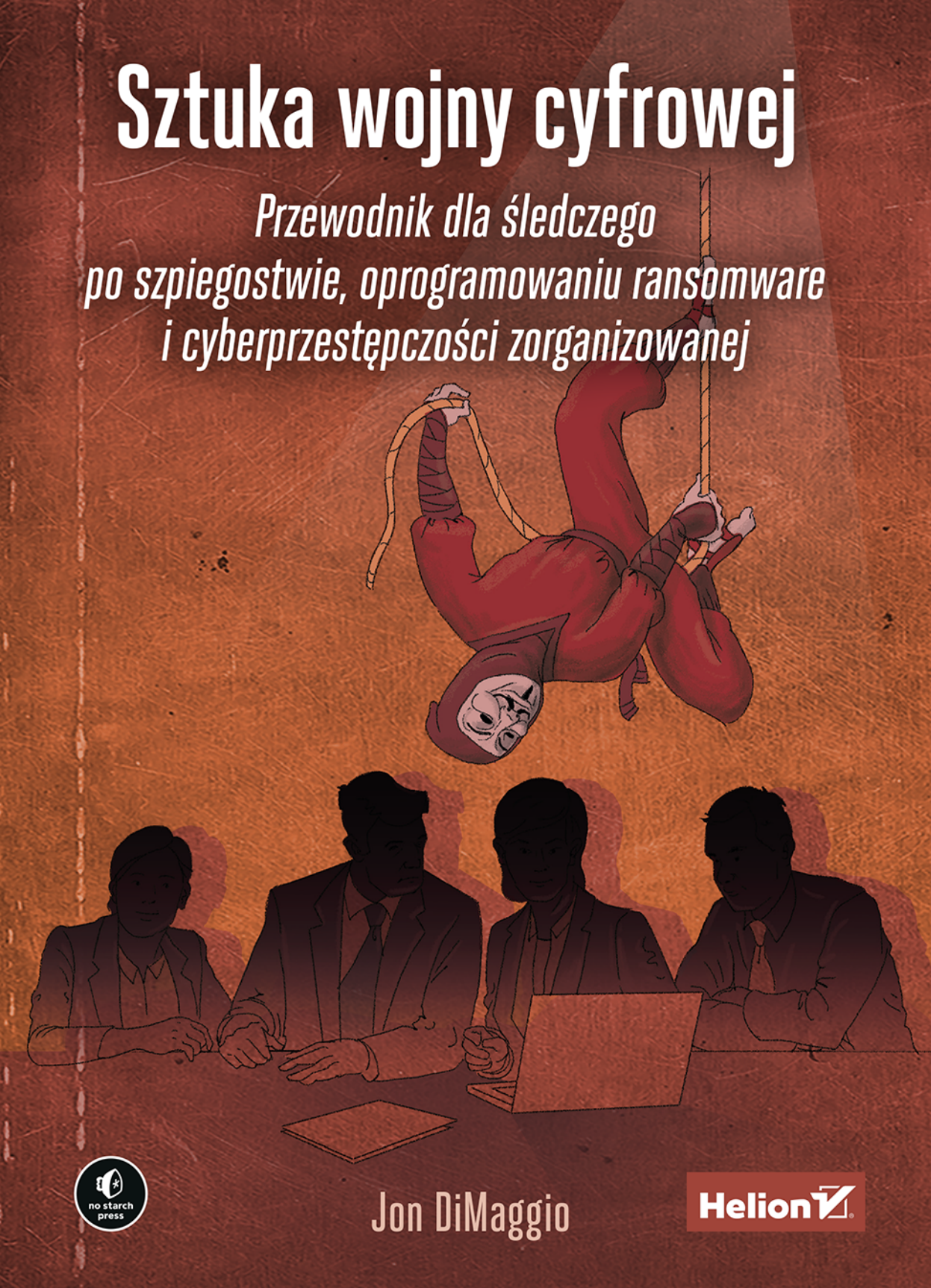
Sztuka wojny cyfrowej

Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej



Jon DiMaggio

no starch press

Helion

Tytuł oryginału: Tytuł oryginału: The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime

Tłumaczenie: Aleksander Łapuć

ISBN: 978-83-8322-081-9

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

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

1

Ataki prowadzone przez organizacje państwowe

Ataki prowadzone przez hakerów na służbie rządów znacznie różnią się od większości zagrożeń, z jakimi możesz mieć do czynienia. W typowych zagrożeniach głównie stosowanym środkiem ataku jest szkodliwe oprogramowanie, więc często do skutecznego przeciwdziałania wystarczą automatyczne narzędzia obronne. Gdy tylko dostawcy oprogramowania antywirusowego opracują sygnatury szkodliwych programów, przechwytywanie i blokowanie ataków następuje automatycznie, bez konieczności ludzkiej interwencji. Zwykły przestępca, gdy jego narzędzie zostanie zablokowane, zazwyczaj weźmie na cel inną ofiarę, ponieważ nie będzie dysponował czasem i środkami niezbędnymi do przeorganizowania nieudanego ataku.

Jednakże automatyczne odparcie ataku hakerów rządowych najpewniej spowoduje zaangażowanie dodatkowych zasobów do osiągnięcia celu. Uporczywość nieraz skutkowała sukcesami w rozpracowywaniu innych rządów, wojska i potężnych prywatnych przedsiębiorstw, takich jak Google lub Sony. Niestety wiele organizacji nieprawidłowo reaguje na ataki rządowe, co prowadzi do druzgocących skutków, znacznie groźniejszych niż powstałe w wyniku ataków przeprowadzanych jedynie dla korzyści finansowych.

W czerwcu 2016 r. dowództwo NATO uznało cyberprzestrzeń za oficjalną domenę działań wojennych[1]. Wcześniej za domeny uznawano fizyczne środowiska

ograniczone wymiernymi granicami, takie jak przestrzeń kosmiczna, lądy, morza i powietrze. Jednak cyberprzestrzeń jest wirtualna i wymaga odmiennych metod nawigowania po niej, gdyż nie ma konkretnych granic. Ale cyberataki mogą mieć bezpośredni wpływ na walki prowadzone w pozostałych domenach, więc stratedzy wojskowi muszą uwzględnić je w doktrynach wojennych.

W tym rozdziale przedstawię tło historyczne obejmujące czasy od narodzin ataków cyberwywiadowczych do współczesności. Kiedy zrozumiesz, czym kierują się agresorzy na usługach obcych rządów, jakie taktyki stosują i jakie zachowania przejawiają, będziesz mógł skuteczniej się przed nimi bronić. Choć omówienie będzie dosyć zwięzłe, powinieneś dzięki niemu zyskać podstawowe pojęcie, jak sobie radzić z podobnymi zagrożeniami.

Chiny

Ye Jianying, jeden z twórców Chińskiej Armii Ludowo-Wyzwoleńczej (ChAL-W), w 1975 r. przedstawił Komitetowi Centralnemu Komunistycznej Partii Chin raport zatytułowany „O wzmocnieniu elektronicznych środków zaradczych". Chińska Republika Ludowa zamierzała prześcignąć Stany Zjednoczone do roku 2049 i stać się światowym supermocarstwem na setną rocznicę swojego powstania. Raport Ye opisywał, jak Chiny mogą wykorzystać broń elektroniczną do wzmocnienia potencjału wojskowego, by zostać znaczącą potęgą światową[2].

Ye wybiegał swoimi koncepcjami w przyszłość. W owym czasie tylko nieliczni uważali, że technologie komputerowe i sieciowe mają znaczenie w wyścigu o globalną dominację. Rząd chiński wykorzystał porady z raportu i zapoczątkował wojskowe programy szkoleniowe ukierunkowane na działania w cyberprzestrzeni. W 1979 r. została założona Wyższa Szkoła Inżynierii Elektronicznej Chińskiej Armii Ludowo-Wyzwoleńczej, która kształciła adeptów wojskowych w zakresie blokowania, zakłócania i unikania elektronicznych transmisji radarowych[3]. Uczelnia wojskowa podlegała jednocześnie władzom krajowym i Sztabowi Generalnemu ChAL-W. Dwanaście lat później rozpoczęto edukację żołnierzy ChAL-W w Szkole Przeciwdziałania Elektronicznego Wojskowego Uniwersytetu Nauki i Technologii. W ramach prowadzonego tam kursu żołnierze zapoznawali się z wykorzystaniem komputerów i sieci, zgłębiając różnorodne zagadnienia, których wiele pozostaje aktualnych do dzisiaj, np. prowadzenie ofensywnych działań informatycznych.

W rezultacie Chiny stały się jednym z pierwszych państw rozwijających zdolności cyberwojenne, co zaowocowało powstaniem jednego z najskuteczniejszych programów cyberwywiadowczych na świecie. Szybki rozwój chińskich sił cyfrowych oraz powiązanych programów wojskowych i badawczych zaczął się przed rokiem 1990 i trwał nieprzerwanie przez kolejną dekadę. Z publicznie dostępnych informacji można wnioskować, że Chiny przynajmniej od 2003 r. prowadzą regularne cyberoperacje, koncentrując się na kradzieży własności intelektualnej[4]. Z czasem ChRL zaczęła wykorzystywać cyberszpiegostwo do umacniania swojej pozycji międzynarodowej. W dalszej części rozdziału opisuję najistotniejsze chińskie operacje w cyberprzestrzeni.

Titan Rain

Wieloletnia, złożona kampania szpiegowska została rozpoczęta w 2003 r. Departament Obrony Stanów Zjednoczonych nadał jej kryptonim Titan Rain. W ramach kampanii przeprowadzono szereg ataków przeciwko znanym laboratoriom inżynieryjnym i wojskowym na terenie Stanów Zjednoczonych[5]. Shawn Carpenter, analityk bezpieczeństwa w Sandia National Laboratories, zdołał zidentyfikować trwające działania ofensywne dopiero rok po ich rozpoczęciu[6]. Carpenter pracował dla firmy Lockheed Martin, uczestniczył w pracach badawczo-rozwojowych nad nowoczesnymi samolotami myśliwskimi. W 2004 r. odkrył, że doszło do włamania do systemów laboratorium i spółki Lockheed Martin, a włamywacze zdołali potajemnie przesłać pewną liczbę plików na własne serwery. W wyniku śledztwa zdołał zlokalizować serwery agresorów, a zebrane dane wskazywały, że atak pochodził z terytorium chińskiego. Rząd Stanów Zjednoczonych z czasem potwierdził, że władze chińskie stały za kampanią Titan Rain, prowadzoną w ramach zakrojonej na szeroką skalę operacji wywiadowczej. Celem działań cyberszpiegów była kradzież informacji o konstruowanych odrzutowcach wojskowych.

Carpenter zdołał rozpracować atak m.in. dzięki spostrzeżeniu, że agresor był zainteresowany przede wszystkim dokumentami na temat technologii lotniczych i kosmicznych. Chińczycy prawdopodobnie zdołali ukraść dane badawczo-rozwojowe niezbędne do budowy myśliwców najnowszej generacji. W ten sposób nie musieli sami inwestować czasu i pieniędzy w prowadzenie badań i zredukowali różnicę w technologiach wojskowych pomiędzy Chinami a Stanami Zjednoczonymi. Chińskie samoloty zyskały osiągi porównywalne z amerykańskimi, ale przy zdecydowanie niższych kosztach w krótszym czasie.

Operacja Titan Rain była jedną z pierwszych kampanii wywiadowczych, o prowadzenie których rząd amerykański publicznie oskarżył rząd chiński[7]. Strona amerykańska nigdy oficjalnie nie zatrzymała żadnego podejrzanego (granice polityczne mogą dosyć skutecznie chronić hakerów przed wszelkimi aktami oskarżenia), jednak od momentu odkrycia kampanii Titan Rain zaczęto identyfikować coraz większą liczbę grup szpiegowskich działających przeciwko Stanom Zjednoczonym z terenu Chin i w służbie rządu chińskiego. Uważa się, że chińskie kampanie cyberwywiadowcze są jednymi z najskuteczniejszych tego typu operacji obserwowanych do tej pory.

Kampanie szpiegowskie Hidden Lynx

Inną chińską grupą szpiegowską o bogatym dorobku jest Hidden Lynx, odpowiedzialna za kilka spektakularnych ataków przeprowadzonych w latach 2011 i 2012[8]. Grupa wzięła na celownik organizacje powiązane z Departamentem Obrony Stanów Zjednoczonych i wiele przedsiębiorstw zajmujących się technologiami informacyjnymi, lotniczymi, kosmicznymi, energetycznymi i wojskowymi.

Jeden z tych ataków był skierowany przeciwko firmie Bit9, dostawcy rozwiązań zabezpieczających i chroniących systemy komputerowe. Atak rozpoczął się w lipcu 2012 r., ale minął co najmniej rok, nim agresorzy zostali zidentyfikowani, a ich działania ujawnione — przez ten czas nieskrępowanie buszowali po sieci ofiary[9].

Grupa dokonała infiltracji infrastruktury spółki Bit9, przeprowadziła rozpoznanie środowiska pracy i wewnętrznych procesów spółki, a następnie wykradła prywatne certyfikaty cyfrowe. Do pierwotnego włamania doszło za pośrednictwem wiadomości phishingowej, której szkodliwa zawartość doprowadziła do instalacji autorskiego wirusa zapewniającego hakerom skryty zdalny dostęp do komputera ofiary. Następnie agresorzy dokonali rozpoznania środowiska firmowego i rozszerzyli zakres włamania, infekując kolejne cele wewnątrz sieci komputerowej.

Kradzież certyfikatu firmy Bit9 i nielegalne posłużenie się nim były wyjątkowo przebiegłym działaniem. Oprogramowanie Bit9 blokuje zagrożenia w sposób odmienny niż większość innych rozwiązań antywirusowych i obronnych. Zamiast korzystać z sygnatur złośliwego oprogramowania i wykrywać szkodliwe treści, produkt Bit9 korzysta z listy dozwolonych plików i aplikacji, które mają prawo być uruchamiane. Dodanie nowych plików do listy następuje po podpisaniu ich stosownym certyfikatem, a każda aplikacja spoza listy jest blokowana. Odkąd grupa Hidden Lynx zdobyła autentyczny certyfikat Bit9, była w stanie dodać dowolny plik do tej listy.

Grupa atakowała także inne wartościowe cele, nie tylko spółkę Bit9. Latem 2013 r. przeprowadziła wieloetapową operację, nazwaną *VOHO*, stosując metodę **zatrutego źródła**. Metoda ta, określana także jako infiltracja strategicznego zasobu sieciowego, polega na przejęciu przez agresora legalnie działającej strony internetowej (źródła) i infekowaniu komputerów łączących się z tą witryną. Hidden Lynx zdołała przejąć kontrolę nad szeregiem witryn często odwiedzanych przez działaczy politycznych, nauczycieli i pracowników przemysłu zbrojeniowego z okolic Waszyngtonu i Bostonu[10]. Agresorzy wiedzieli, że wiele takich osób będzie w jakiś sposób powiązanych z organizacjami politycznymi i rządowymi. Wykorzystując podatność interpretera Javy, instalowali na urządzeniach osób odwiedzających zatrute strony jedno z dwóch szkodliwych narzędzi: Trojan.Naid lub Backdoor.Moudoor. Po pomyślnej początkowej infekcji intruzi analizowali zawartość zaatakowanych systemów i typowali cele o wysokiej wartości, przeciwko którym przeprowadzana była druga faza ataku.

Raport firmy Madiant na temat grupy APT1

Kolejne istotne zdarzenie w historii chińskiego cyberwywiadu miało miejsce w 2013 r. Wtedy firma Madiant, dostawca usług cyberbezpieczeństwa, opublikowała raport ujawniający wieloletnią chińską tajną operację szpiegowską. Analitycy firmy zidentyfikowali jedną z grup działających w ramach ChAL-W, znaną jako Jednostka 61398. Co więcej, zdołali zaprezentować zdjęcia satelitarne budynku, w którym pracowali operatorzy jednostki. Poziom informacji wywiadowczej zebranej przez Madiant był do tej pory niespotykany wśród prywatnych przedsiębiorstw. Przedtem jedynie raporty rządowe lub wojskowe zawierały podobnie szczegółowe informacje.

Oprócz atrybucji ataku armii chińskiej firma Madiant zdołała także ujawnić szczegółowe informacje dotyczące infrastruktury agresorów. Grupie hakerskiej nadano kryptonim *APT1*. W raporcie bardzo dokładnie opisano budowę i działanie

szkodliwego oprogramowania i narzędzi hakerskich, dzięki czemu pozostali dostawcy rozwiązań bezpieczeństwa mogli szybko zaimplementować metody identyfikacji agresorów i obrony przed nimi. Był to pierwszy przypadek w historii, gdy prywatne przedsiębiorstwo zmusiło organizację wojskową do zakończenia swoich działań. Z chwilą opublikowania szczegółów o cyberoperacjach Jednostki 61398 cała jej infrastruktura została wyłączona. Podobnie jak w przypadku kampanii Titan Rain, rząd Stanów Zjednoczonych potwierdził, że to Chiny stały za tymi atakami, a firma Madiant poinformowała, że Departament Sprawiedliwości wystosował akty oskarżenia przeciwko operatorom Chińskiej Armii Ludowo-Wyzwoleńczej zaangażowanym w działania szpiegowskie.

Rząd Stanów Zjednoczonych po raz pierwszy w historii wydał federalny akt oskarżenia przeciwko hakerom, w którym wprost oskarżono obcy rząd o przeprowadzenie cyberataku. Upublicznienie informacji o grupie i podjęte kroki prawne niosły klarowny przekaz dla Chin: powstrzymajcie cyberataki przeciwko organizacjom amerykańskim. Jednak Departament Sprawiedliwości najpewniej miał świadomość, że zatrzymanie podejrzanych będzie niesamowicie trudne, jeżeli w ogóle możliwe — byli oni żołnierzami chińskiej armii i znajdowali się na terytorium chińskim. Na podstawie aktów oskarżenia nigdy nie doszło do aresztowań, a ich wystosowanie było najpewniej metodą poinformowania obcych rządów, że cyberataki przeciwko Stanom Zjednoczonym nie będą tolerowane.

Zawieszenie broni pomiędzy USA a ChRL w 2015 r.

W lipcu 2015 r. na kanale NBC News wyemitowano reportaż o działalności na terenie Stanów Zjednoczonych grup szpiegowskich wspieranych przez Chiny. Ukazana była mapa z zaznaczonymi czerwonymi kropkami pokrywającymi niemal 50 stanów. Każda kropka reprezentowała „udaną chińską próbę kradzieży sekretów przemysłowych lub wojskowych, lub danych na temat amerykańskiej infrastruktury krytycznej, w szczególności energetycznej, telekomunikacyjnej oraz na temat sieci szkieletowej internetu". Innymi słowy: Chiny były zainteresowane infrastrukturą dostarczającą mieszkańcom USA energię i umożliwiającą im komunikację[11].

Relacje pomiędzy Chinami a Stanami Zjednoczonymi były już nadszarpnięte w wyniku wieloletnich cyberataków oraz licznych impasów politycznych. Mapa z anteny NBC, zakładając, że była precyzyjna, wskazywała, jak poważne szkody powodowały cyberincydenty. Długa lista porażonych przedsiębiorstw amerykańskich i organizacji wojskowych stanowiła dowód dla świata, że Chiny z powodzeniem wykorzystały środki cyberwalki, aby wzmocnić swoją pozycję na świecie.

Pod koniec września 2015 r. przewodniczący Chińskiej Republiki Ludowej Xi Jinping odwiedził Waszyngton i spotkał się z prezydentem Stanów Zjednoczonych Barackiem Obamą[12]. Obaj przywódcy poruszali wiele tematów, ale najistotniejsze negocjacje dotyczyły działań w cyberprzestrzeni. Chińskie media podsumowały zawartą umowę w następujący sposób:

> Chiny i Stany Zjednoczone zgadzają się, że w przypadkach złożenia wniosków o przekazanie informacji i udzielenie pomocy w sprawie szkodliwej działalności w cyberprzestrzeni odpowiedzi powinny być

udzielane bezzwłocznie. Co więcej, obie strony deklarują chęć współpracy, w sposób zgodny z odpowiednimi regulacjami krajowymi i stosownymi zobowiązaniami międzynarodowymi, w zakresie prowadzenia śledztw przeciw cyberprzestępstwom, zbierania dowodów elektronicznych oraz powstrzymywania szkodliwej cyberdziałalności prowadzonej z ich terytoriów[13].

W skrócie: obaj przywódcy zgodzili się, aby nie atakować się nawzajem w cyberprzestrzeni. Ale czy umowa nie została zawarta zbyt późno? W owym czasie wielu ekspertów powątpiewało także w jej wiarygodność. Ataki szerzyły się od dłuższego czasu i żadna strona nie przejawiała chęci do wycofania się z konfliktu. ChRL przez lata czerpała korzyści ekonomiczne i polityczne z wykradzionych sekretów handlowych i technicznych. Jako dowód można wskazać, że Chiny mają obecnie znacznie silniejszą pozycję w światowej polityce i walce o dominację niż w 1991 r., gdy zainicjowały swoje programy wojny informacyjnej.

Kilka firm z branży cyberbezpieczeństwa zbadało, czy faktycznie doszło do zawieszenia broni. W 2017 r. firma Symantec, zajmująca się śledzeniem zaawansowanych agresorów na całym świecie, próbowała ustalić, czy w ciągu dwóch lat po zawarciu ugody zmniejszyła się liczba ataków szpiegowskich prowadzonych przez Chiny przeciwko Stanom Zjednoczonym. Sporządziła listę chińskich grup wywiadowczych oraz listy szkodliwego oprogramowania i narzędzi hakerskich używanych przez każdą z grup. Nie każde narzędzie wykorzystywane przez grupę szpiegowską jest unikatowe lub samodzielnie wytworzone, ale Symantec ograniczyła listy wyłącznie do tych przykładów, które mogły być jednoznacznie przypisane do danego agresora.

Do wykonania tego zestawienia użyte były wyłącznie dane pochodzące z ataków przeprowadzonych z użyciem autorskich, unikatowych i wysokiej jakości rodzajów szkodliwego oprogramowania. Autorskie oprogramowanie szpiegowskie zazwyczaj można zaobserwować jedynie podczas wąsko ukierunkowanych ataków, zatem firma Symantec mogła oszacować, czy nastąpiła zmiana w natężeniu takich operacji[14]. Sygnatury szkodliwego oprogramowania użyte do identyfikacji badanych autorskich rozwiązań zostały pobrane z maszyn o potwierdzonych infekcjach. W raporcie zamieszczono następujące podsumowanie:

Poprzez analizę rodzajów szkodliwego oprogramowania używanego przez grupy cyberwywiadowcze, co do których firma Symantec ma uzasadnione przekonanie, że operują z Chin, zdołano zobrazować natężenie działań prowadzonych w badanym okresie. Niemal natychmiast po podpisaniu porozumienia liczba infekcji szkodliwym oprogramowaniem znacząco spadła. W kolejnych miesiącach liczba infekcji nadal spadała i pozostawała na niskim poziomie pod koniec roku[15].

Inaczej mówiąc: umowa obowiązywała. Wszelkie dowody wskazują, że strona chińska dotrzymała swoich zobowiązań. Pozostali dostawcy usług bezpieczeństwa przeprowadzili analogiczne badania i doszli do podobnych wniosków. Niemniej w wielu przypadkach zauważono, że wprawdzie zespoły szpiegowskie przestały atakować cele na terenie Stanów Zjednoczonych, ale kontynuowały działalność przeciwko innym państwom i celom.

To zawieszenie broni nie trwało długo. Z początkiem 2017 r. Obama opuścił urząd, a nowo wybrany prezydent Donald Trump przyjął twardą postawę wobec Chin, jeżeli chodzi o cyberataki i negocjacje handlowe. W miarę jak wzrastało napięcie między państwami, wzrastała też intensywność cyberdziałań. Na przykład w styczniu 2018 r. chiński szpieg o pseudonimie Thrip zainicjował ataki przeciwko przedsiębiorstwom zajmującym się technologiami satelitarnymi, geoinformacyjnymi, obronnymi i telekomunikacyjnymi. Wszystkie firmy, poza jedną, pochodziły ze Stanów Zjednoczonych. Od 2018 r. obserwowany jest wzrost liczby ataków przeciwko Stanom Zjednoczonym przypisywanych Chinom[16].

Rosja

Pewnego wieczoru w 1986 r. administrator systemowy w Lawrence Berkeley National Laboratory w Kalifornii dostrzegł intruza w środowisku komputerowym. Cliff Stoll, z wykształcenia astronom, pracujący jako inżynier systemów, zauważył dziwną rozbieżność księgową, wynoszącą 75 centów.

Zaczął analizować incydent i dosyć szybko zrozumiał, że sprawa jest znacznie poważniejsza niż błąd księgowy. Rozbieżność finansowa spowodowana była brakiem rozliczenia dziewięciu sekund czasu pracy laboratoryjnego komputera. Po krótkim badaniu Stoll ustalił, że niezidentyfikowany haker włamał się do systemu i zdobył uprawnienia administratora. Przeanalizowanie aktywności intruza w sieci laboratorium pozwoliło stwierdzić, że do ataku doszło poprzez 1200-bodowe łącze pochodzące z centrum usług telefonicznych w McLean w Wirginii. Mało prawdopodobne, by ktokolwiek z centrum mógł przeprowadzić taką operację. Stoll uznał, że raczej agresor użył centrum jako stacji pośredniczącej, by ukryć swoją prawdziwą lokalizację, sprawiając wrażenie, że atak pochodzi z McLean. Inżynier opracował więc plan ustalenia faktycznego źródła ataku.

Z pomocą współpracowników Stoll podłączył kilka terminali i dalekopis do wydzielonego segmentu sieci laboratoryjnej, którą agresor wydawał się być najbardziej zainteresowany. Stoll uważał, że przy użyciu podłączonego sprzętu będą mogli śledzić, obserwować i drukować szczegółowe zapisy działalności intruza. Dzięki wysiłkom Stolla pracownicy laboratorium mogli udokumentować każde naciśnięcie klawisza, którego dokonał agresor w trakcie połączenia. Teraz Stoll musiał jedynie czekać, aż zostanie zebrana wystarczająca ilość materiału dowodowego, by przekonać organa ścigania, administrację rządową lub kogokolwiek, kto zechciałby go wysłuchać, że coś groźnego dzieje się we wrażliwych sieciach i systemach laboratorium.

Stoll chciał zrozumieć, jakie są motywy działania agresora, aby ustalić, czego mógł szukać w zasobach laboratorium. Za pomocą swojego tymczasowego systemu monitorowania sieci dostrzegł, że intruz poszukuje wyrażeń związanych z wojskowością i obronnością, które byłyby interesujące wyłącznie dla obcego rządu. W owym czasie technologie sieciowe były jeszcze w powijakach, ale wojsko używało ich powszechnie do zarządzania wrażliwymi systemami i do przechowywania

danych dotyczących satelitów i lokalizacji naziemnych wyrzutni rakietowych. Połączenia sieci wojskowych przechodziły przez systemy laboratorium, stając się łatwym celem.

Stoll zaobserwował, że intruz nie tylko poszukuje wyrażeń związanych z obronnością, lecz także instaluje w systemach laboratorium szkodliwe oprogramowanie zaprojektowane do wyszukiwania i przechwytywania danych uwierzytelniających użytkowników sieci. Co gorsza, wiele kont administratorskich dla różnorodnych technologii i systemów wciąż korzystało z domyślnej nazwy użytkownika i hasła, które zostały ustalone przez dostawcę w momencie instalacji. W wielu innych przypadkach możliwe było uzyskanie dostępu do systemu poprzez aktywne konta gościa, niewymagające podawania hasła. Intruz miał dużą swobodę w dostępie do systemu.

Finalnie Stoll zdołał opisać sposób postępowania intruza, podjęte przez niego działania, godziny aktywności, a także wykorzystywane przez niego języki komputerowe i systemy operacyjne. Haker przejawiał szczególne zainteresowanie systemem obrony przeciwrakietowej związanym z Inicjatywą Obrony Strategicznej (ang. *Strategic Defense Initiative* — SDI). Zgodnie z upublicznionymi informacjami Departament Obrony zainicjował ten program, nazywany programem Gwiezdnych Wojen, w 1984 r. w celu stworzenia środków obrony Stanów Zjednoczonych przed rakietową bronią jądrową[17].

W owym czasie o cyberszpiegostwie jeszcze nie słyszano, więc Stoll musiał przeprowadzić większość dochodzenia samodzielnie — oprócz wykonywania codziennych obowiązków w laboratorium. Jak twierdził, federalne organa ścigania początkowo nie przejawiały zainteresowania włamaniem, ponieważ nie doszło do bezpośrednich strat finansowych. Mimo to Stoll zainicjował kontakt z innymi agencjami rządowymi: Air Force Office of Special Investigations (AFOSI), Centralną Agencją Wywiadowczą (ang. *Central Intelligence Agency* — CIA) i Narodową Agencją Bezpieczeństwa (ang. *National Security Agency* — NSA). W końcu udało mu się przekonać agencje do wysłuchania go.

W celu identyfikacji hakera Stoll postanowił zastawić pułapkę poprzez zwabienie intruza do konkretnej części systemu, dzięki czemu mógłby prześledzić szkodliwą działalność aż do źródła. Było to pierwsze znane zastosowanie pułapki sieciowej, tzw. *honeypot*. Działanie tego rodzaju pułapek polega na przygotowaniu środowiska cyfrowego opartego na fałszywych systemach i danych, by zwieść agresora. Taka przynęta pozwala obrońcom obserwować agresora i zbierać o nim informacje, w miarę jak wchodzi on w interakcje z fikcyjnym środowiskiem.

Stoll wiedział już, że intruz jest szczególnie zainteresowany programem SDI, więc przygotował doskonałą pułapkę. Utworzył konto o nazwie SDInet, którego katalog domowy zapełnił fikcyjnymi, ale pozornie sensownymi dokumentami. Haker połknął haczyk i pozostawił wystarczająco dużo materiału dowodowego, by Stoll, we współpracy z organami ścigania, mógł go zidentyfikować jako Markusa Hessa zamieszkałego w Hanowerze w Niemczech. Okazało się, że Hess był studentem Uniwersytetu w Hadze wynajętym przez KGB do przeprowadzania włamań komputerowych na rzecz ZSRR[18].

Jest to pierwsza znana kampania cyberszpiegowska prowadzona przez Rosję, a jej odkrycie było otrzeźwieniem dla laboratoriów Berkeley i Departamentu Obrony. Po atakach infrastruktura laboratorium została uszczelniona, zbędne konta użytkowników zablokowano i wprowadzono wymogi regularnych zmian haseł uwierzytelniających. Program SDI był prowadzony przez wiele kolejnych lat, a w 1993 r. jego główne cele zostały przeformułowane, aby skupić się na obronie przed pociskami balistycznymi, a mniej zajmować się instalacjami kosmicznymi.

Nie był to ostatni rosyjski atak cyberwywiadowczy. Obecnie w Rosji działa jeden z najbardziej zaawansowanych na świecie ofensywnych programów operacji w cyberprzestrzeni. Jak dowiesz się z tego rozdziału, Rosja wielokrotnie skutecznie wykorzystywała szkodliwe oprogramowanie w połączeniu z kampaniami dezinformacyjnymi i manipulacyjnymi, by osiągnąć zamierzone cele militarne lub polityczne.

Moonlight Maze

Drugiego kwietnia 1999 r. zespół agentów FBI wsiadł w Dulles w Wirginii na pokład samolotu linii Delta realizującego lot numer 2772 do Moskwy. Mieli przeprowadzić dochodzenie w sprawie znacznego cyberataku wymierzonego w Departament Stanu USA. Atakowi nadano kryptonim *Moonlight Maze*. Agenci podejrzewali, że Rosja jest zaangażowana w koordynację ataków przeciwko Stanom Zjednoczonym. Podczas poprzedniego śledztwa, w czasie którego FBI konsultowało się z ambasadorem Stanów Zjednoczonych w Rosji, zebrano dowody wskazujące, że badany incydent nie był osamotnionym atakiem, ale częścią długoterminowej, złożonej i wysoce skoordynowanej operacji mającej na celu kradzież wrażliwych danych od rządu Stanów Zjednoczonych[19].

Śledztwo w sprawie operacji Moonlight Maze zaczęło się blisko rok przed wspólną wyprawą agentów AFOSI i FBI do Moskwy. Obie agencje znalazły dowody cyberataku wymierzonego w organizacje wojskowe, rządowe i edukacyjne wielu krajów, lecz chciały określić sposób działania agresorów, stosowane techniki i narzędzia. W tym celu konieczne było ustalenie, czy zagraniczne służby wywiadowcze koordynowały ataki. A jeżeli tak było — to którego kraju.

Grupa zadaniowa miała twardy orzech do zgryzienia. Agresor zdołał zinfiltrować infrastruktury wielu organizacji podlegających Departamentowi Obrony, włączając w to bazę lotniczą Wright Patterson i laboratoria badawcze armii Stanów Zjednoczonych. Na jego celowniku znalazło się także wiele jawnych systemów wojskowych. Przeciwnik wykorzystał na potrzeby ataku infrastrukturę kilku amerykańskich uniwersytetów. Szkoły nie były głównymi celami, ale ich infrastruktura została przejęta przez hakerów, którzy wykorzystywali te zasoby na dalszych etapach operacji.

FBI rozpoczęło działania od przeprowadzenia rozmów z ofiarami ataków z wydziałów informatyki i inżynierii poszkodowanych uniwersytetów. W szczególności wypytywano o wykorzystanie danych uwierzytelniających i haseł do kont. Czy to samo hasło było używane dla kilku różnych kont? Czy dane uwierzytelniające były dzielone przez kilka osób? Obecnie takie pytania rzadko są zadawane

w ramach oficjalnego śledztwa, ponieważ kradzieże danych logowania są codziennością. Ale w latach 90. ataki komputerowe nie zdarzały się często, a śledczy FBI mieli doświadczenie jedynie w dochodzeniach dotyczących fizycznych ludzi, nie świata cyfrowego. Gdy stało się jasne, że żadna z ofiar kradzieży danych uwierzytelniających nie brała świadomego udziału w przeprowadzeniu ataku, zespół dochodzeniowy zwrócił uwagę na dowody cyfrowe. Zebrane i przeanalizowane zostały dzienniki zdarzeń z wielu skompromitowanych systemów uniwersyteckich.

Aż wreszcie 29 lipca 1998 r. do agenta pracującego w grupie dochodzeniowej Moonlight Maze zadzwonił przedstawiciel organizacji South Carolina Research Authority (SCRA)[20]. Rozmówca stwierdził, że padł ofiarą niezidentyfikowanego hakera z Rosji. I że agresor wykorzystał infrastrukturę SCRA, aby połączyć się z komputerem w bazie lotniczej Wright Patterson.

Był to przełom w śledztwie, którego potrzebowało FBI. Zespół SCRA prawidłowo rozpoznał, że ich systemy są atakowane, i zdołał zebrać szczegółowe informacje o ataku, włączając w to dowody przesyłania plików z bazy Wright Patterson przez infrastrukturę SCRA do komputera znajdującego się w Rosji. Zapisy z dzienników zdarzeń, zawierające szczegółowe informacje o wykradzionych plikach i połączeniach realizowanych z użyciem serwerów SCRA, pozwoliły zrozumieć cele agresora. Dokumenty, którymi interesował się intruz, zawierały rysunki techniczne i wyniki badań dotyczące technologii obronnych służących do wykrywania i unieszkodliwiania międzykontynentalnych nuklearnych pocisków balistycznych. Poszukiwane przez agresora informacje dotyczyły mechanizmów ochrony Stanów Zjednoczonych przed atakiem rakietowym. Tylko przeciwnik zainteresowany atakiem jądrowym mógłby skorzystać z posiadania tych informacji. Niemniej dowody były wciąż niewystarczające, aby jednoznacznie zidentyfikować sprawcę.

W styczniu 1999 r. doszło do serii nowych udanych ataków przeciwko ośrodkowi Brookhaven National Laboratory, Departamentowi Obrony i kilku systemom Departamentu Obrony zlokalizowanym w Vichsburgu w stanie Missisipi. W odpowiedzi Departament Obrony przygotował serwer pułapkę, podobnie jak to zrobiono wcześniej w laboratorium Berkeley. Oficjalne raporty podają, że zdołano ustalić położenie agresora dzięki programowi śledzącemu osadzonemu w dokumentach stanowiących przynętę. W ten sposób przedstawiciele Departamentu Obrony mogli podążyć za dokumentami wprost do faktycznej lokalizacji hakera. Skradzione pliki zostały przesłane na adres IP należący do Rosyjskiej Akademii Nauk, organizacji finansowanej przez rząd w Moskwie i powiązanej z rosyjską armią[21].

Wkrótce po tych wydarzeniach media podchwyciły opowieść. Raporty prezentowane na antenie telewizji ABC i na łamach dziennika „New York Times" szczegółowo prezentowały wielopoziomowy atak. W obu raportach opisywano tę kampanię jako szereg działań podjętych przez obcy rząd i trwających wiele lat, których celem było wykradzenie wrażliwych informacji ze Stanów Zjednoczonych[22]. Jednak ujawnienie ataku nie odstraszyło agresora. I choć światowe media przypisywały przeprowadzenie kampanii Moonlight Maze Rosji, hakerzy kontynuowali swoje działania i przejmowali nowe cele. W niedługim czasie rosyjski haker zdołał się włamać do dwóch kolejnych laboratoriów związanych z Departamentem Obrony.

Wreszcie nastąpił koniec długotrwałej kampanii wywiadowczej, a wkrótce potem, 2 kwietnia 1999 r., odbyła się podróż agentów FBI do Moskwy. W ramach tej podróży agenci spotkali się z wyższym rangą personelem wojskowym w centrali rosyjskiego Ministerstwa Obrony[23]. Jak podają raporty, przedstawili stronie rosyjskiej oskarżenie i wspierające je informacje. W jednym z punktów uwzględnione zostały szczegółowe dowody wskazujące na pochodzenie ataku z serwerów związanych z Rosyjską Akademią Nauk. Kolejnego dnia śledczy zamierzali właśnie udać się z hotelu do Ministerstwa Obrony, aby kontynuować rozmowy. Zamiast tego rosyjska eskorta skierowała zespół na przymusową wycieczkę krajoznawczą. Po kilku dniach stało się jasne, że nie należy się spodziewać żadnej pomocy od strony rosyjskiej. Wkrótce po tym agenci powrócili do kraju. Wprawdzie wyprawa FBI do Rosji nie przyniosła żadnych konkretów, ale dzięki staranności i rzetelnemu postępowaniu analitycznemu zdołano zidentyfikować zagraniczną infrastrukturę, narzędzia, podatności infekowanych systemów oraz szkodliwe oprogramowanie, które były wykorzystywane w ramach kampanii Moonlight Maze. Zebrano przekonywujące dowody, że ataki pochodziły z terytorium Rosji.

Więcej informacji na temat kampanii możesz znaleźć w szczegółowym i precyzyjnym podsumowaniu śledztwa, napisanym przez Chrisa Domana, pt. *The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History*, które jest dostępne na stronie *Medium.com*.

Konflikt z Estonią

W ramach procesu dekomunizacji w lutym 2007 r. estoński parlament przyjął ustawę o demontażu pomników gloryfikujących sowiecką okupację. W owym czasie wciąż nierozwiązany był spór pomiędzy Estonią a Rosją o regiony przygraniczne. Rejony te, po uzyskaniu przez Estonię niepodległości w 1918 r., były częścią jej terytorium, ale z chwilą rozpoczęcia okupacji Estonii przez Związek Radziecki w 1940 r. zostały przejęte przez Rosyjską Federacyjną Socjalistyczną Republikę Radziecką[24].

W konsekwencji uchwalenia ustawy o demontażu usunięto w stolicy kraju, Tallinnie, pomnik upamiętniający wyzwolenie Estonii spod hitlerowskiej okupacji przez Armię Czerwoną. Pomnik ten był punktem spornym, ponieważ rosyjskie wojska pozostały w Estonii także po zakończeniu wojny, a samo państwo zostało wcielone do Związku Radzieckiego, z czym wielu Estończyków się nie zgadzało. Moskwa dodatkowo pogłębiała ten konflikt poprzez wywózki i aresztowania obywateli estońskich pozostałych na terenie Rosji.

Usunięcie pomnika wzbudziło niepokój władz rosyjskich, które publicznie potępiły postępowanie Estonii. Wkrótce potem, 27 kwietnia, wiele istotnych serwisów internetowych Estonii zostało porażonych potężnym rozproszonym atakiem wymuszenia odmowy świadczenia usług (ang. *Distributed Denial of Service* — DDoS)[25]. W wyniku cyberataku kilka estońskich banków nie było w stanie realizować operacji do połowy maja, pozbawiając klientów dostępu do pieniędzy. Dotkniętych zostało także wiele stron rządowych i prywatnych.

Co może być zaskakujące, do wyłączenia znaczącej części estońskiej infrastruktury cyfrowej nie trzeba było działań wysoko kwalifikowanego hakera. Wystarczyło zastosować podstawowe ataki DoS, które skutecznie wysyciły zasoby wybranych serwerów, uniemożliwiając świadczenie usług prawowitym użytkownikom. Na celownik zostały wzięte serwery webowe, DNS, pocztowe i baz danych SQL z terenu całej Estonii. W trakcie ataku infrastruktura wspierająca administrację rządową, telekomunikację, organa ścigania, środki masowego przekazu i instytucje finansowe była całkowicie unieruchomiona, pozbawiając społeczeństwo dostępu do wielu krytycznych usług. W ramach ataku zawartości witryn sieciowych estońskich ugrupowań politycznych zostały podmienione na prorosyjskie przekazy wyświetlane odwiedzającym internautom.

Agresor wykorzystał także bardziej zaawansowaną metodę działania, która nie była wtedy jeszcze szeroko rozpowszechniona: stworzył ogromny botnet. **Botnet** łączy wiele zainfekowanych komputerów, nazywanych **maszynami zombi**, których zasobami może rozporządzać atakujący. W przypadku ataku na Estonię botnet został utworzony w wyniku przeprowadzenia intensywnej kampanii spamowania, za pomocą której wirus został zainstalowany w systemach ofiar. Po infekcji szkodliwe oprogramowanie wykorzystywało konto pocztowe ofiary i wysyłało wiadomości do pierwszych 50 osób znajdujących się w książce adresowej. Pozornie nie wygląda to na poważne zagrożenie, lecz wyrządzone szkody były znaczne. Atakujący wysyłali tak wiele wiadomości utworzonych przez boty, że serwery pocztowe ulegały awariom w wyniku przeciążenia. Estonia oficjalnie oskarżyła Rosję o przeprowadzenie ataku, jednak strona rosyjska wyparła się odpowiedzialności, wskazując jako winnych grupy patriotycznie i prorosyjsko nastawionych hakerów. Estonia nie zdołała dostarczyć dowodów potwierdzających jej stanowisko.

Konflikt z Gruzją

W 2008 r. Gruzja rozpoczęła budowę podmorskich kabli komunikacyjnych, mających zapewnić połączenie krajowej sieci szkieletowej z Europą Zachodnią. Łącze miało zapewnić dostęp do internetu o zwiększonej przepustowości, umożliwiając technologiczny rozwój kraju[26]. Inwestycja spowodowała nasilenie napięcia między Gruzją a Rosją, która obawiała się wzmocnienia politycznej niezależności Gruzji i zmniejszenia uzależnienia od infrastruktury na terytorium rosyjskim.

W lipcu, gdy projekt budowy zbliżał się do końca, strona prezydenta Gruzji Michaiła Saakaszwilego padła ofiarą ataku DDoS. Atakujący zalali serwis komunikatami protokołów ICMP, TCP i HTTP, doprowadzając do jego wyłączenia na ponad 24 godziny. Była to pierwsza oznaka poważnego ataku, który trwał przez kilka tygodni.

Kolejny atak DDoS na Gruzję został przeprowadzony 8 sierpnia, w dniu rozpoczęcia inwazji wojsk rosyjskich na terytorium gruzińskie. W owym czasie większość gruzińskiego ruchu internetowego przechodziła przez infrastrukturę rosyjską, przez co Gruzja pozostawała bezbronna wobec rosyjskich cyberataków i inwigilacji. Już drugi raz tego samego lata strona prezydenta oraz strony Ministerstwa Obrony, Ministerstwa Spraw Zagranicznych i gruzińskich mediów znalazły się

pod cyberostrzałem. Następnego dnia nastąpił atak na ważne gruzińskie instytucje finansowe, kluczowe dla krajowej gospodarki. Oprócz prowadzenia ataków DDoS hakerzy przejęli także pewne serwisy internetowe i zamieścili na nich rosyjskie materiały propagandowe. Według informacji podawanych przez niektóre media zaatakowana została również infrastruktura zapewniająca łączność internetową z Gruzją w takich krajach jak Turcja lub Ukraina.

Ataki DDoS i przejmowanie stron internetowych trwały przez cały sierpień. Na koniec miesiąca Gruzja, z pomocą dostawców usług internetowych, zdołała zablokować źródło ataków i przywrócić działanie infrastruktury. Uważa się, że to Rosja stała za tymi atakami, ze względu na zbieg ich wystąpienia z terminem inwazji rosyjskiej na Gruzję. Niemniej oskarżenie to nigdy nie zostało udowodnione.

Buckshot Yankee

Tego samego roku nieznany intruz włamał się do sieci Departamentu Obrony Stanów Zjednoczonych. W październiku obrońcy sieciowi zidentyfikowali szkodliwe oprogramowanie, któremu później firma F-Secure nadała nazwę *Agent.btz* (w skrócie: BTZ). Wirus z wnętrza sieci rządowej nawiązywał połączenie do własnego serwera dowodzenia i kierowania (ang. *command and control* — C&C). Narzędzie zostało zaprojektowane w niesamowicie wyrafinowany sposób i było niezwykle trudne do wykrycia po instalacji w systemie ofiary. Agresor użył niecodziennego wektora ataku, by uzyskać początkowy dostęp do systemów departamentu, co wyróżniało tę operację na tle innych organizowanych przez obce rządy. W pobliżu budynków rządowych zostały podrzucone pamięci USB zawierające oprogramowanie BTZ. Według przedstawicieli wojska co najmniej jeden pracownik lub żołnierz znalazł zainfekowany dysk i podłączył go do systemu w sieci Departamentu Obrony, doprowadzając do infekcji. Przedstawiciele departamentu przypisują autorstwo odnalezionego szkodliwego oprogramowania BTZ zagranicznej agencji wywiadowczej[27].

Oprogramowanie z dysku USB było rodzajem robaka internetowego, zaprojektowanego, by po aktywacji w docelowym środowisku rozprzestrzeniać się na inne systemy. W miarę infekowania nowych maszyn narzędzie przeszukiwało dysk pod kątem dokumentów biurowych, zwłaszcza zawierających informacje niejawne, i przesyłało pliki do zagranicznych serwerów[28]. Ze względu na zdolność do szybkiego rozprzestrzeniania wirusa specjaliści Departamentu Obrony potrzebowali ponad 14 miesięcy, by zneutralizować zagrożenie. Początkowo stosowane podejście, polegające na identyfikowaniu każdego zainfekowanego systemu i usuwaniu z niego oprogramowania BTZ, okazało się nieskuteczne.

W celu efektywnego zwalczania szkodliwego narzędzia specjaliści Departamentu Obrony poddali analizie komunikaty wymieniane między oprogramowaniem a serwerem C&C. Zainstalowali serwer pośredniczący w komunikacji pomiędzy wirusem a prawdziwym serwerem dowodzenia i kierowania, zdobywając w ten sposób wgląd w strukturę przesyłanych danych. Na podstawie zebranych informacji obrońcy zdołali podszyć się pod serwer dowodzenia i wysłali do narzędzia polecenie zakończenia pracy, kończąc w ten sposób infekcję w sieciach

Departamentu Obrony. Według dziennika „Washington Post", który opublikował tę historię, wywiad ustalił, że kampania, której nadano kryptonim Buckshot Yankee, najpewniej była prowadzona przez jedną z rosyjskich agencji wywiadowczych[29]. Analizy przeprowadzone przez firmy świadczące usługi w zakresie bezpieczeństwa wskazywały, że agresorzy pozostawali aktywni w porach, które pokrywały się z godzinami typowego dnia roboczego w Moskwie. Dalsze badania wykazały, że podobne ataki trwały kilka lat przed odkryciem w 2008 r. wirusa BTZ. Wcześniejsze ataki były ukierunkowane przeciwko wielu organizacjom dyplomatycznym, politycznym i związanym z wojskiem — profil każdego z tych celów pokrywał się z profilem leżącym w obszarze zainteresowania rosyjskich hakerów.

Red October

W styczniu 2013 r. firma Kaspersky, rosyjski dostawca usług cyberbezpieczeństwa i oprogramowania antywirusowego, opublikowała raport zawierający szczegóły długoterminowej kampanii szpiegowskiej uruchomionej w celu kradzieży informacji z „organizacji dyplomatycznych, rządowych i badawczo-naukowych". Ofiarami padały cele w różnych krajach, głównie w rejonie Europy Wschodniej, zwłaszcza pośród byłych republik ZSRR. Agresorzy atakowali także cele w Azji Centralnej[30]. Operacja, której nadano kryptonim *Red October*, rozpoczęła się co najmniej w 2007 r., mniej więcej w trakcie konfliktu estońskiego, ale została odkryta dopiero w 2013 r.

Wnioski z analizy firmy Kaspersky wskazywały, że niektóre z celów obranych przez agresora są zbieżne z profilem preferowanym w czasie ataków prowadzonych przez niektóre rządy. Pośród celów były organizacje wojskowe i rządowe, ambasady dyplomatyczne, uniwersytety, firmy energetyczne i organizacje zajmujące się aeronautyką, zwłaszcza specjalizujące się w dziedzinie napędów rakietowych. Wydaje się, że cele te są bardzo różnorodne, ale fakt, że ataki trwały ponad sześć lat, sugeruje, iż cele te były starannie dobierane, a nie przypadkowe. Podmioty działające w tych branżach zazwyczaj dysponują dosyć skutecznymi środkami obronnymi i możliwościami monitorowania sieci. Mimo to agresor zdołał wykorzystać szkodliwe oprogramowanie utworzone do identyfikowania, zbierania i wykradania konkretnych rodzajów informacji, m.in. dokumentów Microsoft Office i wiadomości e-mail oraz wrażliwych informacji z baz danych[31].

Kampania ta pozostaje jednym z najbardziej zaawansowanych ataków przeprowadzonych do tej pory. Znacznie przewyższała inne operacje pod względem precyzji wykonania, złożoności użytego szkodliwego oprogramowania i sukcesów odniesionych przez agresora. O poziomie sukcesu świadczy fakt, że kampanii nie wykryły automatyczne rozwiązania bezpieczeństwa, zespoły chroniące sieci, badacze bezpieczeństwa i specjaliści rządowi, pomimo aktywnych działań prowadzonych od roku 2007 do co najmniej 2013.

Szczególnie imponującym rozwiązaniem w używanym szkodliwym oprogramowaniu, któremu badacze firmy Kaspersky nadali kryptonim Sputnik, była możliwość infekowania szerokiego spektrum celów poza tradycyjnymi systemami komputerowymi, np.: telefonów komórkowych, elementów sieciowych takich jak rutery,

przełączniki i zapory, a nawet urządzeń USB dołączanych do zainfekowanych systemów. Szkodliwe oprogramowanie miało budowę modułową, pozwalającą dostosować działanie narzędzia do dowolnego środowiska i scenariusza infekcji bez potrzeby modyfikacji kodu. Zawierało moduły realizujące rozpoznanie, kradzież danych uwierzytelniających, kradzież wiadomości e-mail, kradzież danych z dysków USB, rejestrowanie wprowadzanych klawiszy, ustanawianie trwałej obecności w zainfekowanych systemach, rozprzestrzenianie i dystrybucję wirusa oraz pobieranie wykradzionych informacji.

Sposób zaprojektowania i techniczne możliwości niektórych modułów odróżniają oprogramowanie Sputnik od innych rozwiązań obserwowanych w użyciu. Na przykład moduł poczty elektronicznej pozwala na kradzież treści listów i zawartości baz danych z serwerów pocztowych. Jeżeli ofiara podłączy telefon do zainfekowanego komputera, to moduł komórkowy wykradnie z podłączonego urządzenia informacje takie jak książki adresowe, historię połączeń, a nawet treści wiadomości tekstowych.

Dzięki modułowi do wykradania danych uwierzytelniających agresorzy mogli uzyskiwać dostęp do kolejnych obszarów w atakowanym środowisku. Dane uwierzytelniające kont o wyższych uprawnieniach umożliwiały dostęp do wrażliwych aplikacji i danych oraz do narzędzi administracyjnych. Korzystając z dostępu o podwyższonych uprawnieniach, intruzi mogli instalować moduł gwarantujący ponowną infekcję systemu w razie, gdyby oryginalne szkodliwe oprogramowanie zostało skasowane lub usunięte ze środowiska.

Moduł USB dostarczał kilku ciekawych funkcji. Zgodnie z oczekiwaniami pozwalał na kradzież danych z podłączonych nośników USB. Ale pozwalał także na odzyskiwanie uprzednio usuniętych danych z takiego nośnika. A w razie problemów z ustanowieniem połączenia sieciowego, np. w systemie fizycznie odłączonym od sieci komputerowej, narzędzie Sputnik mogło działać za pomocą modułu USB i zachowywać zebrane dane na podłączonym nośniku[32].

Kolejnym przejawem złożoności i zaawansowania oprogramowania Sputnik była jego rozbudowana infrastruktura dowodzenia i kierowania. Zastosowano kilka warstw serwerów zastępczych i pośredniczących w komunikacji pomiędzy atakującymi a zainfekowanymi systemami, dzięki czemu agresorzy byli zabezpieczeni przed wykryciem. Narzędzie mieszało transmisje wykradzionych informacji z bezsensownymi danymi, przez co trudniej było zidentyfikować i przeanalizować jego aktywność. Dodatkowo w kodzie narzędzia zamieszczono fałszywe poszlaki, utrudniające określenie atrybucji ataku. Na przykład w ramach operacji Red October atakujący umieszczali pośród własnych dokumentów kody narzędzi używanych wcześniej przez znaną grupę hakerską z Chin. Sygnatury tego kodu były publicznie znane, a jego istnienie w ramach narzędzia Sputnik miało zmylić śledczych.

Głębsza analiza wykazała istnienie w kodzie szkodliwego narzędzia kilku tekstów w języku rosyjskim. Powszechnie przyjmuje się, że za tym atakiem stali Rosjanie, choć brak jest ku temu twardych dowodów. Wątpliwości budzi fakt, że pośród celów operacji Red October znalazło się także kilka rosyjskich podmiotów rządowych, takich jak Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej.

Po opublikowaniu pod koniec 2013 r. informacji na temat ataków działania w ramach kampanii zostały wstrzymane. Atakujący porzucili swoją infrastrukturę, a grupa hakerska czasowo zniknęła z areny cyberdziałań. Po krótkiej przerwie hakerzy wznowili operację przy użyciu nowych narzędzi. Mimo działania pod nową nazwą CloudAtlas i wykorzystywania nowych rodzajów szkodliwego oprogramowania i narzędzi hakerskich niezmienione pozostały cele operacji.

Iran

Iran przez ponad dwie dekady rozwijał infrastrukturę niezbędną do prowadzenia własnych kampanii szpiegowskich i sabotażowych. Mając na celu osiągnięcie politycznej, religijnej i wojskowej dominacji na Bliskim Wschodzie, Teheran kierował ataki przeciw zagranicznym rządom, m.in. przeciwko Stanom Zjednoczonym i kilku bliskowschodnim państwom. Iran wykorzystuje także cyberoperacje do śledzenia i szpiegowania własnych obywateli, których poglądy często stoją w konflikcie z oficjalną doktryną islamistyczną rządu. Bojąc się, że obywatele mogliby omijać rządowy nadzór i filtry sieciowe, władze w Teheranie zabroniły korzystania z mediów społecznościowych, wirtualnych sieci prywatnych (VPN) i aplikacji z szyfrowaną komunikacją[33].

Dostępne informacje wskazują, że Islamska Republika Iranu rozpoczęła prowadzenie rządowych cyberoperacji ok. 2007 r. Jednakże początki zdolności cyfrowych Iranu sięgają najwcześniejszych lat XXI w., kiedy to kilka irańskich grup hakerskich zwróciło uwagę opinii publicznej.

Wczesne lata

W lutym 2002 r. irańscy hakerzy założyli grupę Ashiyane Digital Security Team, obecnie dobrze znaną irańską grupę hakerską. Złą sławę grupy zapoczątkowało przejmowanie ważnych stron internetowych i umieszczanie na nich własnej treści, co było typową działalnością wczesnych grup hakerskich w Iranie[34]. Grupa podmieniła treści na wielu stronach, m.in. rządowych stronach USA i Izraela, stronach NASA i Mosadu, za każdym razem umieszczając proirańskie komunikaty oraz wyrazy poparcia dla Ashiyane.

Grupa założyła także forum internetowe, gdzie użytkownicy dyskutowali na różnorodne tematy związane z cyberbezpieczeństwem. Forum katalizowało wzrost społeczności hakerskiej w Iranie, bo każdy jego użytkownik mógł działać pod szyldem grupy Ashiyane. Jednakże to pierwszych 12 członków rozsławiło grupę. Najsłynniejszym jest założyciel grupy, Behrooz Kamalian, często określany hakerskim przydomkiem Behrooz_ice[35]. W przypadku niedawnych przejęć stron dokonanych przez członków forum w zmodyfikowanych treściach umieszczane były pseudonimy pierwotnych członków Ashiyane. Hakerzy tacy jak Kamalian lub inni założyciele forum najpewniej nie brali udziału w tych atakach — ich imiona zostały umieszczone przez osoby wspierające forum Ashiyane jako rodzaj hołdu oddawanego założycielom.

Grupa szybko zyskała reputację najlepszego irańskiego zespołu hakerskiego. W celu legalizacji swojej działalności założyła centrum szkoleniowe Ashiyane Digital Training Center, które na zasadach komercyjnych oferowało szkolenia dotyczące technik hakerskich i bezpieczeństwa, niemniej członkowie nadal brali aktywny udział w cyberoperacjach.

Kilka lat po Ashiyane powstała kolejna organizacja hakerska — Iranian Cyber Army (ICA). Od 2009 r. ICA obrała za cel organizacje i pojedyncze osoby podejrzewane o występowanie przeciwko Iranowi. Grupa przeprowadziła cyberataki przeciwko Twitterowi, chińskiej wyszukiwarce Baidu i stronom internetowym wielu polityków opozycyjnych wobec byłego prezydenta Mahmuda Ahmadineżada. Obecnie ta organizacja jest uważana za filię Korpusu Strażników Rewolucji Islamskiej, który z kolei jest jedną z gałęzi irańskich sił zbrojnych[36]. W 2010 r. dowódca Strażników Rewolucji udzielił następującej wypowiedzi dla mediów: „Jesteśmy dumni z założonej przez nas (Irańskiej) Cyberarmii, będącej drugą najsilniejszą Cyberarmią na świecie".

Istnieją dwa dowody łączące grupę Ashiyane z ICA. Po pierwsze, obie organizacje zamieszczały identyczne komunikaty wspierające Hezbollah na przejętych przez siebie stronach. Po drugie, kilku konkretnych hakerów wspiera operacje obu grup[37]. Dodatkową poszlaką jest pochodzenie obydwu grup z tego samego regionu Iranu[38]. Propozycją wyjaśnienia tych zbieżności jest założenie, że ICA nie jest samodzielną organizacją, a jedynie tożsamością fasadową stworzoną przez grupę Ashiyane, aby prowadzić działania dla Strażników Rewolucji.

Przypuszczenia te zostały dodatkowo potwierdzone w Dzienniku Urzędowym Unii Europejskiej w październiku 2011 r. Zgodnie z informacjami tam zawartymi Kamalian, szef cybergrupy Ashiyane, przewodził cyberdziałaniom irańskiego reżimu. Na rysunku 1.1 przedstawiony jest fragment Rozporządzenia Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r., opublikowanego w Dzienniku Urzędowym Unii Europejskiej.

14.	KAMALIAN Behrouz	POB: Tehran DOB: 1983	Head of the IRGC- linked "Ashiyaneh" cyber group. The "Ashiyaneh" Digital Security, founded by Behrouz Kamalian is responsible for an intensive cyber-crackdown both against domestic opponents and reformists and foreign institutions. On 21 June 2009, the internet site of the Revolutionary Guard's Cyber Defence Command posted still images of the faces of people, allegedly taken during post-election demonstrations. Attached was an appeal to Iranians to "identify the rioters".	10.10.2011

Rysunek 1.1. Informacje o powiązaniach Behrouza Kamaliana i grupy Ashiyane z irańskim reżimem pochodzące z Rozporządzenia Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r.

Sankcje wynikające z tego rozporządzenia mają przede wszystkim wywierać presję finansową. Osoby wymienione na tej imiennej liście mają ograniczony dostęp do zasobów ekonomicznych. Instytucje finansowe nie mają prawa przetwarzać transakcji, gdy stroną jest jedna z tych osób, i są zobowiązane do zamrożenia funduszy związanych z tymi osobami lub przedsiębiorstwami, które do nich należą. Unia Europejska umieściła Kamaliana na liście osób objętych sankcjami ze względu na jego zaangażowanie w działania Strażników Rewolucji łamiące prawa człowieka w Iranie[39]. Według publicznie dostępnych raportów Kamalian pomagał w wykorzystaniu środków cyfrowych do identyfikacji uczestników antyprezydenckich protestów, którzy następnie byli aresztowani, torturowani i gwałceni przez Strażników, a w kilku wypadkach także straceni[40]. Kolejne informacje łączące grupę Ashiyane ze Strażnikami Rewolucji wyszły na jaw w 2016 r., gdy Departament Sprawiedliwości postawił w stan oskarżenia kilku irańskich hakerów podejrzewanych o przeprowadzenie ataków przeciwko rządowi Stanów Zjednoczonych, instytucjom finansowym i mediom społecznościowym. Naprawa szkód powstałych w wyniku tych ataków kosztowała dziesiątki milionów dolarów[41]. Dwóch z oskarżonych hakerów było członkami Ashiyane Digital Security Team[42].

Co prawda Ashiyane nie jest jedyną grupą hakerską współpracującą ze Strażnikami Rewolucji, ale jest główną organizacją powiązaną z cyfrowym komponentem zbrojnym Iranu. Inne grupy także miały wpływ na kształtowanie irańskich zdolności cyberprzestrzennych, lecz większość z nich w jakiś sposób łączy się z Ashiyane.

Grupa Ashiyane zniknęła bez żadnych oficjalnych wyjaśnień w połowie 2018 r., pomimo ugruntowanej pozycji wśród Strażników Rewolucji i wśród irańskiej społeczności hakerskiej. Cała infrastruktura użytkowana przez grupę została wyłączona, a ich fora i strony internetowe zlikwidowane. Sam Kamalian zniknął na kilka miesięcy, a po tym czasie powrócił, zakładając nowe przedsiębiorstwo wraz z irańskimi celebrytami branż hakerskiej i cyfrowej. Media i dostawcy usług bezpieczeństwa spekulują, choć nie są to informacje potwierdzone, że infrastruktura Ashiyane była wykorzystywana pod kierownictwem Kamaliana do świadczenia usług hazardu online. Gdyby te informacje się potwierdziły, mogłyby stanowić wyjaśnienie nagłego zatrzymania działania grupy, ponieważ hazard jest przestępstwem w Iranie[43].

Atak na usługę Gmail w 2011 r.

Iran planował wiele swoich ataków DoS tak, by trafić na nagłówki gazet i w ten sposób zagrozić swoim ofiarom. Wydawało się, że w porównaniu do takich państw jak Chiny, Rosja czy Stany Zjednoczone Irańczykom brakuje zaawansowania technicznego, umożliwiającego przeprowadzenie złożonego ataku wywiadowczego.

Sytuacja uległa zmianie latem 2011 r. Irański obywatel występujący w sieci pod pseudonimem Alibo napotkał problemy w dostępie do swojego konta Gmail. W ciągu kilku dni przy każdym logowaniu otrzymywał monit bezpieczeństwa podważający ważność certyfikatu używanego do autentykacji na stronie Gmail[44]. Mimo wyświetlanego ostrzeżenia Alibo akceptował ryzyko, będąc przekonanym o prawdziwości certyfikatu. Uznał, że problem najpewniej wynika z jakiegoś błędu

technicznego i nie stanowi incydentu bezpieczeństwa, ponieważ Gmail od wielu lat była bezpieczną usługą, wykorzystywaną na całym świecie.

Lecz po kilku dniach zorientował się, że utracił całkowicie dostęp do swojego konta pocztowego. Próbując odnaleźć przyczynę problemu, Alibo przekierował swój ruch sieciowy poprzez sieć VPN. Dzięki temu mógł skorzystać z infrastruktury sieciowej pozostającej poza zakresem irańskich adresów IP. Ku swojemu zdziwieniu zdołał bez problemu zalogować się do Gmail i uzyskać dostęp do poczty, ale tylko, gdy korzystał z wirtualnej sieci prywatnej. Kiedy wyłączał przekierowanie ruchu, usługa Gmail stawała się niedostępna.

Wkrótce zrozumiał, że ograniczenie dotyczy wyłącznie użytkowników z terytorium irańskiego. Wciąż jednak nie wiedział, z jakiego powodu tak się działo. Władze Iranu nie wprowadziły jeszcze oficjalnych ograniczeń w ruchu internetowym, więc Alibo nie mógł założyć, że to było przyczyną braku dostępu. Ale nie mógł też tego wykluczyć.

Alibo zadał pytanie na ten temat na oficjalnym forum wsparcia Google. Po kilku dniach firma Google dostarczyła wyjaśnień, choć nie stało się to na forum. Zamiast tego wydano publiczne oświadczenie, że firma padła ofiarą zaawansowanego ataku przeprowadzonego przez stronę trzecią, polegającego na przechwytywaniu szyfrowanej transmisji SSL. Atak miał na celu kontrolowanie aktywności pocztowej irańskich użytkowników[45]. Firma podała, że atakujący uzyskał nieautoryzowany dostęp do komunikacji poprzez wykorzystanie sfałszowanego certyfikatu SSL wystawionego przez organizację DigiNotar, będącą głównym centrum certyfikacji. Google uznała, że centrum DigiNotar nie powinno w ogóle wystawiać takiego certyfikatu SSL, i anulowała go.

Ataki polegające na przechwytywaniu przez pośrednika komunikacji między dwoma systemami (ang. *man-in-the-middle*) nie są szczególnie wyszukane. Standardowym środkiem zabezpieczającym jest wprowadzenie szyfrowania przesyłanych danych z wykorzystaniem certyfikatów SSL. Przygotowanie do przeprowadzenia takiego ataku wymagało cierpliwego i długotrwałego zaplanowania wieloetapowej operacji, a następnie starannego jej wykonania. W szczególności Iran musiał przejąć całą firmę, konkretnie DigiNotar, legalnego wystawcę certyfikatów, aby tworzyć i wystawiać własne certyfikaty SSL, dzięki czemu uzyskał możliwość deszyfrowania przechwyconych danych. Certyfikaty cyfrowe zostały zaprojektowane, by zapobiegać przechwytywaniu ruchu kierowanego do i ze stron internetowych i by uniemożliwiać podszywanie się pod te strony. Gdy zabraknie tej ochrony, atakujący może podglądać informacje wymieniane między użytkownikiem a serwisem internetowym. Dokładnie taki atak przeprowadził agresor w tym przypadku.

Obecnie niemal wszystkie witryny internetowe używają certyfikatów, aby potwierdzić swoją autentyczność i chronić przesyłane dane poprzez ich szyfrowanie. Firma Google była jedną z pierwszych, które wdrożyły taki środek bezpieczeństwa, implementując autentykację serwisu Gmail z użyciem certyfikatów SSL i wprowadzając szyfrowanie danych przesyłanych pomiędzy serwerami a użytkownikami. Jedyną metodą odszyfrowania informacji lub potwierdzenia autentyczności serwera było uzyskanie dostępu do konkretnego certyfikatu. Irańczycy

wiedzieli, że włamanie do tak dojrzałej firmy jak Google byłoby trudne. Zamiast tego przeprowadzili atak przeciwko holenderskiej firmie DigiNotar i uzyskali dostęp do centrum certyfikacyjnego.

Włamanie do firmy DigiNotar najpewniej nie było prostym zadaniem, gdyż działalność ich centrum certyfikacji była okrzepła i uznawana na świecie, a standardy bezpieczeństwa stały na wysokim poziomie. Dostęp do krytycznych obszarów zabezpieczono nie tylko cyfrowo — spółka miała wdrożone także zaawansowane zabezpieczenia fizyczne, takie jak kontrola dostępu oparta na biometrii i indywidualnych kodach dostępowych. Systemy i serwery krytyczne dla działania infrastruktury obsługującej certyfikaty cyfrowe były zamknięte w chronionych pomieszczeniach. Niestety nie można mieć pewności, czy fizyczne ograniczenia dostępu, które spółka obiecywała implementować, faktycznie istniały ani czy pozwoliłyby zatrzymać ten rodzaj ataku, który był przeprowadzony. Gdyby tak było, agresor potrzebowałby pomocy kogoś z wewnątrz organizacji. Nawet z takim wsparciem ominięcie zabezpieczeń fizycznych i cyfrowych byłoby wyjątkowo trudne. I choć istnieje wiele spekulacji i teorii na temat sposobu przeprowadzenia ataku, faktyczny sposób obejścia zabezpieczeń fizycznych pozostaje nieznany. Badacze bezpieczeństwa zdołali jednak prześledzić, w jaki sposób agresor włamywał się do kolejnych wydzielonych segmentów sieci, i zawarli opis tej operacji w niejawnym raporcie sporządzonym po włamaniu[46].

Intruzi rozpoczęli wystawianie fałszywych certyfikatów, gdy tylko uzyskali dostęp do krytycznych systemów firmy DigiNotar. Certyfikaty te były uznawane za prawdziwe przez inne systemy, ponieważ ich wystawcą było legalnie działające centrum certyfikacyjne. Po sporządzeniu certyfikatu dla Google agresorzy mogli przechwytywać dane transmitowane przez rzeczywistych użytkowników irańskich logujących się do swoich kont Gmail. Władze Iranu wykorzystały sfałszowany certyfikat do uruchomienia serwera pośredniczącego w komunikacji pomiędzy obywatelami swojego państwa a faktyczną infrastrukturą Gmail, uzyskując dostęp do wszystkich przesyłanych informacji. W ten sposób rząd w Teheranie mógł przechwytywać, odczytywać i monitorować wszystkie wiadomości Gmail swoich obywateli. Mówiąc krótko: powstał program masowego nadzoru nad aktywnością użytkowników Gmail w Iranie.

Podczas realizacji ataku Iran zdołał znacznie rozwinąć swoje zdolności do prowadzenia cyberdziałań. Jednak operacja została w końcu ujawniona w wyniku braku dyscypliny wśród operatorów. Początkowo nikt nie był w stanie udowodnić, że Iran przeprowadził ten atak. Ale jeden z hakerów wykonał kilka połączeń do systemów firmy DigiNotar, zapominając o skorzystaniu z serwera pośredniczącego, co spowodowało ujawnienie prawdziwego irańskiego adresu IP. Po tej identyfikacji śledczy byli w stanie prześledzić wcześniejszą działalność hakerów, zidentyfikować wszystkie podjęte przez nich kroki i sporządzić całościowy profil ataku, nie pozostawiając cienia wątpliwości, że za operacją stoi Iran[47]. Finalnie atak trwał dosyć krótko, jednak był to jeden z najbardziej udanych ataków przeciwko infrastrukturze publicznej, jakie zostały przeprowadzone przez hakerów rządowych.

Shamoon

Piętnastego sierpnia 2012 r. — podczas święta religijnego, gdy bardzo nieliczni pracownicy byli w pracy — rozpoczęła się gigantyczna operacja sabotażowa, polegająca na usuwaniu danych z systemów i serwerów firmy Aramco, dużej państwowej spółki naftowej z Arabii Saudyjskiej. W ciągu jednego dnia 30 tys. systemów zostało wyczyszczonych, a w miejsce usuniętych danych została załadowana grafika z płonącą amerykańską flagą. Systemy stały się niezdatne do użycia, powodując spustoszenie w sieciach komputerowych spółki. Dziennik „New York Times" oszacował, że zostało wyczyszczone ok. $^{3}/_{4}$ komputerów PC należących do spółki[48].

W owym czasie była to jedna z najbardziej destrukcyjnych operacji sabotażu na świecie. W wyniku ataku spółka Aramco została zmuszona do wyłączenia całej korporacyjnej infrastruktury sieciowej — rzecz nie do pomyślenia w obecnych czasach, zwłaszcza w przypadku jednego z największych koncernów naftowych świata. W ciągu kilku godzin działalność firmy była prowadzona za pomocą maszyn do pisania i ręcznie wypełnianych ksiąg finansowych. Zamiast używać poczty elektronicznej, spółka prowadziła korespondencję wewnętrzną na papierze. Komunikacja w organizacji opierała się także na telefonii internetowej — korzystanie z tej usługi wymagało połączeń sieciowych, więc wiele biur Aramco pozostawało bez łączności telefonicznej.

Na szczęście systemy i sieci odpowiedzialne za przetwarzanie ropy naftowej były oddzielone od sieci korporacyjnych, więc spółka uniknęła całkowitej dewastacji. Gdyby szkodliwe oprogramowanie zdołało zniszczyć systemy kontrolujące produkcję ropy, podobnie jak było z siecią biurową, to szkody finansowe spółki Aramco byłyby znacznie większe.

Infekcja najprawdopodobniej została zainicjowana, gdy osoba wewnątrz spółki celowo podłączyła do systemu komputerowego dysk USB zawierający szkodliwe oprogramowanie czyszczące dane o nazwie Shamoon, choć jednocześnie przeprowadzonych było kilka ukierunkowanych ataków phishingowych, które umożliwiły infiltrację z wykorzystaniem podatności istniejących w systemach Aramco. Wiele osób i grup przypisywało sobie autorstwo ataku. W dniu aktywacji wirusa czyszczącego Shamoon dwie organizacje ogłosiły, że go dokonały: Arab Youth Group i Cutting Sword of Justice. Druga grupa zamieściła następujący komunikat w aplikacji internetowej Pastebin, umożliwiającej wklejanie fragmentów tekstów i udostępnianie ich innym:

> Oto my, występujący w imieniu walczącej z uciskiem grupy hakerskiej, której obmierzły już zbrodnie i potworności popełniane w wielu krajach na świecie, a w szczególności w sąsiednich krajach, takich jak Syria, Bahrajn, Jemen, Liban, Egipt i […], oraz która nie może już znieść podwójnych standardów stosowanych przez społeczność światową wobec tych krajów, zamierzamy naszym działaniem uderzyć w głównych winnych tych katastrof.
>
> Jednym z głównych winnych jest skorumpowany reżim saudyjski, który rozszerza ucisk, wykorzystując do tego muzułmańskie zasoby ropy naftowej. Saudowie uczestniczą w popełnianiu tych zbrodni. Ich ręce są zbrukane krwią niewinnych dzieci i ludzi.

> W pierwszym kroku podjęliśmy działania przeciwko spółce Aramco, ponieważ jest największym źródłem finansowania reżimu saudyjskiego. W tym kroku zinfiltrowaliśmy systemy komputerowe Aramco, korzystając z przejętych systemów w kilku krajach i wysyłając szkodliwego wirusa, który zniszczył 30 tys. komputerów w sieci spółki. Dzieło zniszczenia rozpoczęło się w środę 15 sierpnia 2012 r. o 11:08 czasu lokalnego w Arabii Saudyjskiej i dokona się w ciągu kilku godzin.
>
> To jest ostrzeżenie dla tyranów w tym kraju i innych krajach wspierających zbrodnie swoją niesprawiedliwością i uciskiem. Wzywamy wszystkie przeciwne tyranii grupy hakerskie z całego świata do przyłączenia się do naszego ruchu. Chcemy, by wspierały one nasz ruch poprzez przygotowywanie i przeprowadzanie takich operacji, jeżeli tylko opowiadają się przeciw tyranii i uciskowi.
>
> Karzący Miecz Sprawiedliwości[49]

Po tym jak wirus, realizujący pierwszy krok operacji, znalazł się w systemie ofiary, niezależnie od kanału, jakim się tam dostał, nastąpiła instalacja pozostałych komponentów szkodliwego oprogramowania i dalsza infekcja systemu. Początkowa faza ataku zapewniła intruzowi przyczółek w środowisku ofiary. Korzystając z niego, atakujący dokonał enumeracji urządzeń sieciowych i wykradł dane uwierzytelniające zapewniające dostęp do uprawnień administratorskich. Po zdobyciu odpowiednich danych dostępowych agresorzy użyli ich do połączenia się z istotnymi systemami, takimi jak kontrolery domeny i serwery plików. Następnie w systemach należących do atakowanego środowiska umieszczone zostało szkodliwe oprogramowanie wymazujące dane. By uniknąć wykrycia, atakujący zamaskował wirusa pod postacią prawdziwego sterownika, ukrywając go wśród pozostałych komponentów systemu. A gdy wszystko zostało już przygotowane, uruchamiane było oprogramowanie wymazujące, w wyniku czego zniszczeniu ulegał główny rekord rozruchowy systemu ofiary.

W społeczności specjalistów bezpieczeństwa powszechnie uważa się, że prawdziwym sprawcą ataku był Iran. Po ataku z 2012 r. doszło do jeszcze kilku innych fal ataków z wykorzystaniem wirusa Shamoon. Poziom zaawansowania agresora nieco wzrastał w każdej kolejnej fali. Hakerzy uczyli się na wcześniejszych błędach. Grupy haktywistów, które przypisały sobie przeprowadzenie pierwszego ataku, zniknęły po kampanii z 2012 r. Najpewniej były to wyłącznie tożsamości internetowe utworzone przez atakujących i uprawdopodobnione z użyciem mediów społecznościowych, aby zmylić śledczych. Hakerzy rządowi, w tym irańscy, stanowią zupełnie inny rodzaj cyberzagrożenia niż spotykane do tej pory — m.in. z powodu podszywania się pod cudze barwy, wykorzystywania fałszywych tożsamości i kłamliwych historii oraz stosowania destruktywnego szkodliwego oprogramowania.

Dostawcy usług bezpieczeństwa wciąż obserwują wiele irańskich cyberataków. Zwykle różnią się one od innych ataków prowadzonych przez hakerów rządowych, gdyż Iran do przeprowadzenia swoich operacji przede wszystkim posługuje się wynajętymi wykonawcami[50]. Tacy hakerzy, w odróżnieniu od operatorów rządowych

lub wojskowych, pracują od zlecenia do zlecenia, dołączając do zespołu lub opuszczając go w miarę potrzeb. Ta fluktuacja powoduje brak wykształconych, doświadczonych operatorów, którzy mogliby pracować nad długofalowymi operacjami ofensywnymi. Mimo tych braków Iran zdołał pomyślnie przeprowadzić operacje przeciwko wybranym celom na Bliskim Wschodzie.

Stany Zjednoczone

Spośród wszystkich krajów omówionych do tej pory Stany Zjednoczone najskuteczniej unikały upubliczniania swoich cyberoperacji. W zasadzie niemal nic nie wiedzieliśmy o tych operacjach, dopóki były pracownik NSA Edward Snowden nie ujawnił w 2003 r. ponad 9000 sztuk poufnych dokumentów.

Lecz 23 kwietnia 2015 r. Stany Zjednoczone usunęły klauzulę tajności z 52 tys. dokumentów, pozwalając na prześledzenie historii amerykańskich operacji wywiadowczych. W tej skarbnicy informacji o pracy wywiadu znalazł się także szczegółowy raport dotyczący kariery amerykańskiego łamacza kodów Williama F. Friedmana. Zacznijmy rozdział o Stanach od omówienia tej postaci.

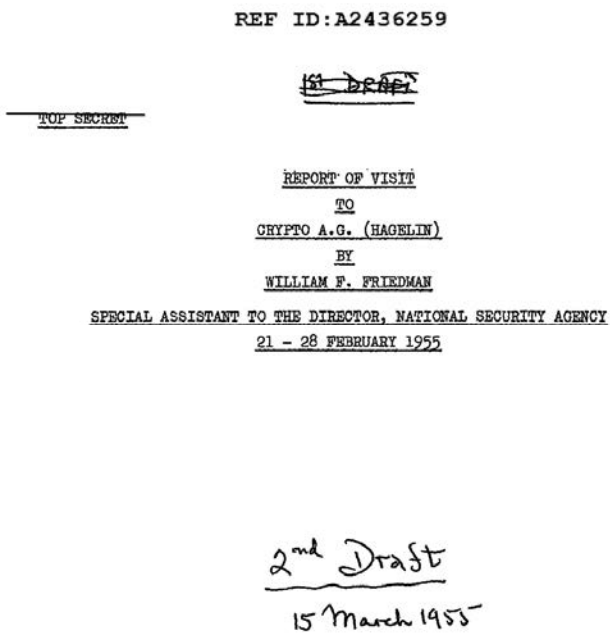
Crypto AG

Obecnie, gdy ludzie mówią o bezpiecznej komunikacji, zwykle mają na myśli szyfrowane transmisje pomiędzy współczesnymi komputerami. Ale ten rodzaj kryptografii sięga korzeniami do drugiej wojny światowej, gdy niemiecka armia opracowała pierwszą maszynę szyfrującą, by zapewnić bezpieczną komunikację dla swoich struktur. Urządzenie, nazwane Enigma, pozwalało szyfrować i odszyfrowywać wiadomości przy użyciu mechanicznych wirników i układu świateł.

Nie tylko Niemcy opracowali szyfrujące urządzenie komunikacyjne w owym czasie. W 1933 r., gdy Adolf Hitler doszedł do władzy w Niemczech, biznesmen Boris Hagelin założył w Szwajcarii niewielkie przedsiębiorstwo, znane dziś pod nazwą Crypto AG. Hagelin wybrał na główną siedzibę firmy Sztokholm w Szwecji i rozpoczął produkcję kryptograficznych urządzeń komunikacyjnych. Gdy wkrótce nadeszła wojna, urządzenia te były wykorzystywane przez Stany Zjednoczone i Wielką Brytanię[51]. Podobnie jak w przypadku Enigmy, podstawą działania maszyn Crypto AG był autorski mechanizm szyfrujący, służący do przesyłania utajonych komunikatów, choć nie był on tak technicznie zaawansowany jak w niemieckim odpowiedniku.

Mimo to spółka Crypto AG miała zapewniony stabilny strumień przychodów dzięki wojnie. Po jej zakończeniu konieczne stało się znalezienie nowych sposobów zarabiania pieniędzy. Hagelin zwrócił się do Williama Friedmana, który zasłynął złamaniem japońskich urządzeń kryptograficznych (Amerykanie nadali im kryptonim Purple) wzorowanych na niemieckiej Enigmie[52]. Podczas wojny Hagelin i Friedman byli współpracownikami i blisko się zaprzyjaźnili. Friedman został potem głównym kryptografem w amerykańskiej agencji Signal Intelligence Service (SIS).

Według obecnie odtajnionych przez rząd amerykański raportów Friedman i Hagelin spotykali się wielokrotnie w okresie od 1955 do 1969 r. Na rysunku 1.2 przedstawiona jest przykładowa strona odtajnionego raportu.



REF ID:A2436259

~~1st Draft~~

TOP SECRET

REPORT OF VISIT
TO
CRYPTO A.G. (HAGELIN)
BY
WILLIAM F. FRIEDMAN
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY
21 - 28 FEBRUARY 1955

2nd Draft
15 March 1955

Rysunek 1.2. Odtajniony raport NSA opisujący szczegóły spotkań pomiędzy Hagelinem a Friedmanem

W raportach tych zawarto szczegółowe informacje o rozmowach prowadzonych przez obu mężczyzn. Można tam m.in. przeczytać o planach Hagelina, by znacząco zwiększyć produkcję spółki Crypto AG poprzez rychłe wprowadzenie do produkcji kolejnego modelu urządzenia szyfrującego. Według słów Hagelina wypowiadanych do Friedmana nowy model był znacznie bardziej złożony od pierwszych maszyn i zawierał wiele usprawnień technicznych. Hagelin zgodził się dostarczyć nowy model rządowi amerykańskiemu do weryfikacji, zanim zostanie wprowadzony na rynek. W ten sposób Stany Zjednoczone uzyskały oczywistą i gigantyczną przewagę nad innymi państwami, ponieważ była to prawdziwie czołowa technologia w owym czasie[53].

Ale wymiana informacji wywiadowczych na tym się nie kończyła. W ciągu kolejnych dwóch lat doszło do licznych spotkań, które Friedman szczegółowo opisał w oficjalnych raportach rządowych. Podczas tych spotkań mężczyźni rozmawiali na temat potencjalnych klientów Crypto AG, m.in. organizacji rządowych z Włoch, Egiptu, Jordanii, Iraku i Arabii Saudyjskiej. W sumie Hagelin dostarczył szczegółowych informacji o swoich kontaktach z przedstawicielami ponad 30 krajów, które były zainteresowane zakupem maszyn Crypto AG[54].

Oprócz własnego opisu zdarzeń Hagelin dostarczał rządowi Stanów Zjednoczonych także kopie wrażliwej korespondencji, jaką prowadził z potencjalnymi klientami, zawierającej opis planowanego użycia urządzeń szyfrujących oraz omawiane wątpliwości. Na przykład opisał szczegółowo kontakty z urzędnikami powiązanymi z francuskim politykiem Patrickiem Ollierem, z którymi rozważał „plany poprawy sytuacji w sprawach kryptografii"[55]. Plany te obejmowały budowę fabryki w Paryżu i wyposażenie jej w narzędzia niezbędne do rozwoju tajnych urządzeń szyfrujących. Jednakże metody kryptograficzne i komponenty techniczne stosowane w tych urządzeniach miały pochodzić od spółki Crypto AG. Francuzi otrzymali specyfikacje, przykładowe egzemplarze i wsparcie ekspertów od szwajcarskiej spółki, lecz nie byli świadomi, że Hagelin podzielił się tymi informacjami z Amerykanami. Podobne sytuacje miały miejsce odnośnie do najważniejszych funkcjonariuszy rządów innych państw świata.

Podczas jednego ze spotkań Friedman złożył ważną propozycję Hagelinowi. Niestety nie wiemy dokładnie, co powiedział, gdyż ten fragment raportu został ocenzurowany przez rząd amerykański. Na szczęście ujawniono pewien szczegół: spółka Crypto AG miała dostarczać Stanom Zjednoczonym pełną kopię korespondencji prowadzonej z klientami oraz złożonych przez nich zamówień.

W 2020 r. dziennik „Washington Post" opublikował artykuł, oparty na wynikach własnego śledztwa i analizie danych zawartych w odtajnionej części raportu, w którym przedstawiono prawdopodobną treść propozycji Friedmana:

> Hagelin, założyciel i właściciel spółki Crypto AG, i William Friedman, twórca amerykańskiej kryptologii, zawarli we wczesnych latach 50. układ, dzięki któremu NSA mogła narzucać spółce, którym klientom należy sprzedać „łatwe do złamania" urządzenia komunikacyjne, a którym w pełni zabezpieczone[56].

Gdyby to okazało się prawdą, byłby to jeden z pierwszych ataków na **łańcuch dostaw**, podczas którego rząd jednego państwa uzyskałby skryty dostęp do kanałów komunikacyjnych, umożliwiający monitorowanie wymiany szyfrowanych informacji przez rządy innych państw.

Crypto AG rozwijała i sprzedawała technologie kryptograficzne do 2018 r., kiedy to została wykupiona. Jednak upublicznienie informacji o ponadsześćdziesięcioletniej tajnej współpracy z rządem Stanów Zjednoczonych nadszarpnęło reputację spółki i znacznie utrudniło jej dalszą działalność.

Stuxnet

W maju 2010 r. betonowe ściany irańskiego kompleksu w Natanzie zadrżały z łoskotem. Wirówki zakładów wzbogacania paliwa jądrowego wymknęły się spod kontroli i doprowadziły do uszkodzeń systemów i precyzyjnego wyposażenia kompleksu. Stanowiący część irańskiego programu wzbogacania uranu Zakład Wzbogacania Paliwa (ang. *Fuel Enrichment Plant* — FEP) w Natanzie znajduje się w samym sercu miasta, ukryty przed wzrokiem postronnych głównie pod ziemią. W kompleksie jest zainstalowanych ponad 7000 wirówek służących do pozyskiwania

izotopu uranu U-235. Jest to jeden z dwóch izotopów uranu, będący kluczowym składnikiem niezbędnym do produkcji broni jądrowej.

Ze względu na swoje właściwości fizyczne, zwłaszcza masę atomową, izotopy U-235 i U-238 ulegają rozdzieleniu w szybkoobrotowych wirówkach. Zestawy wirówek połączonych w szereg umożliwiają absorpcję izotopu U-235 za pomocą odpowiedniego gazu. Gaz jest nośnikiem dla atomów uranu U-235, który po schłodzeniu i zestaleniu może zostać użyty do budowy bomby[57].

Twórcy wirusa *Stuxnet* mieli rozległą wiedzę na temat procesu wzbogacania uranu i konkretnych systemów realizujących ten proces w zakładzie. Szkodliwe oprogramowanie zakłócało ruch wirówek lub zmieniało ich szybkość obrotową, doprowadzając do awarii. Postępujące uszkodzenia kolejnych wirówek sprawiły, że operatorzy systemów i naukowcy zaczęli gorączkowo weryfikować systemy sterowania i zabezpieczenia odpowiedzialne za monitorowanie działania zakładu. Ku ich zdziwieniu nie zostały odnotowane żadne alerty o awariach wirówek. Zepsute wirówki stały się zmorą zakładu, znacznie opóźniając irański program jądrowy.

Dopiero miesiąc później pojawiła się wskazówka dotycząca przyczyn awarii, gdy zaczęły następować przypadkowe restarty **programowalnych sterowników logicznych** (ang. *Programmable Logic Controller* — PLC) — komponentów odpowiedzianych za sterowanie pracą zakładu i monitorowanie jej. Administratorzy systemów komputerowych nabrali podejrzeń, że w ich sieci komputerowej może istnieć intruz (program lub człowiek) powodujący problemy. Przekazali więc dzienniki zdarzeń i zebrane dane do firmy VirusBlockAda, białoruskiego dostawcy zabezpieczeń komputerowych, w celu zbadania sytuacji.

Oprogramowanie sterowników PLC komunikowało się z systemem operacyjnym Microsoft Windows, więc badacze z VirusBlockAda nawiązali współpracę ze specjalistami z Microsoftu. Zespół wkrótce odkrył obecność obcego kodu w systemach zakładu. Przy czym odkrycie kodu było dopiero początkiem rewelacji. Ku ich zdziwieniu w podejrzanym kodzie zastosowano cztery procedury wykorzystujące podatności (ang. *exploit*) „dnia zerowego". Procedura wykorzystująca podatności „dnia zerowego" umożliwia infiltrację systemu za pośrednictwem błędu, który nie jest publicznie znany lub który nie jest naprawiany przez żadną aktualizację. Mówiąc dokładniej: wykorzystuje podatności, przed którymi obrońcy nie mogą się zabezpieczyć, ponieważ dostawca oprogramowania jeszcze nie dostarczył rozwiązania dla błędu powodującego podatność. Zwykle rozwiązanie błędu jest dostarczane w późniejszym czasie pod postacią aktualizacji oprogramowania. Do dziś odnalezienie w bronionym środowisku pojedynczej procedury wykorzystującej podatność „dnia zerowego" jest dosyć niezwykłe. Odkrycie szkodliwego oprogramowania, które korzysta z czterech takich eksploitów, w zasadzie jest niespotykane.

Dzięki wykorzystaniu wspomnianych podatności atakujący uzyskali dostęp do systemów zakładu wzbogacania paliwa i zdołali zainstalować główną część roboczą szkodliwego oprogramowania — przez badaczy z firmy Symantec nazwaną *Stuxnet*, ze względu na obecność w narzędziu plików o nazwach *.stub* i *mrxnet.sys*[58]. Oprogramowanie Stuxnet było tzw. robakiem, posiadającym zdolność do replikacji i rozprzestrzeniania się pomiędzy systemami, którego celem

było odszukanie konkretnego typu systemu: sterowników PLC odpowiedzialnych za pracę wirówek gazowych w zakładzie w Natanzie[59]. Szkodliwe oprogramowanie mogło autonomicznie doprowadzić do infekcji sterowników PLC, wymagane było tylko jego uruchomienie w obrębie zakładu wzbogacania paliwa jądrowego w Natanzie.

Stopień złożoności oprogramowania Stuxnet silnie wskazuje na działanie agresora rządowego. Oprócz wspomnianych już eksploitów „dnia zerowego" badacze odkryli także użycie czterech innych procedur wykorzystywania podatności atakowanego systemu. Atak z użyciem narzędzia Stuxnet jest jednym z najszerzej rozpoznawanych ataków przeprowadzonych do tej pory, głównie ze względu na prezentowaną przez agresora dogłębną znajomość kompleksu w Natanzie, jego zdolność do umieszczenia własnego kodu wewnątrz zabezpieczonego środowiska oraz z powodu ogólnej złożoności ataku.

Głównym podejrzanym o przeprowadzenie ataku wkrótce stał się rząd Stanów Zjednoczonych. Kilka lat wcześniej, w sierpniu 2006 r., irański prezydent Mahmud Ahmadineżad ogłosił, że kraj zbudował zdolności do wzbogacania uranu w stopniu wymaganym przez irański program nuklearny. Iran wcześniej przystąpił do porozumienia, w którym zobowiązał się do zaprzestania rozwoju technologii atomowych do celów militarnych, więc ogłoszenie kontynuacji programu wzbudziło niepokój w wielu krajach, m.in.: Stanach Zjednoczonych, Izraelu i sąsiednich państwach Bliskiego Wschodu. Amerykański prezydent George Bush ostrzegł Iran, że następstwem wznowienia programu jądrowego będą poważne konsekwencje[60].

Z czasem nałożone przez USA sankcje odcisnęły się negatywnie na gospodarce irańskiej. Ale w miarę jak Iran tracił znaczenie polityczne i gospodarcze, jego przywództwo zwiększało wysiłki wkładane w rozwój broni atomowej. Czy atak z użyciem Stuxneta był jedną z pierwszych konsekwencji, o których ostrzegał prezydent Bush? Takie przekonanie było rozpowszechnione. Zaburzenie pracy wirówek, a tym samym całego procesu wzbogacania uranu, znacznie opóźniło realizację irańskich planów budowy broni atomowej. Wprawdzie minęło kilka lat od wygłoszenia przez prezydenta Busha wspomnianego oświadczenia, ale skomplikowana operacja pokroju ataku z użyciem Stuxneta najpewniej wymagała sporo czasu na przygotowanie i wykonanie.

Nie tylko Stany Zjednoczone groziły Iranowi. W 2009 r. izraelski premier Beniamin Netanjahu wygłosił publiczne przemówienie, w którym zwrócił się bezpośrednio do prezydenta Stanów Zjednoczonych Baracka Obamy. Jego słowa zostały podsumowane nagłówkiem magazynu „The Atlantic": „Powstrzymaj Iran — albo ja to zrobię"[61]. Netanjahu nie określił ram czasowych ultimatum, ale według jednego z jego współpracowników oczekiwano, że Stany Zjednoczone odpowiedzą w ciągu kilku miesięcy, a nie lat.

Z powyższych powodów Iran, gdy tylko potwierdził, że oprogramowanie Stuxnet było przyczyną awarii wirówek, zaczął traktować Stany Zjednoczone i Izrael jako prawdopodobnych sprawców ataku. Reza Jalali, dowódca oddziału wojskowego zwalczającego akty sabotażu, publicznie przypisał sprawstwo ataku z użyciem wirusa Stuxnet Stanom Zjednoczonym i Izraelowi[62].

Wprawdzie Iran nie ujawnił żadnych dowodów potwierdzających domniemaną tożsamość sprawców, jednak groźby ze strony Izraela i Stanów Zjednoczonych oraz informacje opublikowane przez dostawców usług bezpieczeństwa stanowią dodatkowe poszlaki uprawdopodabniające te przypuszczenia. Firma Symantec przeprowadziła obszerne badania części wykonawczej złośliwego oprogramowania Stuxnet, aby lepiej zrozumieć, dlaczego doszło do ataku. Specjaliści spółki ustalili, że pierwsze obserwacje tego szkodliwego narzędzia wśród rzeczywistych systemów poczyniono w 2010 r., więc powstało ono znacznie wcześniej. Znalezione w toku badań dowody wskazują, że prace nad narzędziem Stuxnet prowadzono już w maju 2005 r. Niemniej infekcja systemów zakładu wzbogacania uranu nastąpiła dopiero w 2009 r., czyli rok przed odkryciem wirusa. Aby przeprowadzić atak, agresor musiał umieścić szkodliwe oprogramowanie wewnątrz systemów kontrolujących sieć kompleksu w Natanzie.

Według doniesień medialnych[63] agresor umieścił moduł dokonujący instalacji narzędzia Stuxnet na przenośnych dyskach USB. Technicy firmy Symantec znaleźli moduł USB w kodzie Stuxneta, potwierdzając te przypuszczenia[64]. Dziennikarze twierdzili, że osoby odpowiedzialne za atak Stuxneta podrzuciły zainfekowane nośniki w pobliżu pięciu spółek prowadzących bliską współpracę z zakładem wzbogacania paliwa. Atakujący przypuszczalnie znali architekturę wewnętrznych sieci komputerowych zakładu i przewidywali istnienie skutecznych zabezpieczeń. Organizacja dokonująca tego ataku musiałaby posiadać gigantyczne możliwości zbierania danych wywiadowczych, by przeprowadzić rozpoznanie jądrowego zakładu przemysłowego zlokalizowanego w większości pod ziemią i poznać szczegóły budowy jego środowiska technicznego.

Z punktu widzenia agresora atak z wykorzystaniem nośników USB skierowany przeciwko drugorzędnym organizacjom był bardzo sensownym posunięciem. Spółki partnerskie produkowały wyposażenie i oprogramowanie dla zakładu wzbogacania i, co ważniejsze, nie były zabezpieczone w takim stopniu jak główny zakład. W raportach zawarta jest sugestia, że pracownicy znaleźli nośniki USB porzucone na parkingu firmowym, choć nie ma na to jednoznacznych dowodów. Gdy jeden z użytkowników podłączył znaleziony dysk do komputera wewnątrz spółki, nastąpiła infekcja, która następnie rozprzestrzeniała się, by w końcu dotrzeć do systemów zakładu wzbogacania paliwa[65].

Dokładna data i czas początkowej infekcji nie są znane, ale badacze firmy Symantec znaleźli kod narzędzia Stuxnet w jednym z ogólnie dostępnych repozytoriów szkodliwego oprogramowania. Odnalezione próbki, oznaczone numerem wersji 0.500, zostały skompilowane znacznie wcześniej, w 2005 r. Wiele programów antywirusowych przeczesuje publiczne repozytoria kodu w poszukiwaniu szkodliwego oprogramowania. Możliwe, że twórcy Stuxneta wiedzieli o tym i wykorzystali takie repozytorium, aby przed wykorzystaniem Stuxneta w prawdziwej operacji upewnić się, że pakiety antywirusowe wykrywają zagrożenie. Dodatkowo sprawdzono historię rejestracji domen, które w czasie operacji były używane przez serwery sterowania i kontroli dla Stuxneta. Rejestracji dokonała anonimowa osoba w tym samym miesiącu, w którym została skompilowana wersja „0.500" narzędzia[66].

Ataki doprowadziły do przejściowego spowolnienia irańskiego programu nuklearnego, zatem uważa się je za pierwsze w świecie znane wykorzystanie cyberbroni. W wyniku tego zdarzenia doszło do przyspieszenia rozwoju irańskich cyberoperacji ofensywnych, wyraźnie widocznego w latach 2011 – 2013. Obecnie irańskie cyberoperacje stanowią jedno z najpoważniejszych cyberzagrożeń dla Stanów Zjednoczonych i Izraela.

Stany Zjednoczone także kontynuują prowadzenie cyberwojny przeciwko Iranowi. Pomiędzy majem a czerwcem 2009 r. doszło do sześciu ataków na tankowce przechodzące przez cieśninę Ormuz. W kilku wypadkach nieoznakowane łodzie umieściły ładunki wybuchowe na burtach tankowców, w pozostałych w kierunku statków zostały wystrzelone torpedy[67]. Rząd amerykański oskarżył rząd irański o zorganizowanie tych ataków w celu zakłócenia światowych łańcuchów dostaw ropy naftowej, a w ciągu kolejnego roku Stany Zjednoczone, Wielka Brytania, Izrael, Bahrajn i Australia wyekspediowały samoloty i okręty, w tym podwodne, do ochrony szlaków morskich w cieśninie Ormuz. Oprócz stosowania fizycznych metod ochrony statków Stany Zjednoczone użyły cyberbroni, aby utrudnić Iranowi śledzenie statków poruszających się w chronionym obszarze. Według doniesień dziennika „New York Times", potwierdzonych przez amerykańskie dowództwo wojsk cyfrowych (USCYBERCOM), w wyniku amerykańskich cyberoperacji zostały zniszczone możliwości Iranu identyfikowania i śledzenia tankowców oraz pozostałych statków przepływających przez pobliskie akweny[68]. Strona irańska zaprzecza jakiemukolwiek zaangażowaniu w ataki na tankowce. Zamiast tego Iran twierdził, że winne są grupy pochodzące spoza Bliskiego Wschodu, z którymi nie łączą go żadne relacje. Rząd w Teheranie ogłosił, że padł ofiarą zachodniej propagandy i kampanii obwiniania, służących do uzasadnienia prowadzonych przeciwko niemu operacji wojskowych i cyfrowych[69].

Grupa Equation

W lutym 2015 r. zespół ds. badań i analizy (Global Research and Analysis Team — GReAT) firmy Kaspersky opublikował raport analityczny dokumentujący działania grupy szpiegowskiej, której nadano kryptonim *Equation*[70].

Zespół GReAT firmy Kaspersky ma uznaną renomę w zakresie badania działalności cyberwywiadowczych. Przez lata opublikował szereg wnikliwych analiz, a jego odkrycia wielokrotnie trafiały na pierwsze strony gazet. Kryptonim nadany przez zespół GReAT jest powiązany z wykorzystaniem przez grupę zaawansowanych wielopoziomowych technik szyfrowania opartych na prawidłach matematycznych. Odkrycie działalności grupy miało doniosłe znaczenie, gdyż ślady używanego przez nią szkodliwego oprogramowania i infrastruktury, a także prowadzonych operacji sięgają 1996 r. W efekcie Equation jest jedną z najstarszych i najbardziej doświadczonych grup wywiadowczych znanych do chwili obecnej.

Do ujawnienia grupy doszło po odkryciu szkodliwego oprogramowania, potajemnie zamieszczonego na płycie CD, która była dystrybuowana na jednej z międzynarodowych konferencji naukowych w Houston. Pewien naukowiec, posługujący się dla zachowania anonimowości pseudonimem Grzegorz Brzęczyszczykiewicz, otrzymał taką płytę. Gdy umieścił ją w napędzie, jego komputer został

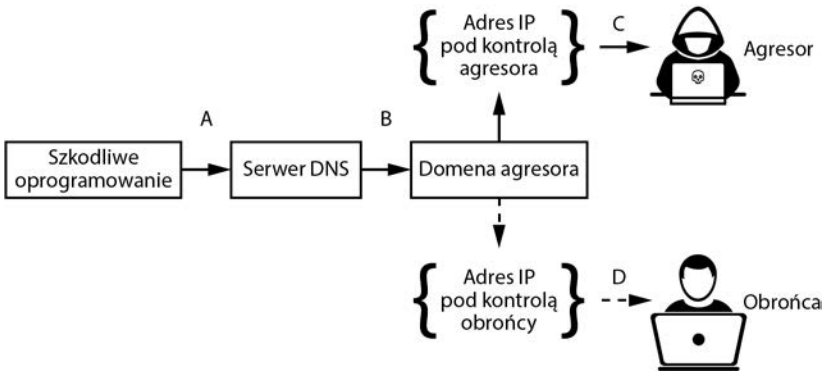
przejęty przez aktywowane szkodliwe oprogramowanie. W ten sposób grupa Equation uzyskała dostęp nie tylko do systemu Brzęczyszczykiewicza, ale także do całej sieci jego pracodawcy.

Nie jest do końca jasne, w jaki sposób zespół GReAT z firmy Kaspersky otrzymał płytę od Brzęczyszczykiewicza, ale gdy tylko się to stało, specjaliści rozpoczęli szczegółowe badania. Początkowo analiza szkodliwego oprogramowania była znacznie utrudniona, ponieważ każdy element narzędzia był zaszyfrowany i trudny do zrozumienia[71]. Ale upór specjalistów GReAT w stosowaniu metod analizy wstecznej w końcu się opłacił. Zespół odkrył na płycie CD kod wykorzystujący kilka podatności systemowych „dnia zerowego". Odkrycie wykorzystania takich podatności było bardzo istotne, gdyż wcześniej jedynym znanym wirusem posiadającym taką zdolność infekowania systemów był Stuxnet.

Szkodliwe oprogramowanie nie tylko korzystało z zaawansowanych eksploitów, także metoda uzyskiwania trwałego dostępu do systemów ofiar była nowatorska. Po aktywacji w systemie wirus infekował firmware, uzyskując w ten sposób pełną kontrolę nad komputerem. Korzystając z uprawnień administratorskich, szkodliwe narzędzie instalowało wirtualny system plików stosowany do kradzieży danych z systemu ofiary. Dodatkowo zespół GReAT zidentyfikował wersje wirusa zaprojektowane do przejmowania systemu operacyjnego macOS, kontrolującego komputery Apple, oraz iOS, kontrolującego telefony Apple iPhone. Większość szpiegowskiego szkodliwego oprogramowania odkrytego do tego czasu wykorzystywała podatności systemu Microsoft Windows. To sugerowało, że Equation ma do dyspozycji ogromne zasoby.

Spółka Kaspersky, przy której działał zespół GReAT, dostarczała popularne rozwiązanie ochrony komputerów, które generowało znaczną ilość danych za każdym razem, gdy została wykryta szkodliwa działalność w systemie. Po przeanalizowaniu szkodliwego oprogramowania możliwe było utworzenie jego sygnatur, przez co produkt Kaspersky'ego był w stanie je wykrywać — czego nie oferowały produkty innych dostawców w owym czasie. Dzięki temu GReAT mógł przeanalizować dane z poprzednich lat i odszukać historyczne wystąpienia narzędzi grupy Equation oraz powiązaną aktywność. Zespół mógł określić tożsamość ofiary i jej lokalizację, ale te informacje nie zostały opublikowane.

Podczas dalszych prac zespół GReAT przyjrzał się infrastrukturze cyfrowej wykorzystywanej do komunikacji przez narzędzia grupy Equation. Poprzez analizę danych rejestracyjnych, historii hostingu serwisów i sesji komunikacyjnych inicjowanych przez szkodliwe oprogramowanie udało się zidentyfikować aktywne i nieaktywne serwery dowodzenia i kierowania. Specjaliści GReAT zdołali przejąć kontrolę nad niewielką częścią infrastruktury komunikacyjnej narzędzia, a tym samym nad przesyłanymi danymi. Zastosowano w tym celu technikę o nazwie **sinkholing**, polegającą na przechwyceniu przez obrońców komunikacji nadawanej do infrastruktury agresora i przekierowaniu jej do własnej infrastruktury. W ten sposób zakłócana jest operacja atakującego, a obrońcy mogą przeprowadzić analizy przesyłanych informacji. Na rysunku 1.3 technika ta została objaśniona graficznie.



Rysunek 1.3. Przykład zastosowania techniki sinkholingu

Przepływ danych pomiędzy punktami A, B i C reprezentują strzałki narysowane linią ciągłą. Strzałki narysowane linią przerywaną reprezentują zmianę w drodze transmisji danych następującą po przejęciu domeny za pomocą techniki sinkholingu.

A — szkodliwe oprogramowanie nadaje wykradzione dane do domeny agresora.

B — serwer nazw tłumaczy zrozumiały dla człowieka adres domenowy na numeryczny adres IP, dzięki czemu transmisja i kierowanie ruchem w internecie mogą być zorganizowane w bardziej wydajny sposób.

C — przesyłane dane docierają do adresu IP przydzielonego maszynie w domenie agresora. Agresor następnie może połączyć się ze swoją maszyną i użyć wykradzionych danych w dowolny sposób.

D — w celu przejęcia szkodliwego ruchu dostawca usług internetowych zmienia przypisanie nazwy domeny do adresu IP. W ten sposób agresor traci dostęp do skradzionych danych, a obrońcy i badacze mają szansę ustalenia, jakimi informacjami agresor jest zainteresowany i przeciwko komu prowadzi atak.

Zespół GReAT firmy Kaspersky wykorzystał przechwycony ruch sieciowy do zebrania dodatkowych informacji na temat działań grupy Equation, rozszerzając wiedzę uzyskaną poprzez analizę ich kodu. Specjaliści zidentyfikowali pewną liczbę domen kontroli i sterowania Equation, których rejestracja nazwy wygasła. Poprzez zarejestrowanie tych domen na własny rachunek badacze mogli uruchomić własną infrastrukturę. Przywrócenie tych domen online spowodowało, że instancje szkodliwego oprogramowania, które wciąż działały niewykryte w zainfekowanych systemach i miały skonfigurowane stare adresy serwerów C&C, zaczęły nawiązywać połączenia z maszynami GReAT i przesyłać do nich dane ofiar. Tylko że teraz to obrońcy odbierali i poddawali analizie te informacje.

W podsumowaniu śledztwa, które zostało zakończone w 2015 r., specjaliści firmy Kaspersky zidentyfikowali ponad 500 systemów w 42 krajach przejętych przez grupę Equation. Najwięcej infekcji zaobserwowano w Rosji, Iranie, Chinach i kilku innych krajach. Po przeanalizowaniu danych ofiary zostały skatalogowane w podziale na kraj pochodzenia i branżę. Wśród ofiar były organizacje pracujące dla rządów, wojska, przemysłu aeronautycznego, jądrowych ośrodków badawczych, firm telekomunikacyjnych i zajmujące się kryptografią, co stanowi wzorzec dosyć typowy dla obszaru zainteresowań hakerów rządowych.

Niestety zespół GReAT nie ujawnił, kogo podejrzewa o prowadzenie działań grupy Equation. Organizacje takie jak Council on Foreign Relations[72] lub magazyn „Wired"[73] wskazywały jedną z amerykańskich agencji wywiadowczych jako odpowiedzialną za prowadzenie ataków. Domniemanie takie było oparte na fakcie, że Equation dysponowała dostępem do metod stosowania podatności „dnia zerowego", a fragmenty tekstów obecne w kodzie narzędzia były zapisane po angielsku. Teorię tę dodatkowo wspierały dwie obserwacje poczynione przez zespół GReAT. Po pierwsze, badacze ustalili, że szkodliwe oprogramowanie grupy Equation znajdowało się w systemach kilku „pacjentów zero" wirusa Stuxnet, zanim ataki z jego wykorzystaniem się rozpoczęły. Innymi słowy: Equation mogła prowadzić działania wstępne i rozpoznanie irańskich celów jako przygotowanie do operacji Stuxnet[74]. Po drugie, kilka podatności „dnia zerowego", pierwotnie zidentyfikowanych w oprogramowaniu Stuxnet, było używanych przez Equation ponad rok przed operacją Stuxnet. Można się spierać, czy są to wystarczające dowody, by oskarżyć amerykański wywiad o organizację tych ataków, ale bez wątpienia za grupą Equation i atakiem Stuxneta stała ta sama organizacja.

Regin

Szkodliwe oprogramowanie Stuxneta wiele łączyło z tym używanym przez grupę Equation — m.in.: miały podobną budowę, korzystały z tych samych podatności i były skierowane przeciwko podobnym ofiarom. Specjaliści firmy Symantec odkryli trzeci rodzaj szkodliwego oprogramowania o podobnej modularnej budowie i porównywalnym stopniu zaawansowania. Rodzaj ten, nazwany Regin, istniał co najmniej od 2008 r. i był stosowany do ataków na badaczy, rządy, przedsiębiorstwa oraz krytyczną infrastrukturę telekomunikacyjną[75].

Jednak narzędzie Regin w jednym różniło się od poprzednio omawianych rodzajów szkodliwego oprogramowania: nie zostało zaprojektowane w celu przejmowania pojedynczych hostów, lecz było platformą programistyczną umożliwiającą uruchamianie długotrwałych operacji zbierania danych wywiadowczych. Na przykład jeden z modułów pozwalał na monitorowanie i przechwytywanie ruchu sieciowego z serwerów webowych usług IIS (ang. *Internet Information Services*), a inny umożliwiał analizę treści wiadomości z serwerów poczty elektronicznej Exchange. Prawdopodobnie najbardziej imponujący moduł pozwalał na przechwytywanie ruchu z kontrolerów stacji bazowych GSM[76]. Ta ostatnia funkcjonalność umożliwiała atakującemu szpiegowanie sieci telefonii komórkowej, na co nie pozwala żaden inny przykład szkodliwego oprogramowania omawiany w tej książce.

Oprócz tych unikatowych możliwości platforma Regin oferowała ogromną liczbę narzędzi, dzięki którym agresorzy mogli przeprowadzić ataki w obrębie całego środowiska informatycznego przedsiębiorstwa. Istniały narzędzia zapewniające zdalny dostęp do maszyn, wykradające hasła, rejestrujące znaki wprowadzane z klawiatury, a nawet dokonujące zrzutów ekranu komputera ofiary. Po infiltracji systemu platforma Regin nie ogranicza atakującego do instalacji tylko jednego narzędzia prowadzącego atak, jak w większości szkodliwego oprogramowania. Zamiast tego pozwala na dobieranie spośród licznych modułów najbardziej adekwatnych do zastanej sytuacji, przez co stanowi zagrożenie dla niemal każdego rodzaju środowiska.

Największa aktywność narzędzia została zaobserwowana w Rosji, co stanowi istotną poszlakę jego miejsca pochodzenia — cele dobierane przez hakerów rządowych są spójne z planami politycznymi i wojskowymi nadzorujących rządów. Często na podstawie analizy doboru ofiar można wskazać cele i poglądy polityczne atakującego kraju.

O ofiarach ataków z wykorzystaniem narzędzia Regin niewiele wiadomo oprócz jednego przypadku. Atak dotyczył Belgacom, dużej spółki telekomunikacyjnej w Belgii. Belgacom świadczy usługi komunikacji globalnej i utrzymuje łącza danych służące milionom klientów w całej Europie. Atak wykryto pierwszy raz w 2013 r., a rozpoczął się w 2010 i obejmował liczne wieloletnie etapy[77]. Nie jest jasne, w jaki sposób intruz pierwotnie dostał się do zaatakowanej sieci, niemniej zdołał zinfiltrować zarówno sieć korporacyjną spółki, jak i systemy wykorzystywane przez klientów, zyskując dostęp do wrażliwych danych komunikacyjnych. Według doniesień niektórych mediów europejskich, pośród głównych celów zaatakowanych poprzez infrastrukturę komunikacyjną Belgacom były Parlament Europejski, Rada Europejska i Komisja Europejska[78].

Ten atak wciąż powoduje problemy. Gdy tylko spółka Belgacom go odkryła, rozpoczęła operację czyszczenia o znacznych rozmiarach, kosztującą miliony, zmierzającą do usunięcia agresora ze środowiska i zablokowania mu dalszego dostępu. Jednak według doniesień „The Intercept" operacja ta mogła się nie powieść, a intruz mógł zachować niewykrytą metodę dostępu i kontynuować działanie. Oficjalnie Belgacom sprzeciwia się takim stwierdzeniom, więc ustalenie, czy atakujący wciąż mają dostęp do środowiska spółki, jest problematyczne.

Kolejną trudnością jest fakt, że ani Belgacom, ani żadna inna organizacja zaatakowana za pomocą narzędzia Regin nie jest w stanie ustalić, jakie dokładnie dane pozyskał intruz. Jedną z przyczyn tego braku wiedzy jest metoda zastosowana na platformie Regin do przechowywania i wysyłania skradzionych danych. Są one przechowywane w pamięci operacyjnej komputera, skąd są wysyłane bezpośrednio na serwer agresora bez dokonywania żadnych zapisów na dysku ofiary. Inne szkodliwe narzędzia wykorzystują pamięć operacyjną komputera do przechowywania niewielkich porcji własnego kodu, ale pomysł składowania w pamięci wykradanych informacji jest w zasadzie niespotykany. Taki sposób działania nastręcza pewnych technicznych trudności, które twórcy narzędzia musieli wyeliminować, by zapewnić pomyślne wykonanie techniki. Przechowywanie danych ofiary w pamięci zamiast na dysku jest nie tylko nowatorskim i rzadkim

podejściem, ale dodatkowo uniemożliwia obrońcom zidentyfikowanie metodami śledczymi, czym intruz był zainteresowany i jakie dane wykradł. Aby obrońcy mogli ustalić motywy działania agresora i ocenić rozmiar wycieku danych, muszą się dowiedzieć, jakie treści są wykradane.

Platforma Regin używa także bardzo sprytnej metody wysyłania skradzionych danych. Przed wysyłką dane są szyfrowane za pomocą autorskiego szyfratora RC5. Następnie narzędzie używa komunikatów protokołu ICMP (ang. *Internet Communication Management Protocol*) i ciasteczek HTTP do ukrycia danych. Protokół ICMP został opracowany do przesyłania informacji o błędach pomiędzy urządzeniami sieciowymi, a ciasteczka HTTP są krótkimi zbiorami informacji używanymi przez przeglądarki internetowe do przechowywania informacji o użytkownikach. Finalnie narzędzie nawiązuje komunikację z serwerami sterowania i nadzoru z wykorzystaniem niestandardowych numerów portów. Atakujący nadużywa mechanizmu przechowywania ciasteczek w przeglądarkach internetowych i korzysta z rozpowszechnionego protokołu komunikacji sieciowej do przesyłania informacji między platformą Regin a zainfekowanymi maszynami. W ten sposób agresor zyskał możliwość przechowywania i przesyłania informacji w obrębie sieci ofiary, a przez używanie autorskich metod szyfrowania znacznie utrudniony był odczyt tych danych, nawet gdy obrońcy mogli je znaleźć. Zastosowanie standardowych komponentów internetowych i sieciowych do implementacji niestandardowej metody skrytego przesyłania danych wskazuje na wysoki poziom umiejętności programistów platformy.

Istnieją dwie znane wersje narzędzia Regin. Wersja 1.0 była aktywnie używana pomiędzy rokiem 2008 a 2011. Pomimo kilkuletniego wykorzystywania do prowadzenia ukierunkowanych ataków ta wersja nie została odkryta, a rozwiązania obronne dostawców usług bezpieczeństwa nie wykrywały narzędzia, co jest bardzo rzadką sytuacją. Kolejne unikatowe i ciekawe zdarzenie dotyczące platformy miało miejsce w 2011 r., kilka lat przed jego odkryciem. W tym roku, zanim wersja 2.0 weszła do operacyjnego wykorzystania, istniejące kopie wersji 1.0 narzędzia zostały planowo usunięte z systemów. Innymi słowy: organizacja stojąca za atakami podjęła celowy wysiłek zmierzający do usunięcia wszelkich śladów narzędzia z komputerów ofiar i z internetowych repozytoriów szkodliwego oprogramowania[79].

Należy pamiętać, że platforma Regin była używana wyłącznie w precyzyjnie kierowanych atakach, więc w internecie pozostały jedynie bardzo nikłe ślady jej działania. Mimo to nawet zatarcie śladów pojedynczego ataku, a co dopiero kilku na przestrzeni trzech lat, byłoby bardzo trudne, lecz organizacja korzystająca z platformy zdołała, poza kilkoma wyjątkami, pomyślnie tego dokonać. Liczba dostępnych próbek jest bardzo niewielka w porównaniu do domniemanej liczby przeprowadzonych ataków. Nawet ta ograniczona ilość przykładów istnieje tylko dlatego, że agresorzy popełnili błędy podczas zacierania śladów lub utracili dostęp do środowiska, zanim zdążyli usunąć swoje narzędzia.

Nie sposób ustalić pochodzenia platformy Regin, ale uważa się, ze względu na istniejące podobieństwa do innych rodzajów szkodliwego oprogramowania wyprodukowanych na Zachodzie, obejmujące zaawansowane możliwości i budowę

wewnętrzną, że platforma, podobnie jak Stuxnet, została utworzona przez amerykańskie agencje wywiadowcze. Alternatywne przypuszczenia mówią o brytyjskim rodowodzie platformy[80]. Istnieją też zwolennicy trzeciej teorii, wskazującej, że narzędzie i ataki były skutkiem łączonej operacji prowadzonej przez oba kraje.

Korea Północna

Zanim Kim Dzong Un objął władzę w Korei Północnej w 2011 r., kraj właściwie nie miał połączenia z internetem ani z resztą świata. Poprzedni władca Korei, Kim Dzong Il, ojciec Kim Dzong Una, wzmacniał swoje wojsko, inwestując w sprzęt i ludzi. Natomiast Kim Dzong Un, w odróżnieniu od swojego ojca, spędził kilka lat poza Koreą Północną, studiując informatykę w Szkole Międzynarodowej w Bernie. Jako dyktator dosyć szybko pojął, jakie znaczenie ma cyberarmia, prawdopodobnie ze względu na swoje doświadczenie akademickie, i zainicjował rozwój zdolności cyberofensywnych Korei Północnej.

Obecnie, według doniesień medialnych, Korea Północna uzyskuje dostęp do internetu oraz szkolenia cyberofensywne zarówno od Chin, jak i od Rosji. Dodatkowo, wedle zeznań uciekiniera z Korei Północnej, północnokoreańscy hakerzy szkolą się w rzemiośle cyberwojennym na dwóch północnokoreańskich uczelniach wyższych[81]. Dzięki dostępowi do internetu oraz rozbudowie cyberzdolności Korea Północna dokonywała kradzieży pieniędzy z instytucji finansowych, zapewniając sobie przychody pomimo ciężkich sankcji ekonomicznych nałożonych na kraj. Sankcje te, narzucone przez Stany Zjednoczone i ONZ, miały zmusić Koreę do przerwania programu nuklearnego, finansowanego ze środków pochodzących z kradzieży.

Jednakże sankcje i ograniczenia raczej motywują Koreę Północną do kontynuowania ataków przeciwko reszcie świata. Najpewniej cyberataki będą trwały, dopóki Korea Północna będzie istniała.

Jednostka 121

Prowadzenie ofensywnych cyberoperacji w Korei Północnej najpewniej należy do kompetencji Generalnego Biura Zwiadowczego (GBZ), północnokoreańskiej agencji wywiadowczej, a konkretniej do oddziału znanego jako Jednostka 121[82]. Północnokoreański zbieg Kim Hueng Kwang podaje w wywiadzie udzielonym serwisowi Reuters, że stan osobowy Jednostki 121 wynosił w styczniu 2015 r. ok. 1800 cyberżołnierzy. Od tamtej pory jednostka została powiększona i obecnie uważa się, że obejmuje od 3000 do 6000 hakerów[83].

Co ciekawe, Jednostka 121 operuje z hotelu położonego w Shenyang w Chinach, którego głównym właścicielem jest przedsiębiorstwo z Korei Północnej. Głównym inwestorem hotelu jest firma Dandong Hongxiang Industrial Development, pochodząca z Chin i utrzymująca długotrwałe relacje biznesowe z Koreą Północną mimo sankcji narzucanych przez Stany Zjednoczone. W 2019 r. właścicielowi spółki i członkom zarządu postawiono w USA zarzuty „prowadzenia niedozwolonej

działalności handlowej w imieniu podmiotów północnokoreańskich, objętych sankcjami w wyniku ich zaangażowania w rozprzestrzenianie broni masowego rażenia”[84].

Oprócz Jednostki 121 agencja GBZ dysponuje także kilkoma innymi oddziałami realizującymi cyberoperacje: Jednostką 180, Jednostką 91 oraz Laboratorium 110. Każdy z tych oddziałów ma osobne zadania wpisujące się w cele GBZ. Co najmniej jeden oddział jest odpowiedzialny za zbieranie i analizę danych wywiadowczych, podczas gdy inny skupia się na hakowaniu i prowadzeniu ataków[85]. Na przykład Jednostka 180 specjalizuje się w atakach na technologie i systemy finansowe, podczas gdy Jednostka 91 odpowiada za kradzież technologii związanych z bronią jądrową i pociskami dalekiego zasięgu. Publicznie znane szczegóły działania tych jednostek pochodzą głównie z zeznań zbiegłych dysydentów, ale jasne jest, że Korea Północna używa cyberataków do rozwoju swojego potencjału militarnego, gospodarczego i wywiadowczego.

Cyberataki

Pomiędzy rokiem 2009 a 2013 Korea Północna przeprowadziła szereg ataków DoS przeciwko instytucjom finansowym, organizacjom rządowym i mediom. Wiele zaatakowanych organizacji zostało także porażonych działaniem szkodliwego oprogramowania, które wymazało dane z ich systemów komputerowych, powodując długofalowe straty.

W 2014 r. Korea Północna przeprowadziła jeden ze swoich najbardziej wyróżniających się ataków przeciwko Sony Pictures Entertainment, rzucając spółkę na kolana. Jak opisywałem we wprowadzeniu do tej książki, w wyniku ataku zostały opublikowane wrażliwe dane pochodzące z firmowej poczty elektronicznej, obejmujące m.in. listy płac i szczegółowe informacje dotyczące filmów w trakcie produkcji. Agresorzy udostępnili także do darmowego pobierania i oglądania wiele filmów, które miały przynieść wytwórni miliony dolarów. W konsekwencji drugocących ataków w firmie doszło do zwolnień[86]. Wytwórnia musiała także ponieść koszty produkcji i gaż aktorskich wykradzionych filmów — kwoty te również sięgały milionów dolarów.

Aby jeszcze pogorszyć sprawę, agresor wkrótce uruchomił drugi etap ataku: sabotaż. Dwudziestego czwartego listopada użył autorskiego oprogramowania czyszczącego, znanego jako Backdoor.Destover, aby wykasować dane z komputerów i serwerów wytwórni oraz zniszczyć infrastrukturę sieciową Sony. W efekcie spółka została zmuszona do przerwania działalności. Wytwórnia zatrudniła firmę Mandiant do usunięcia szkód i zagrożeń z sieci Sony. Jednak zniszczenia już się dokonały, a kurs akcji spółki i jej reputacja zapikowały w dół.

Korea Północna przeprowadziła także długotrwałe cyberataki przeciwko instytucjom finansowym, o których piszę w rozdziale 2.

Podsumowanie

Obrona przed atakami prowadzonymi przez hakerów rządowych wymaga innego podejścia niż obrona przed większością zagrożeń. Jak pokazałem na przykładach w tym rozdziale, hakerzy rządowi działają z zupełnie innych pobudek niż typowi agresorzy. Zwykle dysponują znacznie większymi zasobami i prowadzą długoterminowe, zaawansowane cyberoperacje. Dlatego badanie takich ataków najczęściej wymaga zaangażowania większych środków niż do typowego śledztwa i trwa znacznie dłużej. Lecz jeżeli do odparcia cyberataku rządowego zostaną zastosowane nieprawidłowe metody lub zostanie on potraktowany tak samo jak typowe zagrożenie, to konsekwencje dla bronionej organizacji mogą być druzgocące. Poświęcenie czasu na zrozumienie potencjalnie wrogich obcych krajów może dać obrońcom przewagę w zakresie identyfikowania, poznawania i usuwania hakerów rządowych.

Zwykle analitycy specjalizujący się w atakach prowadzonych przez rządy zajmują się konkretnymi regionami geograficznymi lub państwami. Od takich ekspertów wymagana jest znacznie większa wiedza i zrozumienie przeciwnika niż od większości analityków, ponieważ muszą oni rozumieć także polityczne i militarne motywy działania agresora i być na bieżąco, jeżeli chodzi o wydarzenia dotyczące danego państwa. Zgłębienie tych tematów pozwala lepiej typować kraje, które mogłyby zyskać na przeprowadzeniu danego ataku. Takie zrozumienie klimatu politycznego i wojskowego panującego w regionie zainteresowań pozwala również rozpoznawać i weryfikować fałszywe tożsamości internetowe, działania prowadzone pod fałszywą flagą oraz kampanie dezinformacyjne wiążące się z atakami kierowanymi przez rządy obcych państw.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Tu nie chodzi tylko o hakerów anarchistów. To jest regularna wojna!

Cyberprzestępcy mogą nie tylko wykradać dane i pieniądze. Mogą atakować instytucje rządowe, prać brudne pieniądze i dokonywać aktów terroru. Na naszych oczach toczy się wojna hybrydowa — operacje wojenne przeniosły się częściowo do cyberprzestrzeni. Agresorzy posługują się wyrafinowanymi technikami z rosnącą skutecznością. Niebezpieczeństwo grozi każdemu, również rządom, instytucjom i wielkim korporacjom. Aby się obronić, najpierw trzeba dobrze poznać wroga.

Dzięki temu przewodnikowi zrozumiesz techniki ataków, jak również metody śledcze obrońców. Nauczysz się analizować i śledzić ataki, a także stawiać hipotezy dotyczące ich sprawców. Znajdziesz tu opisy najważniejszych cyberataków, w tym przeprowadzonych na zlecenie rządów. Poznasz świat ukierunkowanych ataków szyfrujących i prób wymuszeń okupu, które sparaliżowały wiele korporacji. Dowiesz się też, w jaki sposób cyberataki służą do zakłócania przebiegu wyborów na całym świecie. Następnie prześledzisz krok po kroku proces analityczny, stosowany przez obrońców do badania każdego etapu cyberkampanii, pozwalający poprawnie zidentyfikować agresora i przygotować się do odpierania kolejnych ataków.

Z pomocą tej książki nauczysz się:

- określać najbardziej prawdopodobnego sprawcę ataku
- chronić się przed najczęściej popełnianymi błędami atrybucji
- analizować wiadomości phishingowe, zawartość rekordów DNS, dane rejestracyjne domen internetowych i wskazówki językowe
- wykrywać długotrwałe kampanie wywiadowcze
- stosować narzędzia analityczne, takie jak Recon-ng lub Wireshark

Jon DiMaggio

od ponad 15 lat zajmuje się identyfikacją, badaniem i opisywaniem zaawansowanych zagrożeń w cyberprzestrzeni. Specjalizuje się w kwestiach wykorzystywania szkodliwego oprogramowania szyfrującego i cyberoperacji obcych rządów. Współpracował z organami ścigania przy sporządzaniu federalnych aktów oskarżenia. Często bierze udział w konferencjach branżowych poświęconych bezpieczeństwu.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-8322-081-9

9 788383 220819

Cena: 69,00 zł

no starch press