zainfekował ponad 300 000 komputerów w ciągu zaledwie 4 dni. WannaCry propagowany był za pomocą exploita znanego jako EternalBlue i ukierunkowany był na systemy operacyjne Microsoft Windows (najbardziej dotknięte atakiem były komputery z systemem Windows 7). Atak został zatrzymany dzięki awaryjnie wydanymi łatkami przygotowanymi przez firmę Microsoft. Sam malware został udostępniony w sieci 14 kwietnia przez grupę Shadow Brokers. To ci sami, którzy rok temu chwalili się, że ukradli złośliwe oprogramowanie, nad którym pracowała Amerykańska Agencja Bezpieczeństwa Narodowego (NSA).*

NotPetya (2017) - *Jeżeli przyjąć, że WannaCry był początkiem "nowej epoki ransomware", NotPetya stało się jej potwierdzeniem. Petya po raz pierwszy została odnotowana w 2016 roku, a kilka tygodni po pojawieniu się WannaCry została zaktualizowana. Specjaliści ds bezpieczeństwa określili modyfikację jako NotPetya, aby uniknąć pomyłek, gdyż była tak rozbudowana, że diametralnie różniła się od oryginału. Pogłoski mówiły, że nie jest to ransomware, ale narzędzie rosyjskiego ataku na Ukrainę. NotPetya za pomocą MEDoc podczas startu pobrał uaktualnianie serwera upd.me-doc.ua. Podczas zakończenia szyfrowania Master File Table (MFT – umożliwia dostęp do plików na komputerze) wyświetlone zostało żądanie okupu. Jak się później okazało, backdoor był obecny w systemie aktualizacji już od kwietnia. NotPetya została rozpowszechniona poprzez wykradzenie exploitów z NSA takich jak: Eternalblue i Eternalromacne, Doublepulsar (podobnie jak WannaCry).*



12. Jak działał/działa robak Conficker?

*Nazwa wirusa „**Conficker**” to gra słów, która w tłumaczeniu oznacza, że „program manipuluje konfiguracją komputera”. Jeden z groźniejszych znanych dotychczas robaków komputerowych. Pojawił się w sieci w październiku 2008 roku. Atakuje systemy operacyjne z rodziny Microsoft Windows. Robak wykorzystuje znane luki w zabezpieczeniach platformy systemowej Windows Server oraz różne usługi składowe wykorzystywane przez systemy Windows. Robak Conficker rozprzestrzenia się głównie poprzez lukę w Windows Server Service (MS08-067), błąd programistyczny tzw. przepełnienie bufora. Robak wykorzystuje specjalnie spreparowane żądania RPC wykonania kodu na komputerze docelowym.*

Po zainfekowaniu komputera Conficker wyłącza szereg usług systemowych, takich jak:

- ***aktualizacje automatyczne Windows***
- ***centrum zabezpieczeń systemu Windows***
- ***Windows Defender – ochrona przed spyware***
- ***usługa raportowania błędów Windows***

Następnie łączy się z serwerem, gdzie otrzymuje kolejne rozkazy i wytyczne np.: aby gromadzić dane osobowe, oraz pobierać i instalować dodatkowe złośliwe oprogramowanie na komputerze ofiary. Robak „podczepia się” również pod niektóre procesy systemowe, takie jak: svchost.exe, explorer.exe i services.exe. Jedna z modyfikacji robaka Conficker stworzy serwer HTTP i otwiera losowy port z zakresu 1024-10000. Jeżeli zarażony komputer wykonuje polecenia wirusa, następuje nawiązanie połączenia zwrotnego z serwerem HTTP oraz pobranie aktualnej (nowej, zmodyfikowanej) kopii robaka. Dodatkowym działaniem wirusa jest kasowanie punktów przywracania systemu i wysłanie zebranych informacji do komputera docelowego (atakującego). Wirus korzysta z różnych adresów IP co uniemożliwia jego zablokowanie.

Dnia 13 lutego 2009 roku firma Microsoft wyznaczyła po 250 tys. dolarów nagrody dla każdego, kto jest w stanie udzielić informacji mogących pomóc w ujęciu twórcy wirusa.