Helion

one press

MARC GOODMAN

ZBRODNIE PRZYSZŁOŚCI

JAK CYBERPRZESTĘPCY, KORPORACJE I PAŃSTWA MOGĄ UŻYWAĆ TECHNOLOGII PRZECIWKO TOBIE

Tytuł oryginału: Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It

Tłumaczenie: Michał Lipa
Projekt okładki: Jan Paluch

ISBN: 978-83-283-1729-1

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

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

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

Printed in Poland.

Spis treści

Część II
Przyszłość przestępczości

Część III
Przetrwać postęp

ROZDZIAŁ 1.

Połączeni, zależni, narażeni

Technologia (...) to dziwna rzecz; jedną ręką daje nam wspaniałe dary, a drugą rani nas nożem w plecy.

— CHARLES PERCY SNOW

Życie Mata Honana wyglądało całkiem dobrze na ekranie komputera. W jednej zakładce przeglądarki internetowej wyświetlały się zdjęcia jego maleńkiej córeczki, w drugiej przewijały się „ćwierknięcia" tysięcy osób obserwujących jego profil na Twitterze. Będąc reporterem magazynu „Wired" mieszkającym w San Francisco, wiódł wygodne życie podłączony do sieci i był równie obeznany z technologią jak wiele osób w jego środowisku. Nie miał jednak pojęcia, że jego cyfrowy świat można zniszczyć za pomocą kilku uderzeń w klawisze komputera. Nagle w pewien sierpniowy dzień doszło do katastrofy. Wszystkie jego zdjęcia, e-maile i inne dane wpadły w ręce hakera. Zostały skradzione w ciągu zaledwie kilku minut przez nastolatka z drugiego końca świata. Honan był łatwym celem. Wszyscy jesteśmy.

Honan dobrze pamięta popołudnie, kiedy to wszystko się stało. Bawił się na podłodze ze swoją małą córeczką, kiedy nagle jego iPhone się wyłączył. Bateria mogła się rozładować. Ponieważ czekał na ważny telefon, podłączył urządzenie do ładowarki i uruchomił je. Zamiast zwykłego ekranu startowego z aplikacjami zobaczył jednak wielkie, białe logo Apple i wielojęzyczny komunikat zapraszający do skonfigurowania nowego telefonu. Dziwne.

Honan nie zmartwił się zbytnio, ponieważ co wieczór robił kopię bezpieczeństwa swojego telefonu. Następny krok był zupełnie oczywisty: należało się zalogować do usługi iCloud i odzyskać konfigurację telefonu oraz zapisane w nim dane. Kiedy jednak spróbował to zrobić, dostał komunikat, że jego hasło zostało uznane za niepoprawne przez bogów zarządzających chmurą. Bystry reporter najlepszego na świecie magazynu dotyczącego nowoczesnych technologii miał jeszcze jedną sztuczkę w zanadrzu. Zamierzał podłączyć iPhone'a do laptopa i odzyskać dane z twardego dysku komputera. Kiedy jednak włączył swojego maca, serce niemal zatrzymało mu się w piersi.

Na ekranie pojawił się komunikat wygenerowany przez kalendarz Apple, informujący o nieprawidłowości hasła do usługi Gmail. Zaraz potem wyświetlacz komputera poszarzał i zgasł, jakby urządzenie się wyłączyło. Jedyną rzeczą widoczną na ekranie była prośba o podanie czterocyfrowego hasła. Honan wiedział, że nigdy nie ustalał żadnego hasła dostępu do swojego komputera.

Później dowiedział się, że haker uzyskał dostęp do jego konta iCloud i użył przydatnej funkcji „znajdź mój telefon", żeby zlokalizować wszystkie urządzenia elektroniczne w otoczeniu Honana. Zneutralizował je po kolei. Wydał polecenie zdalnego kasowania danych, wymazując wszystko to, co Honan gromadził całymi latami. Jako pierwszy ofiarą intruza padł iPhone, następnie iPad, a na końcu — choć nie najmniej ważny — MacBook. W jednej chwili wszystkie dane, w tym zdjęcia z pierwszego roku życia córeczki Honana, zniknęły. W ich ślady poszły bezcenne wspomnienia fotograficzne dawno zmarłych krewnych, skasowane przez nieznanego sprawcę.

Następnym celem ataku było konto Google. W mgnieniu oka wyparowały z niego e-maile, które Honan pieczołowicie gromadził i porządkował przez osiem lat. Wątki dotyczące pracy, notatki, przypomnienia i pamiątki zniknęły za jednym kliknięciem myszy. W końcu haker sięgnął po swój najważniejszy łup: konto Honana na Twitterze, przypisane do nicka @Mat. Nie dość, że przejął nad nim kontrolę, to jeszcze podszywając się pod Honana, wykorzystał je do rozpowszechniania rasistowskich i homofobicznych bluzgów wśród obserwujących konto osób.

Po tym internetowym szturmie Honan wykorzystał swoje umiejętności reporterskie w celu ustalenia, co się właściwie stało. Zadzwonił do działu wsparcia technicznego w firmie Apple, żeby odzyskać kontrolę nad kontem iCloud. Po ponad 90-minutowej rozmowie udało mu się ustalić, że „on sam" zadzwonił zaledwie pół godziny wcześniej, aby ustanowić hasło. Okazało się, że w celu dokonania tej operacji wystarczyło podać adres zamieszkania i cztery ostatnie cyfry numeru karty kredytowej. Adres Honana był ogólnie dostępny w rejestrze na stronie Whois, do którego dziennikarz wpisał się, tworząc własną stronę internetową. Nawet gdyby go tam nie było, łatwo byłoby go znaleźć w innych bezpłatnych rejestrach internetowych, takich jak WhitePages.com czy Spokeo.

Chcąc zdobyć ostatnie cztery cyfry numeru karty kredytowej reportera, haker założył, że dziennikarz (podobnie jak większość z nas) ma konto w sklepie Amazon.com. Miał rację. Uzbrojony w imię i nazwisko, adres e-mail oraz adres zamieszkania Honana skontaktował się z działem obsługi klienta sklepu i skutecznie zmanipulował telefonistkę, żeby podała mu końcówkę numeru karty. To wszystko wystarczyło, żeby wywrócić życie Honana do góry nogami. Choć w tym przypadku nic takiego nie miało miejsca, haker mógł wykorzystać te same informacje, żeby zdobyć dostęp do internetowych rachunków bankowego i inwestycyjnego Honana i je splądrować.

Nastolatek, który w końcu przyznał się do ataku — znany w kręgach hakerów pod pseudonimem Phobia — twierdził, że chciał zwrócić uwagę na poważne problemy z bezpieczeństwem usług internetowych, z których korzystamy każdego dnia. Wszystko jasne. Honan założył nowe konto na Twitterze, żeby nawiązać kontakt z napastnikiem. Phobia, występujący teraz w tym serwisie jako @Mat, zgodził się obserwować jego nowe konto, dzięki czemu mogli ze sobą rozmawiać. Honan zadał Phobii jedno pytanie, które nurtowało go od chwili ataku: Dlaczego? Dlaczego zrobiłeś to właśnie mnie? Okazało się, że utracone dane i wspomnienia z całej dekady jego życia były tylko czymś w rodzaju zniszczeń ubocznych.

Odpowiedź Phobii była przerażająca: „Tak naprawdę nic do ciebie nie mam. (...) Po prostu podobała mi się twoja nazwa użytkownika [na Twitterze]". To wszystko. Chodziło tylko o zgrabną, trzyliterową nazwę użytkownika. Haker z drugiego końca świata zapragnął jej dla siebie.

Myśl o tym, że ktoś, kto „nie ma nic do Ciebie", może za pomocą kilku uderzeń w klawisze zniszczyć Twoje cyfrowe życie, graniczy z absurdem. Kiedy historia Honana pojawiła się na okładce magazynu „Wired" w grudniu 2012 roku, wywołała dość duże zainteresowanie, które jednak szybko wygasło. Sprowokowała dyskusję o tym, jak lepiej zabezpieczyć technologie, z których korzystamy na co dzień, ale podobnie jak wiele innych dyskusji w internecie w końcu umarła ona śmiercią naturalną. Od czasu przykrych doświadczeń Honana niewiele się zmieniło. Wciąż jesteśmy tak samo narażeni na ataki jak on wtedy — a może nawet bardziej, ponieważ w jeszcze większym stopniu korzystamy z łatwych do zhakowania aplikacji mobilnych i usług świadczonych w chmurze.

Podobnie jak w przypadku większości z nas różne konta Honana były wzajemnie ze sobą powiązane w sieć opartą na domniemanym zaufaniu: ten sam numer karty kredytowej był przypisany do profilu Apple i konta na Amazonie; adres e-mail przypisany do konta iCloud prowadził do Gmaila i tak dalej. Wszystkie wykorzystywały te same dane — w tym dane logowania, numery kart kredytowych i hasła — powiązane z tą samą osobą. Zabezpieczenia, z których korzystał Honan, nie były niczym więcej niż cyfrową linią Maginota; wątłym domkiem z kart, który zawalił się pod wpływem byle muśnięcia. Wszystkie (lub prawie wszystkie) informacje potrzebne do zniszczenia cyfrowego życia Mata Honana (albo Twojego) są łatwo dostępne dla każdego, kto ma nieczyste intencje albo po prostu jest wystarczająco kreatywny[1].

Postęp i zagrożenia w cyfrowym świecie

W ciągu zaledwie kilku lat bez większego namysłu przebiegliśmy na złamanie karku drogę od surfowania po internecie za pomocą wyszukiwarki Google do korzystania z usług tej firmy w zakresie nawigacji, prowadzenia kalendarza, udostępniania filmów, rozrywki, poczty głosowej i rozmów telefonicznych. Miliard z nas upublicznił najbardziej intymne szczegóły swojego życia na Facebooku i ujawnił wszystkie powiązania z przyjaciółmi, członkami rodziny i współpracownikami. Pobraliśmy z sieci miliardy aplikacji i robimy za ich pomocą wszystko — zaczynając od obsługi kont bankowych, przez gotowanie, po archiwizowanie zdjęć dzieci. Łączymy się z internetem za pomocą laptopów, telefonów komórkowych, iPadów, dekoderów telewizyjnych, konsol do gier, odtwarzaczy filmów, telewizorów i innych urządzeń.

Pozytywne aspekty zmian technologicznych są oczywiste. W ciągu ostatnich stu lat szybki rozwój medycyny doprowadził do dwukrotnego zwiększenia średniej długości życia człowieka oraz dziesięciokrotnego spadku śmiertelności dzieci[2]. Średni dochód *per capita* skorygowany o inflację uległ potrojeniu na całym świecie. Dostęp do wysokiej jakości edukacji, przez tak długi czas będący przywilejem nielicznych, dziś jest powszechny i darmowy dzięki takim stronom jak Khan Academy. A sam telefon komórkowy jest bezpośrednim źródłem rozwoju ekonomicznego narodów na całym świecie, liczonego w miliardach miliardów dolarów[3].

Możliwość nawiązywania wzajemnych połączeń, którą internet zapewnia dzięki swej szczególnej architekturze, oznacza, że obcy sobie ludzie na całym świecie mogą się kontaktować ze sobą w sposób wcześniej niespotykany. Mieszkanka Chicago może grać w *Words with Friends* z zupełne obcym mężczyzną z Holandii. Lekarz z indyjskiego Bangaluru może na odległość odczytywać i interpretować wyniki prześwietlenia pacjenta z Boca Raton na Florydzie. Rolnik z RPA może za pomocą swojego telefonu komórkowego uzyskać dostęp do tych samych danych na temat plonów co doktorant z MIT. Ta cecha internetu jest jedną z jego największych zalet, a w miarę jak globalna sieć się rozwija, rośnie jej potęga i użyteczność. We współczesnym cyfrowym świecie jest się z czego cieszyć.

Niemniej choć zalety tego świata są dobrze opisane i często podkreślane przez osoby z branży, ów skomplikowany system wzajemnych powiązań ma także pewne wady.

Działanie naszych sieci energetycznych, systemów kontroli lotów, systemów dyspozytorskich w straży pożarnej, a nawet wind w biurowcach jest w ogromnym stopniu uzależnione od komputerów. W coraz to większym stopniu podłączamy swoje życie do globalnej sieci informacyjnej, nie poświęcając ani chwili na zastanowienie się, co to wszystko znaczy. Mat Honan przekonał się na własnej skórze, czym to grozi, podobnie jak tysiące innych osób. Pytanie brzmi, jak powinniśmy się zachować w sytuacji, w której wszystkie technologiczne atrybuty współczesnego społeczeństwa — narzędzia, od których coraz bardziej się uzależniamy — nagle przestaną funkcjonować. Jaki mamy plan awaryjny? Tak naprawdę nie mamy żadnego.

Świat jest płaski (i szeroko otwarty)

Przez całe wieki w naszym świecie dominował westfalski model suwerennych państw narodowych[4]. Zgodnie z nim państwa miały pełną niezawisłość w ramach własnych granic terytorialnych i żadne zewnętrzne organy władzy nie mogły się wtrącać w wewnętrzne sprawy kraju. Gwarancją trwałości systemu westfalskiego były granice, armie, straże, bramy i karabiny. Można było kontrolować i ograniczać imigrację i emigrację. Co więcej, istniały cła i instytucje kontrolne nadzorujące przepływ towarów przez granice. Niemniej o ile sygnatariusze traktatu westfalskiego wykazali się w 1648 roku pewną dalekowzrocznością, żaden z nich nie mógł przewidzieć powstania Snapchata.

Choć granice fizyczne wciąż mają pewne znaczenie, w cyfrowym świecie takie podziały są coraz mniej wyraźne. Bity i bajty przepływają swobodnie z jednego kraju do drugiego bez żadnej kontroli granicznej, imigracyjnej ani celnej, które mogłyby spowalniać ich transfer. Tradycyjne międzynarodowe bariery przestępczości ograniczające swobodę poprzednich pokoleń złodziei, bandytów i skazańców zniknęły w wirtualnym świecie, dzięki czemu różne podejrzane indywidua mogą swobodnie odwiedzać wszystkie wirtualne lokalizacje, jakie przyjdą im do głowy.

Pomyśl o tym, jakie wynikają z tego implikacje dla naszego bezpieczeństwa. Kiedyś gdy przestępcy obrabowali bank na nowojorskim Times Square, kilka rzeczy można było uważać za oczywiste. Po pierwsze, z góry zakładano, że rabusie musieli wejść do oddziału banku mieszczącego się w rejonie podlegającym komisariatowi Midtown South nowojorskiej policji (NYPD). Obrabowanie banku stanowiło pogwałcenie przepisów stanowych i federalnych, zatem wiadomo było, że śledztwo poprowadzą wspólnie NYPD i FBI. Ofiara przestępstwa (w tym przypadku bank) miała siedzibę w obrębie właściwości terytorialnej odpowiednich organów władzy, co znacznie upraszczało postępowanie. Podstawą śledztwa były dowody fizyczne pozostawione na miejscu przestępstwa przez złodzieja, w tym odciski palców na kartce podanej kasjerowi, ślady DNA pozostawione na kontuarze, przez który przeskoczył bandyta, a być może także obraz jego twarzy zarejestrowany przez kamerę bezpieczeństwa. Co więcej, samo przestępstwo również podlegało konkretnym ograniczeniom fizycznym. Ukradzione dolary miały określoną objętość i masę, zatem rabuś nie mógł zabrać ich zbyt dużo. W workach z pieniędzmi mogły się znajdować eksplodujące pojemniki z farbą do trwałego oznaczania ukradzionych banknotów. Niemniej w dzisiejszym świecie istniejące od dawien dawna wypróbowane pewniki śledcze, takie jak jurysdykcja organów ścigania i dowody fizyczne — podstawowe niegdyś narzędzia wyjaśniania zbrodni — często zupełnie tracą znaczenie.

Porównaj powyższy scenariusz kradzieży na Times Square z niesławnym przypadkiem obrabowania banku przez internet w 1994 roku przez Vladimira Levina działającego z własnego mieszkania w Petersburgu. Levina, z zawodu programistę, oskarżono o włamanie na szereg kont klientów korporacyjnych Citibanku i kradzież

10,7 miliona dolarów[5]. Korzystając z pomocy wspólników na całym świecie, Levin przelał środki na konta w Finlandii, Stanach Zjednoczonych, Holandii, Niemczech i Izraelu.

Kto powinien prowadzić śledztwo w tej sprawie? Czy policja w Stanach Zjednoczonych, w których mieściła się siedziba poszkodowanego banku? A może stróże prawa z Petersburga, w którym podejrzany dopuścił się czynu zabronionego? Dlaczego nie organy ścigania w Izraelu albo Finlandii, skoro tam trafiły ukradzione pieniądze? Levin nie pojechał do Stanów Zjednoczonych, żeby popełnić przestępstwo. Nie zostawił odcisków palców ani śladów DNA, a banknoty nie zostały zabrudzone farbą z eksplodującego pojemnika. W ogóle nie było żadnych banknotów — Levin nie musiał na własnych plecach wynosić z banku tysięcy kilogramów papierowych pieniędzy, ponieważ dokonał przestępstwa za pomocą myszy i klawiatury. Nie potrzebował też maski ani obrzyna. Po prostu schronił się za ekranem komputera i ukrył ślady, korzystając z wirtualnych okrężnych dróg.

Natura internetu sprawia, że wszyscy żyjemy w świecie zanikających granic. Dziś każdy, niezależnie od intencji, może podróżować wirtualnie z prędkością światła po całej planecie. Dla przestępców ta technologia jest dobrodziejstwem, ponieważ pozwala skakać z kraju do kraju i kluczyć po całym świecie ku rozpaczy policji. Kryminaliści nauczyli się też, jak uchronić się przed wyśledzeniem w sieci. Sprytny haker nigdy nie zainicjuje ataku na bank w Brazylii bezpośrednio ze swojego mieszkania we Francji. Zamiast tego będzie się włamywał do kolejnych sieci, przenosząc się na przykład z Francji do Turcji, następnie do Arabii Saudyjskiej i tak dalej, aż do osiągnięcia ostatecznego celu w Brazylii. Ta możliwość skakania z kraju do kraju, będąca jedną z największych zalet internetu, jest źródłem ogromnych problemów jurysdykcyjnych i administracyjnych dla organów ścigania oraz jest jedną z głównych przyczyn, dla których śledztwa w sprawach dotyczących cyberprzestępczości są tak trudne i często nieudolne. Policjant z Paryża nie ma uprawnień, by dokonać aresztowania w São Paulo.

Stare dobre czasy cyberprzestępczości

Charakter zagrożeń cyfrowych bardzo się zmienił w ciągu ostatnich 25 lat. W pierwszych latach istnienia komputerów osobistych hakerzy dokonywali włamań głównie „dla beki", czyli dla śmiechu. Włamywali się do systemów komputerowych po to, żeby udowodnić, że potrafią, albo przekazać jakiś komunikat. Jednym z pierwszych wirusów infekujących komputery klasy IBM PC był Brain, stworzony w 1986 roku przez braci Amjada Farooqa Alviego i Basita Farooqa Alviego z pakistańskiego miasta Lahore[6]. Amjad miał 24 lata, jego brat 17. Ich wirus miał być zupełnie nieszkodliwy, a jego celem miało być powstrzymanie ludzi przed kopiowaniem oprogramowania, nad którym bracia pracowali przez kilka lat. Brain infekował sektor rozruchowy dyskietki,

zapobiegając kopiowaniu zawartości i umożliwiając jego twórcom śledzenie nielegalnych kopii ich programu. Bracia zmartwieni tym, że ludzie kradną ich oprogramowanie, zapisali w kodzie wirusa złowieszczy komunikat, który wyświetlał się na ekranach komputerów należących do zainfekowanych użytkowników:

> **Welcome to the Dungeon © 1986 Brain & Amjads (pvt). BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791, 443248, 280530. Beware of this VIRUS… Contact us for vaccination…**

Ten komunikat jest godny uwagi z kilku powodów. Po pierwsze, bracia stwierdzili w nim, że ich wirus jest chroniony prawem autorskim, co było dość odważnym posunięciem. Jeszcze dziwniejsze było to, że podali swój adres i numery telefonów, umożliwiając ludziom kontaktowanie się z nimi w sprawie „szczepionki", czyli usunięcia wirusa. Przesłanki, którymi Basit i Amjad kierowali się, tworząc wirusa, wydawały im się zupełnie logiczne. Bracia nie wiedzieli jednak, że ich dziecko posiada zdolność samoreplikacji i rozprzestrzeniania się w bardzo staroświecki sposób: za pośrednictwem ludzi przenoszących dyskietki (wtedy jeszcze o średnicy 5,25 cala) z komputera do komputera. W końcu Brain okrążył naszą planetę, przedstawiając Basita i Amjada całemu światu[7].

Wraz z upływem czasu hakerzy stawali się coraz bardziej ambitni i złośliwi. Możliwość kontaktowania się z innymi użytkownikami na grupach dyskusyjnych sprawiła, że wirusy cyfrowe nie musiały już rozprzestrzeniać się za pomocą „trampkonetu", czyli osób przenoszących dyskietki z komputera do komputera, lecz dzięki modemom mogły podróżować liniami telefonicznymi do ludzi korzystających z usług pierwszych dostawców internetu, takich jak CompuServe, Prodigy, EarthLink i AOL. Nowsze wirusy i konie trojańskie, takie jak Melissa (1999), ILOVEYOU (2000), Code Red (2001), Slammer (2003) i Sasser (2004), mogły z łatwością zarażać komputery z systemem Windows na całym świecie, kasując prace semestralne, przepisy kulinarne, listy miłosne i sprawozdania przedsiębiorstw zapisane na twardych dyskach. Nagle okazało się, że każdy z nas może coś stracić.

Złośliwe oprogramowanie komputerowe, określane mianem *malware*, będącym zbitką słów *malicious* (złośliwy) i *software* (oprogramowanie) przybiera dziś różne formy, ale jego celem zawsze jest niszczenie, przeszkadzanie, dokonywanie kradzieży albo wykonywanie nielegalnych lub nieautoryzowanych działań w systemie albo sieci:

- Wirusy komputerowe rozprzestrzeniają się poprzez dołączanie kopii samych siebie do innych programów, tak samo jak biologiczne wirusy zarażają dostępne organizmy żywe.
- Robaki komputerowe także wyrządzają szkody, ale są odrębnymi programami i nie potrzebują nosiciela, żeby się rozprzestrzeniać.

- Konie trojańskie, nazwane tak na wzór mitycznego drewnianego konia, w brzuchu którego Grecy dostali się do Troi, często udają prawidłowe i bezpieczne oprogramowanie, a ich aktywacja następuje w momencie, w którym użytkownik daje się namówić do pobrania i uruchomienia plików w systemie będącym celem ataku. Trojany często tworzą „tylne wejścia" umożliwiające hakerom uzyskanie stałego dostępu do zainfekowanego systemu. Nie powielają się metodą infekowania innych plików, lecz raczej skłaniają użytkowników do kliknięcia pliku albo otwarcia zarażonego załącznika do wiadomości e-mail.

Dzisiejsi twórcy wirusów wiedzą, że do opinii publicznej powoli (bardzo powoli) zaczynają docierać przestrogi przed otwieraniem plików przysłanych przez obce osoby. Dlatego zmienili sposób postępowania i stosują technikę *drive-by download*, polegającą na wykorzystywaniu przez złośliwe oprogramowanie słabości języków skryptowych, takich jak Java i ActiveX, powszechnie używanych przez przeglądarki internetowe. Świat przeniósł się do sieci, a hakowanie takich narzędzi jak Internet Explorer, Firefox i Safari jest sensowne z punktu widzenia przestępców, choć ich nowy modus operandi naraża niczego niepodejrzewających użytkowników na duże koszty. Badacze z Palo Alto Networks odkryli, że nawet 90% współczesnego złośliwego oprogramowania rozprzestrzenia się za pośrednictwem uprzednio zhakowanych popularnych stron internetowych, które zarażają system w momencie, w którym niepodejrzewający niczego internauta wyświetla je na swoim komputerze[8]. Wiele dużych firm, w tym Yahoo! — operator jednego z najczęściej odwiedzanych portali w internecie — padło ofiarą hakerów i mimowolnie zarażało swoich klientów zaglądających na ich strony w poszukiwaniu wyników rozgrywek sportowych i notowań rynku[9].

Wysyp złośliwego oprogramowania

Dzisiejsi hakerzy nie uprawiają już swojego rzemiosła „dla beki", lecz dla pieniędzy, informacji i władzy. Na początku XXI wieku, kiedy zorientowali się, że mogą zarobić na złośliwym oprogramowaniu, dopuszczając się kradzieży tożsamości i innych występków, liczba nowych wirusów zaczęła rosnąć w błyskawicznym tempie. Do 2015 roku osiągnęła zdumiewający poziom. W 2010 roku niemiecki instytut badawczy AV-Test oszacował, że istnieje około 49 milionów odmian złośliwego oprogramowania[10]. W 2011 roku produkująca oprogramowanie antywirusowe firma McAfee donosiła, że co miesiąc wykrywa dwa miliony nowych złośliwych programów. Latem 2013 roku zajmująca się cyberbezpieczeństwem firma Kaspersky Lab poinformowała, że codziennie identyfikuje i wyizolowuje prawie 200 tysięcy próbek złośliwego oprogramowania[11].

Przyjmując cyniczne podejście do powyższych statystyk i zakładając, że w interesie firm produkujących oprogramowanie antywirusowe leży wyolbrzymianie problemu,

który mają zwalczać, moglibyśmy znacznie obniżyć te szacunki — powiedzmy o 50 albo nawet 75%. Nawet wtedy musielibyśmy się jednak pogodzić z faktem, że codziennie na świecie pojawia się 50 tysięcy nowych wirusów. Pomyśl o olbrzymim wysiłku badawczo-rozwojowym w skali globalnej, który jest potrzebny do stworzenia tak dużej ilości oryginalnego kodu.

Właściciele przedsiębiorstw wiedzą, jak kosztowna jest działalność badawczo-rozwojowa. Wobec tego zwrot z inwestycji uzasadniający nieustające tworzenie tak ogromnej ilości nielegalnego oprogramowania przez środowisko przestępcze musi być olbrzymi. Wyniki niezależnego badania przeprowadzonego przez godną zaufania instytucję Consumers Union, wydającą magazyn „Consumer Reports", wydają się potwierdzać rosnący wpływ złośliwego oprogramowania na nasze życie. Ankieta przeprowadzona wśród członków tej organizacji ujawniła, że jedna trzecia gospodarstw domowych w Stanach Zjednoczonych przeżyła w zeszłym roku infekcję sprzętu komputerowego złośliwym oprogramowaniem, co kosztowało konsumentów zawrotną sumę 2,3 miliarda dolarów w ujęciu rocznym[12]. A trzeba pamiętać, że dane te dotyczą tylko ludzi, którzy wiedzą, że zostali zaatakowani.

Iluzja bezpieczeństwa

Każdego roku konsumenci i firmy na całym świecie pokładają wiarę w to, że branża zajmująca się produkcją programów antywirusowych ochroni ich przed narastającym zagrożeniem ze strony złośliwego oprogramowania. Z badań przeprowadzonych przez Gartner Group wynika, że w 2012 roku na całym świecie wydano prawie 20 miliardów dolarów na programy antywirusowe, a kwota ta wzrośnie do 94 miliardów dolarów w 2017 roku[13].

Kiedy zapytasz przeciętnego użytkownika komputerów, jak należy się chronić przed wirusami, w odpowiedzi usłyszysz przede wszystkim, że należy korzystać z oprogramowania antywirusowego takich firm jak Symantec, McAfee czy Trend Micro. To instynktowna reakcja dobrze wytresowanych klientów. Choć tego typu narzędzia mogły być przydatne w przeszłości, szybko tracą skuteczność, a dane statystyczne są bardzo odkrywcze. W grudniu 2012 roku eksperci z mieszczącej się w kalifornijskim mieście Redwood Shores firmy Imperva, która zajmuje się monitorowaniem bezpieczeństwa danych, oraz studenci izraelskiego Instytutu Technologii Technion w Hajfie postanowili poddać próbie standardowe narzędzia antywirusowe. Zebrali 82 nowe wirusy komputerowe i uruchomili je pod okiem programów wykrywających zagrożenia, wyprodukowanych przez ponad 40 największych na świecie firm zajmujących się tworzeniem takiego oprogramowania, w tym takich gigantów jak Microsoft, Symantec, McAfee i Kaspersky Lab. Wynik: do wykrycia zagrożenia doszło w zaledwie 5% przypadków, co oznacza, że 95% wirusów nie zostało wykrytych[14]. To znaczy również, że opro-

gramowanie antywirusowe działające na Twoim komputerze prawdopodobnie wyłapuje tylko 5% pojawiających się zagrożeń. Gdyby skuteczność układu odpornościowego Twojego organizmu spadła nagle do takiego poziomu, umarłbyś w ciągu kilku godzin.

Po kilku miesiącach od pojawienia się nowego zagrożenia najwięksi gracze w tej branży w końcu aktualizują swoje oprogramowanie, ale oczywiście wtedy jest już za późno. Faktem jest, że przestępcy i twórcy wirusów są o wiele bardziej innowacyjni niż firmy mające nas chronić przed zagrożeniem z ich strony i potrafią je przechytrzyć w każdej sytuacji. Co gorsza, od momentu wprowadzenia złośliwego oprogramowania do chwili jego wykrycia upływa coraz więcej czasu. Na przykład w 2012 roku specjaliści z moskiewskiej firmy Kaspersky Lab odkryli bardzo skomplikowany złośliwy program o nazwie Flame, który wykradał dane z systemów informatycznych na całym świecie przez ponad pięć lat przed wykryciem. Mikko Hypponen, cieszący się wielkim szacunkiem dyrektor pionu badawczego w firmie F-Secure, nazwał ten przypadek porażką branży antywirusowej i stwierdził, że on i jego koledzy mogą być „poza ligą we własnej dyscyplinie". Choć miliony ludzi na całym świecie wierzą w skuteczność tych narzędzi, jest całkiem jasne, że era programów antywirusowych dobiegła końca[15].

Jedną z przyczyn, dla których coraz trudniej jest przeciwdziałać niezwykle różnorodnym zagrożeniom technologicznym w dzisiejszym życiu jest gwałtownie rosnąca liczba tak zwanych *zero-day exploits*. Taki atak polega na wykorzystaniu wcześniej nieznanej dziury w oprogramowaniu komputerowym, której programiści i specjaliści od zabezpieczeń nie zdążyli jeszcze załatać. Zamiast aktywnie szukać takich niedoskonałości oprogramowania na własną rękę, producenci systemów antywirusowych uwzględniają tylko znane informacje. Blokują złośliwy kod tylko wtedy, gdy jest podobny do innego złośliwego kodu, z którym mieli wcześniej do czynienia. To tak, jakbyśmy rozsyłali listy gończe za Bonnie i Clyde'em, ponieważ wiemy, że w przeszłości okradali banki. Kasjerzy wypatrywaliby w tłumie klientów ich twarzy, ale dopóki w zasięgu wzroku nie pojawiłby się nikt pasujący do rysopisu tej słynnej pary, nie obawialiby się napadu — przynajmniej dopóki nie dopuściłby się go inny rabuś. Coraz częściej dochodzi do ataków *zero-day* na szeroką gamę popularnych produktów, zaczynając od systemu Microsoft Windows, przez routery Linksys, po bardzo rozpowszechnione programy PDF Reader i Flash Player firmy Adobe.

W końcu hakerzy nauczyli się, że im więcej hałasu narobią przy włamywaniu się do systemu, tym szybciej problem zostanie naprawiony, a oni pozbawieni dostępu. Dlatego teraz liczy się przede wszystkim ostrożność i ukradkowość, jak w przypadku instalowania „śpiochów" w atakowanych komputerach. Można by pomyśleć, że ujawniony przez Impervę zatrważająco niski wskaźnik detekcji wirusów, wynoszący 5%, dotyczy tylko przeciętnych obywateli używających podstawowych programów antywirusowych na swoich komputerach domowych. Firmy dysponujące ogromnymi środkami na rozbudowę i ochronę infrastruktury informatycznej powinny przecież lepiej sobie radzić z hakerami, czyż nie? Niezupełnie. Dziesiątki tysięcy skutecznych ataków na największe

korporacje, organizacje pozarządowe i instytucje państwowe na całym świecie świadczą o tym, że duże organizacje mimo skali ponoszonych wydatków wcale nie radzą sobie z ochroną własnych informacji dużo lepiej niż przeciętny użytkownik urządzeń elektronicznych.

Według opublikowanego przez firmę Verizon raportu *2013 Data Breach Investigation Report* większość firm okazała się po prostu niezdolna do wykrycia dokonanego przez hakera włamania do ich systemów informatycznych. Z bardzo ważnego badania przeprowadzonego przez dział usług biznesowych Verizona, amerykańską Secret Service, holenderską policję i działającą w brytyjskiej policji centralną jednostkę ds. zwalczania cyberprzestępczości wynika, że w 62% przypadków wykrycie ataków na firmy zajmowało co najmniej 2 miesiące[16]. Podobne badanie przeprowadziła firma Trustwave Holdings: okazało się, że średni czas upływający od pierwszego włamania do sieci przedsiębiorstwa do jego wykrycia wynosi aż 210 dni[17]. To prawie siedem miesięcy, w czasie których atakujący — bez względu na to, czy jest nim zorganizowana grupa przestępcza, konkurencyjna firma, czy organy państwowe innego kraju — może swobodnie penetrować sieć przedsiębiorstwa, wykradać jego sekrety, zdobywać informacje wywiadowcze, szperać w systemie finansowym i kraść dane osobowe klientów, w tym numery ich kart kredytowych.

Kiedy firma w końcu zauważa, że jej najważniejsze systemy informatyczne padły ofiarą włamywaczy i ktoś ją szpieguje, w 92% przypadków odkrycia tego nie dokonuje dyrektor ds. systemów informatycznych, zespół zajmujący się bezpieczeństwem danych ani administrator systemu[18], lecz organy ścigania, wściekły klient albo podwykonawca. Skoro największe przedsiębiorstwa, wydające w sumie miliony dolarów na zabezpieczenia systemów i posiadające zespoły specjalistów, którzy przez całą dobę czuwają nad bezpieczeństwem sieci, mogą tak łatwo paść ofiarą hakerów, szanse użytkowników domowych na uchronienie się przed wykradaniem informacji wydają się raczej nikłe.

Jak trudno jest włamać się do przeciętnego komputera? Śmiesznie łatwo. Według raportu Verizona kiedy hakerzy zainteresują się Twoim komputerem, w 75% przypadków na pokonanie zabezpieczeń wystarcza im kilka minut. Z tego samego dokumentu można się dowiedzieć, że tylko w 15% przypadków na włamanie się do systemu potrzeba więcej niż kilku godzin. Wnioski płynące z tego raportu są bardzo doniosłe. Jeśli haker postanowi wejść do Twojego świata, w 75% przypadków zabawa kończy się po kilku minutach[19]. Zostajesz pobity, obezwładniony i powalony na ziemię, zanim się zorientujesz, co się dzieje. W dzisiejszym świecie hakerzy bez skrępowania i zupełnie swobodnie całymi miesiącami buszują po naszych komputerach, czekając na dobrą okazję, czając się i wykradając wszystko, zaczynając od haseł, przez dane dotyczące spraw zawodowych, a kończąc na starych zdjęciach. Jesteśmy celem równie łatwym jak siedząca kaczka. To bardzo dziwne, że jako społeczeństwo pozwalamy na to. Gdyby ktoś z nas zauważył w swoim domu włamywacza przyglądającego się mu w czasie snu i filmującego go pod prysznicem, natychmiast zadzwoniłby na policję (ewentualnie zacząłby krzy-

czeć albo nawet sięgnął po broń). W cyberprzestrzeni do takich sytuacji dochodzi codziennie, a mimo to większość z nas zachowuje spokój, pławiąc się w błogiej nieświadomości zagrożenia, mimo ogromnej podatności na ataki i ciągłej obecności złoczyńców podglądających nas w czasie snu.

Koszty globalnego braku bezpieczeństwa w cyberprzestrzeni nieustannie rosną. Choć firmy na całym świecie są na najlepszej drodze do wydania blisko 100 miliardów dolarów do 2017 roku na programowe i sprzętowe zabezpieczenia systemów, ta kwota jest zaledwie punktem wyjścia przy szacowaniu całkowitych skutków ekonomicznych naszej wrażliwości technologicznej. Rozważmy na przykład dokonany w 2007 roku atak na firmę TJX, do której należą sieci sklepów T.J. Maxx i Marshalls w Stanach Zjednoczonych oraz T.K. Maxx w Europie.

Hakerzy wykradli numery kart kredytowych ponad 45 milionów klientów, tym samym dopuszczając się największego przestępstwa hakerskiego w tamtym czasie[20]. Podczas procesu sądowego ujawniono, że faktyczna liczba poszkodowanych sięgała 94 milionów[21]. Choć spółka TJX doszła do porozumienia z firmami Visa i MasterCard oraz z klientami, co kosztowało ją 256 milionów dolarów, wielu analityków uważa, że rzeczywiste koszty mogły sięgać nawet miliarda dolarów[22]. Jednym z najbardziej wiarygodnych źródeł informacji na temat kosztów naruszeń bezpieczeństwa danych jest Ponemon Institute — organizacja przeprowadzająca niezależne badania dotyczące ochrony danych i polityki bezpieczeństwa informacji[23]. Jej specjaliści uważają, że podczas kalkulowania kosztów należy uwzględnić w analizie znacznie więcej niż tylko wartość bezpośrednich strat poniesionych przez poszkodowanych.

Na przykład ofiara ataków taka jak TJX musi wydać dużo pieniędzy na wykrycie naruszenia, pozbycie się intruzów, zbadanie sprawy, zidentyfikowanie sprawców oraz naprawę i przywrócenie do pełnej sprawności sieci komputerowej. Co więcej, często następuje znaczny spadek sprzedaży, kiedy nieufna klientela rezygnuje z korzystania z usług firmy uważanej za niepewną i niedostatecznie zabezpieczoną. Dodajmy do tego koszty wymiany kart kredytowych (obecnie szacowane na 5,1 dolara za jedną kartę), cenę usług monitorowania kart kredytowych, z których musi skorzystać ofiara ataków, żeby zapobiec okradaniu kart klientów, a także rosnące składki z tytułu ubezpieczeń od cyberataków, żeby zrozumieć, jak szybko mogą rosnąć całkowite straty będące efektem działań hakerów[24]. Nic dziwnego, że większość firm niechętnie się przyznaje do bycia ofiarą cyberprzestępców, a wiele stara się dementować doniesienia o atakach tak długo, jak to możliwe.

Są także inne, jeszcze wyższe koszty, które należy uwzględnić, w tym karę wymierzaną ofiarom ataku przez giełdę, na której notowania ich akcji gwałtownie spadają po ujawnieniu cyberataku. Na przykład wartość rynkowa spółki Global Payments spadła o 9% w ciągu jednego dnia, zanim nowojorska giełda NYSE zawiesiła jej notowania[25]. Skalę problemów finansowych dodatkowo zwiększają pozwy grupowe składane przez klientów i akcjonariuszy firm oraz organy nadzoru. Biorąc to wszystko pod uwagę, Ponemon Institute oszacował, że koszty związane z wykradnięciem jednego rekordu

danych wynoszą prawie 188 dolarów[26]. Wystarczy pomnożyć tę wartość przez liczbę niemal 100 milionów rekordów wykradzionych z komputerów firmy TJX, żeby zobaczyć, jak szybko rosną koszty naruszeń bezpieczeństwa danych i że jest to wzrost wykładniczy.

Warto dodać, że oprócz sum wydawanych na w większości nieskuteczne działania zapobiegawcze oraz zamykanie wrót systemu już po tym, jak dane wydostały się na zewnątrz (a złodzieje dostali się do środka), słono płacimy jako społeczeństwo za naszą technologiczną niepewność. Co gorsza, rosnący poziom wzajemnych połączeń w oplecionym siecią świecie oraz towarzysząca mu radykalna zależność od łatwych do spenetrowania technologii mogą zaszkodzić nie tylko naszym portfelom.

Internet stracił cnotę. Świat opleciony siecią staje się coraz bardziej niebezpieczny, a im chętniej korzystamy z podatnych na ataki technologii w życiu codziennym, tym bardziej sami się narażamy. Kolejna rewolucja przemysłowa, tym razem pod postacią rewolucji informatycznej, jest w bardzo zaawansowanym stadium i niesie ze sobą poważne, choć jeszcze niedostrzegane implikacje dla naszego bezpieczeństwa osobistego i globalnego. Niemniej choć zagrożenia dla ludzi, organizacji, a nawet najważniejszych elementów infrastruktury już teraz wydają się przerażające, technologiczny pociąg właśnie odjeżdża ze stacji, nabierając prędkości w tempie wykładniczym. Sygnały można dostrzec wszędzie, jeśli się wie, gdzie patrzeć.

Tuż nad horyzontem widoczne są już nowe technologie z zakresu robotyki, sztucznej inteligencji, genetyki, biologii syntetycznej, nanotechnologii, drukowania 3-D, neurologii i rzeczywistości wirtualnej, które będą miały poważny wpływ na kształt naszego świata i pociągną za sobą takie zagrożenia, przy których dzisiejsza cyberprzestępczość będzie się wydawała dziecinną zabawą. Za kilka lat wszystkie te innowacje będą odgrywały ważną rolę w życiu codziennym, a mimo to nie przeprowadzono żadnego wnikliwego, zakrojonego na dużą skalę badania, które pomogłoby nam zrozumieć ryzyko z nimi związane.

Głębokość i zakres tej transformacji oraz towarzyszących jej zagrożeń do tej pory umykały uwadze wielu z nas, ale zanim zdamy sobie z nich sprawę, podłączymy do internetu aż bilion nowych urządzeń, które będą obecne w każdym aspekcie naszego życia. Będziemy nieustannie połączeni z ludźmi i maszynami na całej planecie, na dobre i na złe, i staniemy się nieodłączną częścią ogromnego królestwa rozwijającej się w tempie wykładniczym kolektywnej świadomości. W efekcie technologia przestanie dotyczyć tylko maszyn i stanie się częścią samej historii życia. Ci, którzy wiedzą, jak działają jej podstawowe mechanizmy, będą zajmowali coraz lepszą pozycję, pozwalającą im wykorzystywać ją dla własnej korzyści oraz — o czym już się przekonaliśmy — ze szkodą dla przeciętnego człowieka. Obfitość nowinek technologicznych, które wpuszczamy do swojego życia bez żadnej refleksji i głębszego namysłu, może odbić nam się czkawką. Związane z nimi zagrożenia są zapowiedzią nowej normalności — przyszłości, na którą jesteśmy zupełnie nieprzygotowani. Oto książka o człowieku i maszynie oraz o tym, jak niewolnik może stać się panem.

Nie istnieje taki system informatyczny, który byłby w pełni bezpieczny. Codziennie zdarzają się włamania do systemów bankowych czy kradzieże najwrażliwszych danych z serwerów. Hakerzy potrafią także wykorzystać telefon ofiary do szpiegowania, szantażu i stalkingu. Dynamiczny rozwój technologii i nauki może zaowocować wieloma niespotykanymi dotąd zagrożeniami, związanymi z bezpieczeństwem danych. Hakerzy, szantażyści, terroryści, psychopaci i zwykli złodzieje stale przetrząsają sieć w poszukiwaniu słabych punktów, podatnych na atak.

Niniejsza książka jest zadziwiającą podróżą do najmroczniejszych otchłani cyfrowego świata. Choć momentami sprawia wrażenie dobrze wyreżyserowanej fikcji, opisuje wyłącznie czyste fakty. Autor pokazuje, jak technologie jutra, takie jak robotyka, biologia syntetyczna, sztuczna inteligencja, nanotechnologia i komputery kwantowe, mogą być wykorzystane przez przestępców. Książka uświadamia, jakie konsekwencje niesie ze sobą istnienie globalnej sieci. Opisano tu także proste czynności, dzięki którym łatwiej jest uchronić sieć przed atakami. To książka prowokująca i ekscytująca, prawdziwy poradnik przetrwania w niebezpiecznym świecie potężnych zbiorów danych.

Przeczytasz tu między innymi o:

- konsekwencjach tworzenia globalnej sieci i podłączania do niej nowych urządzeń
- niebezpiecznych usługach, naruszeniach prywatności i kradzieży tożsamości
- tym, dokąd zmierza przestępczość i jak będą wyglądać zbrodnie przyszłości
- celach hakerów, którymi za chwilę staną się domy, samochody i... nasze ciała
- podstawowych zasadach bezpieczeństwa w technologicznie zaawansowanym świecie

MARC GOODMAN – niekwestionowany autorytet w dziedzinie bezpieczeństwa globalnego. Od początku swojej kariery jest związany z kryminalistyką. Był głównym futurologiem w FBI, doradcą Interpolu, a także policjantem patrolującym ulice. Jako założyciel Future Crimes Institute oraz szef Katedry Polityki, Prawa i Etyki na Uniwersytecie Osobliwości w Dolinie Krzemowej nie przestaje badać intrygującego, a często i przerażającego pogranicza nauki i bezpieczeństwa, odkrywa rodzące się zagrożenia i zwalcza ciemną stronę technologii.

ZBRODNIE PRZYSZŁOŚCI DZIEJĄ SIĘ JUŻ DZIŚ!

Helion
41599 numer katalogowy
księgarnia internetowa
http://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900
Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci
Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl
ISBN 978-83-283-1729-1
9 788328 317291
Informatyka w najlepszym wydaniu
cena: 49,90 zł