ODLICZAJĄC DO ZERO

KIM ZETTER

DNIA

STUXNET, CZYLI PRAWDZIWA HISTORIA CYFROWEJ BRONI

Helion

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

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-283-3712-1

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

SPIS TREŚCI

ROZDZIAŁ 1

PIERWSZE OSTRZEŻENIE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pierwszy „strzał" zwiastujący erę wojen cyfrowych padł na przełomie 2009 i 2010 r. w zakładzie wzbogacania uranu pod Natanz w środkowym Iranie. Przedstawiciele jednostki ONZ odpowiedzialnej za monitorowanie irańskiego programu nuklearnego zorientowali się, że wirówki służące do wzbogacania uranu zaczęły się psuć na ogromną skalę bez pozornie wytłumaczalnych przyczyn. Nie wiedzieli jeszcze, że kilka miesięcy wcześniej, w czerwcu 2009 r., ktoś dyskretnie uruchomił niszczycielską broń cyfrową na komputerach w Iranie. **Ta broń, nazwana Stuxnet, po cichu wślizgnęła się do krytycznych systemów w Natanz z jednym zadaniem: sabotować program nuklearny w Iranie**.

Nie, to nie jest kolejna powieść science fiction. Na stronach tej książki znajdziesz całą historię tej pierwszej na świecie cyberbroni, od jej genezy za murami Białego Domu do skutków jej użycia w irańskim zakładzie. Przeczytasz też niesamowitą opowieść o geniuszach, którzy zdołali rozwikłać sekret tego sabotażu. Jednak ta książka to nie tylko fascynująco napisana historia Stuxneta. Znajdziesz tu wizję przyszłości cyberwojen i dowiesz się, co się może stać, jeśli Twój świat będzie celem podobnego ataku. Przekonasz się, że nasza wspaniała cywilizacja Zachodu znajduje się na krawędzi…

KIM ZETTER jest znaną, niezależną dziennikarką z Kalifornii. Zajmuje się różnymi tematami, jednak najlepiej znana jest z artykułów publikowanych w magazynie „Wired" i „PC World" o cyberprzestępstwach, swobodach obywatelskich, prywatności i bezpieczeństwie. Była jednym z pierwszych dziennikarzy opisujących Stuxnet po jego wykryciu. Pisała też o wielu innych sprawach związanych z WikiLeaks, inwigilacją przez agencję NSA i hakerskim półświatkiem. Otrzymała kilka prestiżowych nagród dziennikarskich.

WITAJ W MROCZNYM ŚWIECIE CYBERWOJEN!

CANCEL OK

sięgnij po WIĘCEJ

KOD KORZYŚCI

Helion

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

ISBN 978-83-283-3712-1

Informatyka w najlepszym wydaniu

cena: 39,90 zł