Pamiętniki hakerów

Autor: Dan Verton
Tłumaczenie: Krzysztof Masłowski
ISBN: 83-7197-923-1
Tytuł oryginału: The Hacker Diaries: Confessions of Teenage Hackers
Format: B5, stron: 198

Książka opowiada historie życia tych, którzy stanowili elitę hakerskiej subkultury nastolatków, odgrywających główne role na tej scenie. To więcej niż prosty ciąg kilku opowieści o technicznych aspektach ich wyczynów hakerskich i włamań do systemów. Jest to historia technologicznego czarodziejstwa, kreatywności i poświęcenia. Historia młodzieńczego buntu, nudy i frustracji, oderwania od społeczeństwa, gniewu i czasu spędzonego w więzieniu. Historia nastoletnich hakerów, którzy nie są potworami, o jakich czytamy. Są jak inni w ich wieku, a niektórzy z nich zapewne mieszkają w Waszym sąsiedztwie.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.

Operacja Claymore, czyli wielkie polowanie na Mafiaboya

We wtorek 8 czerwca 1999 roku krótko po 12.00 uczniowie szkoły średniej w małym miasteczku Sisters w stanie Oregon zbiegli na dół do holu, szukając Johna Rennera. Znaleźli go w sali, gdzie jak zawsze prowadził zajęcia z wiedzy o społeczeństwie.

Jeden z uczniów wsadził głowę do klasy i powiedział: „Padł jeden z serwerów. Nie możemy dostać się do naszych plików i stron WWW".

Renner, który pełnił również funkcję szkolnego koordynatora technicznego, nie przejął się zbytnio wieścią o awarii serwera. System padał już wcześniej i zwykle wystarczało kilka niewielkich poprawek, by zaczął ponownie działać. Ale w głosie uczniów było coś, co kazało mu się zastanowić, a wyraz twarzy jednego z chłopców sugerował mu, że należy od razu zobaczyć, co się stało. Ponadto serwer, o którym była mowa, nie był zwykłym serwerem szkolnym i służył do prowadzenia legalnego przedsięwzięcia gospodarczego.

Wszystko zaczęło się 5 lat wcześniej. Renner, otrzymawszy od jednego z lokalnych biznesmenów dotację w wysokości 50000 dolarów, pomógł w założeniu uczniowskiej firmy prowadzącej działalność dostawcy usług internetowych. Firmę nazwano Outlawnet, Inc. co było nawiązaniem do nieoficjalnej nazwy szkoły, którą w Sisters nazywano Outlaws[1]. Było to niewielkie przedsięwzięcie, które w założeniu miało przynosić zyski pokrywające opłaty za dostęp do Internetu 500 uczniów szkoły. Ale firma się rozrastała i miała już ponad 1000 klientów wśród społeczności lokalnej i w kołach biznesu z Sisters, Black Buttle i Camp Sherman. Grono nauczycielskie wybrało 22 uczniów wykazujących szczególne uzdolnienia komputerowe, którzy prowadzili firmę, tworzyli strony WWW, instalowali oprogramowanie u klientów

[1] Wyjęci spod prawa — *przyp. tłum.*

i zarządzali kontami. Każdego roku zmieniano grupę, dzięki czemu dziesiątki uczniów zdobywało praktyczne doświadczenie przydatne potem w przemyśle komputerowym. Był to powód do dumy.

Ale tego dnia, zaledwie kilka dni po uroczystości wręczenia absolwentom świadectw, duma i nadzieja na przyszłość ustąpiły uczuciu strachu. Już po kilku minutach sprawdzania Renner i pomagający mu kolega przekonali się, że nie była to niegroźna usterka. Tym razem było to coś poważniejszego.

Jakiś haker znalazł wejście do serwera Outlawnetu. Łatwe do odgadnięcia hasło pozwoliło mu na utworzenia konta powłokowego i legalne wejście do sieci. Nikt tego nie zauważył. Nikt się nawet tego nie spodziewał. Outlawnet to nie Yahoo! ani America Online!, lecz mała rybka wśród wielorybów. Był to niewielki dostawca usług internetowych stworzony niewielkim nakładem kapitału i prowadzony przez uzdolnionych uczniów. Jaką korzyść haker mógł odnieść z włamania do takiego serwera?

Odpowiedzi na to pytanie nie trzeba było długo szukać. Główny serwer uniksowy został spustoszony i stał się niedostępny, nawet dla administratorów. Programy narzędziowe do obsługi technicznej zostały skasowane. Przepadło ponad 3000 należących do szkoły plików oraz kilkadziesiąt kont użytkowników. Włamywacz zainstalował program monitorujący ruch w sieci (sniffer), przechwytujący hasła użytkowników i zamieniający szkolny serwer w serwer e-mailowy z wolnym dostępem. Nie upłynęło wiele czasu i posypała się lawina telefonów od klientów zdenerwowanych nagłą blokadą połączeń internetowych. Był to poważny incydent wymagający natychmiastowego zawiadomienia policji.

Sprawa została szybko przekazana do biura FBI w Portland. Reakcja była natychmiastowa i wzbudziła najwyższe uznanie Rennera dla profesjonalizmu działania agentów federalnych przysłanych w celu przeprowadzenia dochodzenia. Outlawnet był niewielkim lokalnym dostawcą usług internetowych, ale skoro zainteresowało się tym FBI, musiało to dotyczyć przestępstwa o znacznie większym znaczeniu i być może międzynarodowych implikacjach. Przeprowadzenie ataku typu „odmowa usługi" było przestępstwem zagrożonym karą więzienia — niezależnie od rozmiaru i ekonomicznego znaczenia zaatakowanego serwera. FBI bardzo poważnie podchodziło do każdego ataku tego rodzaju. Outlawnet nie mógł być wyjątkiem.

14 czerwca agenci federalni poinformowali Rennera o zamiarze otwarciu śledztwa w sprawie ataku na serwer i o usilnych próbach ujęcia hakera lub hakerów odpowiedzialnych za ten atak. Renner obiecał ścisłą współpracę i przyrzekł tropić hakerów za pomocą wszelkich prawnie dozwolonych środków, jakie miał do dyspozycji. Zapowiedział, że jeżeli okaże się, iż włamywacz pochodzi z USA, wystąpi do sądu z żądaniem zadośćuczynienia za poniesione straty. Dostawcy usług internetowych w rodzaju Outlawnetu nie mogli pozwolić, aby tego rodzaju ataki pozostawały bezkarne. Myślał o odzyskania zaufania zarówno klientów, jak i uczniów. Dopiero po miesiącu udało się odtworzyć zniszczone pliki, a pełne trzy miesiące zajęło usuwanie wszystkich uszkodzeń systemu.

Na szczęście Outlawnet posiadał kopię bezpieczeństwa wszystkich zniszczonych plików uczniowskich. Ale atak sporo kosztował. Naprawa oprogramowania i utrata dochodów spowodowana unieruchomieniem serwera kosztowały młodą firmę ponad 11000 dolarów — sumę, za którą można było opłacić dostęp uczniów do Internetu.

Tymczasem śledztwo FBI postępowało naprzód. Badając dzienniki nadzoru (logi) dostarczone przez Rennera, agenci znaleźli podejrzanego na terenie USA. Jednak ta osoba okazała się być właścicielem legalnie działającej firmy, której system został opanowany przez hakera i użyty jako narzędzie ataku na Outlawnet. Tym razem ślad się urwał, ale istniała nadzieja odnalezienia go.

Po udzieleniu agentom FBI odpowiedzi na masę pytań biznesmen dostarczył im systemowe dzienniki nadzoru ze wszystkimi adresami IP (Internet Protocol). Taki adres to ciąg liczb, który w Internecie pełni dla komputera taką rolę jak zwykły adres dla człowieka. W tym przypadku adres IP rzekomo należał do komputera, z którego dokonano infiltracji komputera biznesmena, skąd z kolei dokonano ataku na Outlawnet. Z wolna agenci zaczęli składać łamigłówkę. Choć było możliwe, że hakerzy oszukali kolejny komputer, udając, że działają spod legalnego adresu IP — czyli stosując taktykę zwaną spoofingiem[2] — agenci FBI wiedzieli, że jeżeli będą działać wystarczająco szybko, w końcu powinni znaleźć łącze prowadzące do prawdziwego winowajcy. Kolejny ślad prowadził do Sprint Canada[3].

^()<[]>()*^*

Mark Gosselin już trzy lata pracował w oddziale do badania przestępstw komputerowych Królewskiej Konnej Policji Kanadyjskiej w Montrealu, gdy FBI poinformowało go o prowadzeniu dochodzenia w sprawie przestępstwa popełnionego w USA, którego ślady prowadzą do Kanady. Według FBI, haker zawładnął serwerem dostawcy usług internetowych w Oregonie, łącząc się z nim z Ohio za pomocą szybkiej linii DSL (digital subscriber line[4]), a stamtąd, jak udało się ustalić, ślady prowadziły do Kanady w rejon działania Marka Gosselina. Było to w grudniu 1999 roku.

Na pierwszy rzut oka wszystko wyglądało na sprawę dokładnie rozpracowaną, do szybkiego załatwienia. Gosselin był oficerem śledczym Królewskiej Konnej Policji Kanadyjskiej z 20-letnią praktyką. Cztery lata spędził w SWAT[5], a resztę, służąc w zwykłej policji, śledząc operacje narkotykowe, defraudacje i inne przestępstwa kryminalne. Jeżeli FBI miało dane o koncie, znalezienie śladu prowadzącego do źródła było jedynie kwestią czasu. Wtedy wyśle chłopaków, żeby aresztowali rzezimieszka. Tak mu się wtedy zdawało.

Gosselin wiedział, że gdziekolwiek ślad miał go zaprowadzić, ma w ręku niezłą sprawę. W przypadku przestępstw komputerowych prawo kanadyjskie jest równie surowe jak w USA. Nawet debiutanci za nieuprawnione wejście do systemu mogą wylądować w więzieniu na 10 lat. Ponadto zniszczenie lub zmiana danych, znana w prawie kanadyjskim jako „mischief to data" oraz zdobycie haseł w celu nielegalnego dostępu do komputera są również zagrożone wyrokiem 10 lat więzienia.

---

[2] *To spoof* — naciągać, blagować, podszywać się — *przyp. tłum.*

[3] Wielka firma telekomunikacyjna w Kanadzie — *przyp. tłum.*

[4] Od 1 lipca 2002 tę usługę oferuje również TPSA. Informacje finansowe i techniczne można znaleźć na stronie *http://www.tpsa.pl/biznes/msp/dsl/ — przyp. tłum.*

[5] *Pecial Weapon and Tactics* (specjalna broń i taktyka) — oddziały przeznaczone do wykonywania szczególnie trudnych i niebezpiecznych zadań — *przyp. tłum.*

Pierwszym krokiem Gosselina było uzyskanie nakazu rewizji w Sprint Canada. Dzięki pomocy Sprinta udało mu się znaleźć kilka aliasów e-mailowych przypisanych do konta w Delphi Supernet — małego dostawcy usług internetowych w Montrealu. Ale konto zostało zamknięte przed rokiem z powodu podejrzenia o działania hakerskie niezgodne z zasadami bezpieczeństwa przestrzeganymi przez firmę. Rzecz stawała się interesująca. Gosselin postąpił o krok do przodu, ale daleko było jeszcze do znalezienia „dymiącego pistoletu" będącego dowodem przestępstwa. Nawet mając informacje o koncie, nie mógł stwierdzić, kto siedział przed komputerem, dokonując ataku na Outlawnet. Śpiesząc się, mógł zniszczyć dowody potrzebne do późniejszego wytoczenia procesu przeciw hakerowi, którym — jak wyczuwał na podstawie swego wieloletniego doświadczenia — był nastolatek. Ale musiał wiedzieć na pewno. W Montrealu i okolicy było zapewne kilkadziesiąt tysięcy nastolatków, którzy mogli posiadać umiejętności pozwalające na dokonanie takiego ataku. Nie był to rodzaj przestępstwa, gdzie możliwe jest zidentyfikowanie winnego przez konfrontację ofiary z grupą podejrzanych. A dowody były bardzo „cienkie". Na razie nie miał dowodu pozwalającego uzyskać to, co było naprawdę potrzebne, czyli prawo podsłuchu połączeń.

Zawęził poszukiwania źródła ataku do dwupiętrowego budynku na Rue de Golf Street w West Island — zamożnej dzielnicy Montrealu leżącej jedynie 30 mil od granicy ze Stanami Zjednoczonymi. Teren przylegał do modnego i ekskluzywnego pola golfowego St. Raphael położonego między malowniczym jeziorem Lake of Two Mountains i potężną rzeką Św. Wawrzyńca. Zdaniem większości ludzi, była to wymarzona siedziba w ekskluzywnym otoczeniu, w pełni wyposażona, z dwoma garażami, brukowanym boiskiem do koszykówki, gdzie dzieci mogły się bawić. Do najbliższej szkoły średniej było stąd 12 minut jazdy samochodem.

Większość mieszkańców tego domu niczym się nie różniła od sąsiadów z okolicy — poza kilkoma wyjątkami. Właściciel John Calce — prezes zarządu firmy transportowej, powtórnie żonaty — zgodnie z opinią sąsiadów, był szorstkim, aroganckim, nieokrzesanym i wrzaskliwym facetem, który lubił przesiadywać przed domem w sportowej koszulce i szortach, wrzeszcząc i klnąc przez telefon komórkowy. Nie interesował się zbytnio swymi trzema synami, z których dwaj byli braćmi, a trzeci bratem przyrodnim z drugiego małżeństwa. Najstarszy, 17-letni, chciał zostać aktorem i rzeczywiście udało mu się załatwić udział programie rozrywkowym pokazywanym w lokalnej telewizji. Niewiele wiedziano o przyrodnim bracie. Był najmłodszy i lubił grać w koszykówkę. Gdy nie było go na boisku przy domu, kibicował drużynie nastolatków Brookwood Jazz. Gdy nie miał ochoty na grę w koszykówkę, czasem pomagał sąsiadom i przyjaciołom myć samochody. W opinii większości tych, którzy go znali, nie było w nim nic szczególnego. Był normalnym dzieckiem.

Ale młody miłośnik koszykówki był także miłośnikiem komputerów. Miał tylko 12 lat, gdy Delphi Supernet z powodu podejrzenia o hakerstwo zamknęło dwa konta używane przez mieszkańców budynku przy Rue de Golf Street. Goselin mógł później podejrzewać, ale nigdy nie był w stanie udowodnić, że chłopak nauczył się podstaw hakerstwa od jednego ze swych starszych braci. Dzieciak zapewne niezbyt dokładnie zdawał sobie sprawę z tego, co robi jego starszy brat, ale czuł w głębi serca, że chciałby robić to samo — włamywać się do innych komputerów. Do dziś nie udało się ustalić, kto odpowiadał za incydenty, które doprowadziły do skasowana kont w Delphi Supernet. Jedyna rzecz, której Gosselin mógł być pewny, to fakt, że ten dom miał coś wspólnego z hakerstwem.

Nikt nie mógł przewidzieć, że niewielki, ciemnowłosy, 14-letni chłopak, który lubił koszykówkę i dziewczyny, miał wkrótce ściągnąć na siebie uwagę całego świata internetowego, a nawet sfer rządowych Stanów Zjednoczonych. Gosselin nie mógł wiedzieć, że telefon z FBI w sprawie hakerskiego incydentu ze stosunkowo nieznanym dostawcą usług internetowych w stanie Oregon był początkiem tego, co potem zostało nazwane Operacją Claymore. W świecie operacja ta znana była jako polowanie na Mafiaboya, najbardziej notorycznego nastoletniego hakera od czasów Kevina Mitnicka.

^()<[]>()*^*

Dokładnie miesiąc przed atakiem na Outlawnet oficer CIA uporczywie usiłował ostrzec dowództwo wywiadu w Europie, że jugosłowiańskie oddziały pomocnicze mieszczą się o jeden blok dalej od miejsca, w którym piloci NATO mieli zrzucić bomby. Ani piloci, ani planiści podający współrzędne bombardowania nie wiedzieli, że oddziały te, służące Serbom pomocą w brutalnej kampanii tortur i mordowania niewinnych Albańczyków, zostały przed paroma laty przemieszczone do innego budynku. Ale zanim CIA przetrawiło informacje przekazane przez swego oficera i przekazało je dowódcom w Europie, samoloty Zjednoczonych Sił NATO były już w drodze do celu. Gdy następnego dnia rano wiatr rozwiał dymy, szefowie NATO musieli pogodzić się z kompromitującym faktem, że zbombardowano część ambasady Republiki Chin, zabijając trzy osoby i raniąc wiele innych.

Tego dnia w cyberprzestrzeni rozpoczęła się wojna przeciw NATO i rządowi Stanów Zjednoczonych. Był to również początek największej w USA akcji służb specjalnych mającej na celu spenetrowania hakerskiej społeczności.

Bombardowanie oddziałów serbskich w Kosowie oraz zaatakowanie ambasady chińskiej zjednoczyły hakerów na całym świecie przeciw kierowanej przez USA koalicji NATO. Początkowo serbscy hakerzy prowadzili defensywno-informacyjną kampanię, której celem było zwalczanie amerykańskiej dominacji w środkach masowego przekazu; teraz przybrała ona charakter ofensywny, a celem ataków stały się strony WWW rządu USA i NATO. Chodziło o wykorzystanie umiejętności hakerów sympatyzujących z Serbami do sparaliżowania natowskich możliwości informowania świata o wojnie za pomocą Internetu, który w coraz większym stopniu stawał się źródłem informacji dla milionów ludzi.

Hakerzy z USA, Serbii, Chin i Rosji, sympatyzujący z Serbami lub czynnie wspierający ich działania w Kosowie, rozpoczęli atakowanie serwerów internetowych dowództwa NATO w Brukseli metodą ping-of-death[6]. „Ping" to słowo powstałe z pierwszych liter Packet InterNet Groper, jest to narzędzie służące do sprawdzania, czy interesujący nas system jest obecny w sieci i działa prawidłowo. Gdy użytkownik sieci „pinguje" serwer, wysyła do niego pakiet testowy i oczekuje na odpowiedź. To coś takiego, jak telefonowanie do kogoś, żeby sprawdzić, czy jest w domu i czy odpowie. Gdy do sprawdzanego serwera wyślemy w krótkim czasie zbyt wiele pakietów testowych, zostanie przekroczona jego zdolność odpowiadania, co

[6] *Ping-of-death* (ping śmierci) — ogólne wyjaśnienie tej metody ataku zostało podane w następnych zdaniach — *przyp. tłum.*

zablokuje także możliwość ściągania informacji przez legalnych użytkowników. Właśnie to się stało z serwerem NATO. Przez kilka dni sojusz nie mógł wysyłać w świat informacji o tym, co się dzieje w Kosowie.

W tym czasie Bill Swallow, doświadczony oficer śledczy Sił Powietrznych Stanów Zjednoczonych ze specjalnego oddziału dochodzeniowego, przydzielony do sformowanej przez FBI w Los Angeles grupy zajmującej się włamaniami komputerowymi, zdołał pozyskać informatora tkwiącego głęboko w społeczności serbskich hakerów. Miało się potem okazać, że był to jeden z najważniejszych kontaktów, które udało mu się nawiązać w jego zawodowej karierze.

W miarę eskalacji walk w Kosowie nasilały się ataki na system informatyczny NATO, a zwłaszcza rządu Stanów Zjednoczonych. Departament Bezpieczeństwa Narodowego poinformował FBI o kilku nieudanych próbach naruszenia systemu zabezpieczeń sieci Białego Domu i Pentagonu. Z posiadanych dowodów wynikało jasno, że ataki były dokonywane za pomocą łączy zamorskich, co wskazywało na związek z wydarzeniami na froncie serbskim.

Kwatera główna FBI w Waszyngtonie telefonicznie powiadomiła swoje oddziały w całym kraju, że sprawa ataków hakerskich na serwery rządowe ma najwyższy priorytet. Jak się potem okazało, ogromne znaczenie miał telefon do szefa FBI w Los Angeles, Charlesa Neala, który przed laty zajmował się dobrze znaną sprawą hakera Kevina Mitnicka. Był on jednym z najbardziej doświadczonych policjantów zajmujących się sprawami przestępstw komputerowych, który pomógł w tworzeniu wielu stosowanych przez FBI technik śledzenia tego rodzaju przestępstw. Przed wstąpieniem do FBI wykładał nauki komputerowe na wyższej uczelni i zajmował się sprawami bezpieczeństwa komputerowego w firmach z branży bankowości i służby zdrowia. Znał się na swojej robocie.

Wkrótce po telefonie z Waszyngtonu wezwał on do swego biura Swallowa i spytał, na ile wiarygodne są informacje pochodzące od jego serbskiego informatora. Okazało się, że w rzeczywistości pochodzą one z dwóch źródeł. Jednym był haker mieszkający w USA i mający ścisłe związki z serbskim podziemiem hakerskim oraz rodzinę w Serbii. Drugim źródłem był przebywający w Kosowie dawny bohater wojenny zajmujący się w serbskiej armii antynatowską kampanią informacyjną. Neal zorientował się od razu, że jeżeli te osoby są tymi, za które się podają, oddział FBI w Los Angeles będzie miał najlepszy w Stanach wywiad hakerski.

W roku 1999 tylko kilku agentów FBI mogło w dziedzinie przestępstw komputerowych równać się wiedzą, zdolnościami i doświadczeniem z Jill Knesek. Przydzielona w roku 1998 jako oficer śledczy do biura w Los Angeles, Jill była tą, która przekopała się przez góry dowodów sądowych zebranych przeciw Kevinowi Mitnickowi. To dzięki niej udało się uporządkować te dane w sposób pozwalający na wysłane notorycznego cyberprzestępcy do więzienia federalnego. Knesek wniosła do FBI 10-letnie doświadczenie w pracy nad bezpieczeństwem komputerowym. Między innymi na stanowisku specjalisty komputerowego w Naval Satellite Operations Center[7], gdzie była programistką odpowiedzialną za utrzymanie sprawności

[7] Centrum operacji satelitarnych marynarki wojennej — *przyp. tłum.*

15 satelitów nawigacyjnych. Znała się na wielu typach komputerów i systemów operacyjnych. Pisanie i odkodowywanie skryptów hakerskich było dla niej równe proste jak składanie podpisu na papierze.

Zaangażowanie Swallowa do pracy grupy pociągało za sobą konieczność współdziałania z Knesek. Należało sprawdzić hakerski kontakt w USA — Swallow był prawie nowicjuszem w tej dziedzinie, zaś Knesek dysponowała wszystkimi potrzebnymi umiejętnościami technicznymi. Sprawa była zbyt ważna, aby rościć sobie pretensje do samodzielnego jej rozwiązania. Ani dla niej, ani dla niego nie stanowiło to żadnego problemu. Oboje byli profesjonalistami najwyższej klasy, którzy równie mocno wierzyli w konieczność obrony Internetu przed wandalami i kryminalistami, jak hakerzy w przyrodzoną wolność informacji i prawo do swobodnej penetracji sieci.

Swallow i Knesek spotkali się z amerykańskim hakerem, którego tożsamość została utajniona. Zaczął on natychmiast dostarczać FBI informacje o hakerach rozsianych po całym świecie, również w USA. Przez tego pośrednika nawiązali kontakt z hakerem z Serbii. Do Swallowa i Knesek, a także do kwatery głównej FBI w Waszyngtonie zaczęły płynąć informacje z frontu w Kosowie. Docierały bardzo skomplikowaną drogą okrężną, która mogła być w każdej chwili odcięta z powodu hakerskiej ostrożności i braku zaufania. Trudno też było zweryfikować prawdziwość danych przysyłanych przez hakera z Kosowa. W sieci rzadko się zdarza, by dana osoba rzeczywiście była tym, za kogo się podaje.

Dzięki serii bombardowań Knesek mogła zlokalizować wtyczkę w Kosowie. Sprawdzając czas wysłania informacji i porównując go z danymi o bombardowaniach z kwatery głównej FBI, była w stanie dokładnie wskazać pozycję hakera. FBI wciąż mogło otrzymywać informacje szybciej niż media, nawet szybciej niż CNN, więc gdy informator przekazywał wiadomość, że bomby spadły blisko niego, Knesek i Swallow porównywali te dane z danymi Pentagonu i Departamentu Sprawiedliwości. Haker potrafił przekazywać informacje o bombardowaniach, o których media jeszcze nie wiedziały. Knesek stwierdziła, że znaleźli kontakt w odpowiednim miejscu i czasie oraz — co jeszcze ważniejsze — źródło prawdziwych informacji.

^()<[]>()*^*

Wojna powietrzna prowadzona przez Stany Zjednoczone w Kosowie trwała 78 dni. W tym czasie FBI wykryło jeszcze jednego hakera, który, zagrożony postawieniem przed sądem, zgodził się na współpracę i stał się źródłem informacji o istotnym znaczeniu. Dane personalne hakerów od początku związanych z tą sprawą są nadal tajne, gdyż śledztwo i procesy jeszcze trwają.

Operacja zakończyła się wielkim sukcesem. Nigdy wcześniej nie dokonano czegoś takiego, przynajmniej w śledztwach dotyczących cyberprzestrzeni. Oczywiście, FBI miało wieloletnie doświadczenie w infiltracji takich grup przestępczych jak mafia, kartele narkotykowe i różne frakcje obrońców supremacji białej rasy, ale nigdy nie próbowało przeniknąć do subkultury stworzonej przez tak bezimienne indywidua, dla których kłamstwo i fałsz były nie tylko narzędziem samoobrony, lecz po prostu sposobem życia. Podziemie hakerskie w niczym nie przypominało żadnej organizacji,

z jaką FBI przyszło się zmierzyć kiedykolwiek w przeszłości. Nawet grupy przestępczości zorganizowanej łatwiej było przeniknąć i zdezintegrować, podburzając ich członków przeciw sobie. Hakerzy zaś tworzą zwartą społeczność — niezależnie od stopnia umiejętności i doświadczenia — i nie zrażają się pierwszymi trudnościami. Zamiast rezygnować przybierają inną tożsamość i stosują inne manewry zwodzące, co znacznie utrudnia ich identyfikację w sieci. Niełatwo jest wejść do tego świata i czasem przez całe miesiące trzeba się uwiarygodniać, zanim uzyska się pełną akceptację.

A jednak FBI przeprowadzało w przeszłości podobne operacje. Znana była sprawa przeniknięcia do grup lokalnych organizacji hakerskiej 2600, infiltracja zebrań lokalnych grup i dorocznej konferencji DefCon w Las Vegas. Odnoszono sukcesy, ale nieliczne. Agenci FBI i inni przedstawiciele władz pozostawali na zewnątrz, jak lisy węszące wokół zamkniętego kurnika. Co roku organizatorzy konferencji DefCon ogłaszali konkurs „łap glinę". Zadanie było proste: „Jeżeli zobaczysz jakiegoś MIB-a[8] (Men in Black) ze słuchawkami, w czarnych półbutach i ciemnych okularach, czającego się na wzór Clinta Eastwooda w „Żyć i umrzeć w Los Angeles[9]", wskaż go, a dostaniesz koszulkę z napisem „Nakryłem glinę"".

Wykrywanie agentów federalnych na konferencji DefCon było tak łatwe, że stało się zabawą. Agentom FBI znacznie trudniej przychodziło śledzenie i identyfikowanie hakerów z wyraźnie przestępczymi inklinacjami. Często było to niewykonalne i przypominało szukanie igły w stogu siana. Efektywna infiltracja podziemia w sieci wymagała bardzo aktywnego działania. Przesiadywanie na kanale IRC-a #dc-stuff (DefCon Stuff) i czytanie zwierzeń niewydarzonych ekshakerów dyskutujących o tym, co wypili i jak się spili, jeszcze z nikogo nie zrobiło hakera. Również dyskutowanie o hakerstwie w nic nie da. Trzeba się za to zabrać samemu.

Pod koniec roku 1999 tajna operacja Kosowo zbliżała się ku końcowi. Zmniejszyła się liczba ataków internetowych na serwery NATO i rządu Stanów Zjednoczonych. Ale przez sześć miesięcy tajnego działania Swallow, Knesek i około stu agentów FBI rozsianych po całym kraju zebrało wraz z lokalnymi siłami porządkowymi i wojskowymi masę informacji o dziesiątkach hakerów zamieszanych w działania kryminalne. Jak wspomina Swallow: „Przekonaliśmy się, że w zasadzie udała nam się infiltracja hakerskiego podziemia". Rzeczywiście się udała, a Neal był wytrawnym agentem, który rozumiał wartość wywiadu. Bez wahania złożył FBI i Departamentowi Sprawiedliwości propozycję kontynuowania działań. Otrzymanie zgody nie było trudne, gdyż w Departamencie Sprawiedliwości nikt się temu nie sprzeciwiał. Tak się narodziła pierwsza tajna operacja penetracji podziemia hakerskiego, objęta taką tajemnicą, że do dzisiaj nie ujawniono, jaką nazwą została określona.

Zarówno Gosselin w Kanadzie, jak i pracownicy biura FBI w Los Angeles nawet się nie spodziewali, co ich czeka w najbliższej przyszłości i jak ważna okaże się ich

[8] *MIB* (*Men in Black* — ludzie w czerni) — osobnicy ubrani w czarne garnitury, w czarnych butach i z czarnymi krawatami, jeżdżący czarnymi cadillacami lub latający czarnym helikopterem. Odwiedzają ponoć ludzi, którzy widzieli UFO i straszą ich śmiercią w razie ujawnienia wiadomości na ten temat. Niektórzy uznają ich za agentów rządowych, inni za… tu możliwości jest wiele, więc ciekawych odsyłam do Internetu. Stali się bohaterami filmów i gier komputerowych — *przyp. tłum.*

[9] „*To live and die in Los Angeles*" — *przyp. tłum.*

działalność. Pozyskani informatorzy i nabyte umiejętności stały się kluczowym narzędziem w walce z nastoletnim hakerem, który wkrótce miał rozłożyć na łopatki wielkie firmy internetowe.

^()<[]>()*^*

Operacja nabrała tempa w styczniu roku 2000. Swallow przeszedł ze stanowiska kierowniczego do tajnej grupy agentów udających nieletnich hakerów. Knesek pomagała mu koordynować ogólnokrajową obławę, pilnując, aby wszystko przebiegało legalnie. To właśnie stanowiło największą trudność i wielkie wyzwanie.

Swallow, mężczyzna po czterdziestce, nigdy nie spotkał się twarzą w twarz z żadnym hakerem, czyli obiektem swego polowania. Nigdy nie przyszło mu do głowy, że ktoś w jego wieku może zostać hakerem. Ale musiał w środowisku hakerskim „złożyć listy uwierzytelniające" i zdobyć reputację. Bez tego niemożliwe było zdobycie informacji wystarczających do postawienia kogoś przed sądem. Oznaczało to, że on i inni agenci z grupy muszą rzeczywiście złamać zabezpieczenia jakichś stron WWW i zniszczyć je. To tak samo jak w sytuacji, gdy szef mafii, przyjmując do „rodziny" nowego członka, wręcza mu pistolet i każe usunąć szefa konkurencyjnego gangu. Tyle tylko, że w tym przypadku tolerancja FBI dla tego, co można zrobić w celu potwierdzenia fałszywej tożsamości agenta, była znacznie większa. Tak czy inaczej, hakerstwo nie było przestępstwem szczególnie drastycznym, to nie to samo co morderstwo. Strony WWW nie krwawiły.

Sporym problemem była współpraca z biurami prokuratorów okręgowych. Każdy federalny oskarżyciel, nawet niewiele wiedzący o przestępstwach komputerowych i o subkulturze hakerskiej, chciał sobie dodać splendoru kosztem tej operacji. Ale Departament Sprawiedliwości wymagał udziału w specjalnych kursach, dając do zrozumienia, że nie zamierza tracić czasu, gdy przyjdzie do postawienia hakerów przed sądem. W rzeczywistości, zgodnie z opinią agentów działających w terenie, spowodowało to wielkie zamieszanie i wzajemną rywalizację, która paraliżowała śledztwo. Lokalni prokuratorzy bali się podjąć jakąkolwiek decyzję bez wcześniejszej aprobaty z góry.

Pomimo politycznej rywalizacji Waszyngtonu i biur prokuratorów okręgowych Neal i jego grupa uzyskali zgodę Departamentu Sprawiedliwości na zniszczenie różnych rządowych stron WWW w celu wsparcia agentów usiłujących zinfiltrować świat podziemia hakerskiego. Dla agentów działających w sieci uzyskanie tej zgody stało się sprawą szczególnie ważną. Był na to najwyższy czas. „Musieliśmy się dobrać do jakiejś strony, aby nie stracić wiarygodności" — wspomina Neal. „Nie różniło się to od zdobywania zaufania gangu, czy mafii, bowiem lepsi hakerzy tworzą własne pokoje czatowe, do których trzeba być zaproszonym.

Grupa w końcu zniszczyła około tuzina rządowych stron w sieci, aby się godnie zaprezentować w podziemiu. Przekonali nawet kilka prywatnych firm do wyrażenia zgody na uszkodzenie ich stron. Swallow i inni tajni agenci posłali kopie swoich hakerskich wyczynów do administratorów strony Attrition.org[10], sieciowego archiwum

[10] *Attrition* — tarcie, ścieranie, skrucha i wojna na wyczerpanie — wybór pozostawiam domyślności Czytelników — *przyp. tłum.*

służącego hakerom do gromadzenia efektów destrukcyjnych działań. Attrition dla nastoletnich twórców skryptów jest ulubionym forum prezentacji osiągnięć i powodem hakerskiej chwały, że właśnie oni zniszczyli największą liczbę stron internetowych. Attrition nie troszczy się o to, kim są niszczyciele stron i dba jedynie o to, by przesyłane rezultaty włamań pochodziły z legalnych stron internetowych, a nie z założonych specjalnie w celu dokonania włamania, co również się zdarzało.

Wszystko przebiegało gładko dzięki pomocy dwóch hakerów współpracujących przed paroma miesiącami ze Swallowem i Knesek nad sprawą dotyczącą Kosowa. W miarę upływu czasu przybywało hakerskich wybryków, ale spora ich część była dziełem niedoświadczonych nastolatków, którzy dali się zwabić atmosferą hakerskiego podziemia. Inni nie byli tak naiwni, ale wyłapywanie ich i tak nie stanowiło trudności dla informatorów FBI. Prawdziwi kryminaliści potrzebują zwykle dużo czasu, by uwierzyć, ze zostali przyparci do muru, natomiast hakerzy, zwłaszcza nastoletni, w przypadku wpadki nie są tak odporni na stres. Nie trzeba ich wykańczać nerwowo trzydziestoma telefonami w ciągu dnia, ani znienacka żądać spotkania w kafejce i zmuszać do przypominania sobie, co robili minuta po minucie. Tego rodzaju taktyka przydaje się, gdy ma się do czynienia z dealerami narkotyków lub innego rodzaju zatwardziałymi przestępcami.

Hakerzy, gdy zrozumieją, że zostali przyparci do muru, szybko stają się szkoleniowcami i konsultantami FBI. Oni nauczyli Swallowa poruszania się w różnych pokojach czatowych i podpowiedzieli, jak odpowiadać na pytania i wyzwania innych hakerów. Nie ma wątpliwości, że najlepszym źródłem informacji o hakerze jest inny haker. Są oni zaufanymi członkami podziemnej społeczności, w której świat wirtualny zastępuje świat rzeczywisty i gdzie ludzie, którzy wyrażają się jak agenci, są traktowani jak agenci.

Podczas jednej z nocnych zmian, które trwały często od 10 do 12 godzin, ze Swallowem nawiązał kontakt haker, który pochwalił się kradzieżą numerów 400 kart kredytowych i ukryciem ich na jednym z serwerów niemieckich. Aby to udowodnić, pokazał skrawek skradzionych danych, po czym stwierdził „Jeżeli ci to do czegoś potrzebne, to je sobie stamtąd ściągnij". Nie robił wrażenia kogoś, kto chce się przysłużyć, ani takiego, co pragnie pochwalić się zdobyczą. To było wyzwanie. Wyzwanie i sprawdzian, kim Swallow jest naprawdę, a zwłaszcza, czy nie jest gliną.

Swallow dwoił się i troił, by odkryć tożsamość hakera. Złodziej kart kredytowych na pewno był grubą rybą, prawdziwym kryminalistą. Numery kart były równie cenne jak gotówka. Jedna wpadka z kartą kredytową mogła zrujnować całą firmę. Zwykle po takim incydencie klienci odchodzą i nigdy nie wracają, zwłaszcza ci, których dane skradziono. W przypadku kart z kredytem do 5000, 10000 dolarów lub jeszcze wyższym taka kradzież mogła sięgnąć kwoty 4 milionów dolarów. Swallow miał ochotę przygwoździć drania.

Nie był to pierwszy przypadek, gdy Neal musiał nakazać w grupie posłuszeństwo. „Musiałem mu zabronić posunąć się dalej" — wspomina. „Nasze śledztwo wkracza na terytorium innego państwa, byłoby to pogwałceniem zawartych traktatów i mógłbyś spowodować międzynarodowy incydent". Chociaż nie było wytycznych, jak dalej postępować, Neal wolał być przesadnie ostrożny. Jego agenci, postępując naprzód, określali zasady, wkraczali na dziewiczy teren. Swallow był profesjonalistą i wiedział, że w przypadku danych kart kredytowych zapisanych na zagranicznym serwerze oczekiwanie na zgodę zwierzchników jest zwykłą stratą czasu.

W sytuacjach takich jak ta umiejętność zatrzymania się we właściwym miejscu była sprawą zasadniczą, przynajmniej z formalnego punktu widzenia. W końcu Swallow zdobył sobie zaufanie młodocianych członków hakerskiego podziemia, którzy w trudnych przypadkach zwracali się do niego o pomoc w przeprowadzeniu hakerskiego ataku. Jednak to zadanie było dla niego i innych niemożliwe do wykonania lub raczej — prawie niemożliwe, gdyż wymagało zezwolenia biura prokuratora. Knesek wspomina: „Chcieliśmy prowokację pchnąć o krok dalej, ale nie mogliśmy sobie pozwolić na zrobienie czegoś, co mogłoby spowodować wstrzymanie całej operacji". Często zdarzało im się wstrzymanie działań do czasu otrzymania odpowiedzi. Zawsze przecież mógł im się „nagle" załamać system operacyjny, albo musieli wyjść do ubikacji, albo ktoś mógł się pojawić w drzwiach i zostać na całonocną pogawędkę. Używali różnych wymówek, aby zyskać czas potrzebny do uzyskania zgody na atak.

Ale było mnóstwo przypadków, gdy żadna zgoda nie była potrzebna. Podczas trwania operacji Neal i jego grupa znaleźli w sieci tysiące stron, których zabezpieczenia zostały złamane. Organizacje rządowe i korporacje posiadające dane o dużym znaczeniu dla bezpieczeństwa państwa lub systemu gospodarczego były tak szybko, jak to możliwe, informowane o lukach w systemie zabezpieczeń. Ale grupa Neala nie miała ani czasu, ani możliwości, by wszystkie poszkodowane firmy informować o włamaniach. Musiałby posadzić przy telefonach wszystkich swoich agentów i nakazać wydzwanianie po kolei do tysięcy firm, które nie miały pojęcia o włamaniach do swoich systemów. Takie działanie rychło doprowadziłoby do zakończenia całej operacji. „Podjąłem decyzję o nieinformowaniu o włamaniach do wszystkich kwiaciarni itp. i ograniczeniu się do zawiadamiania jedynie ważnych instytucji rządowych" — wspomina Neal.

Innym ważnym zadaniem wykonywanym podczas tej operacji było ustalanie fizycznych miejsc pobytu poszczególnych hakerów. Komputerowi przestępcy rzadko podają o sobie jakiekolwiek dodatkowe informacje. Są to hakerzy dbający o własne bezpieczeństwo, a nie o reklamę. Myślą jak kryminaliści i wielu z nich zdaje sobie sprawę z finansowych implikacji ich umiejętności. Niektórzy dają wskazówki początkującym nieletnim hakerom, po czym niezauważalne w ślad za nimi wchodzą do systemów. Neal przekonał się, że większość z nich jest zatrudniona na dobrze płatnych stanowiskach w firmach zajmujących się sprawami bezpieczeństwa sieci i bierze aktywny udział w tworzeniu 0-Day-Exploits[11]: szkodliwych programów, których używanie zmusza firmy w całym kraju do wykonywania ekspertyz i szukania technicznej pomocy w wyszukiwaniu wad systemów. O dziwo, firmy zatrudniające tych hakerów zwykle pierwsze przygotowują poprawki systemów i programy ratownicze oraz przeprowadzają analizę poszczególnych przypadków.

Ale w IRC-u, gdzie Swallow występował często jako operator kanału, dominują nastoletni twórcy skryptów, tzw. skrypciarze. Będąc operatorem, Swallow decydował, kto może pozostać w kanale, a kogo należy wyłączyć. Na pierwszy ogień szli krzykacze i pozerzy. Nie można było prowadzić poważnej dyskusji o hakerskiej taktyce i narzędziach z bandą szczeniaków wtrącających wciąż uwagi nie na temat, a do tego

[11] *Exploit* — tu: technika włamania lub narzędzie temu służące, wykorzystujące słabości konkretnego systemu operacyjnego. Znaczenie tego słowa nie jest jeszcze ustabilizowane i bywa różnie interpretowane przez środowiska informatyczne — *przyp. tłum.*

pełne przechwałek i wulgaryzmów. Jednak to właśnie oni najczęściej byli naiwniakami, którzy podawali informacje pozwalające agentom FBI na zlokalizowanie. Byli jak bolący wrzód na tyłku zarówno dla FBI, jak i dla prawdziwych hakerów.

A na Swallowa czekał jeszcze jeden wrzód, większy od wszystkich, które kiedykolwiek dotknęły Internet.

^()<[]>()*^*

Pierwszy atak rozpoczął się w poniedziałek rano. Zdarzyło się to 7 lutego 2000 roku. Yahoo! — jeden z największych portali informacyjnych i biznesowych — został całkowicie zaskoczony atakiem. Strumień pakietów danych spadł na jeden z głównych routerów[12] Yahoo! z szybkością 1 gigabajta na sekundę, co odpowiada ponad 3,5 mln średniej wielkości maili na minutę. Router wytrzymał atak, ale Yahoo! straciło połączenie z jednym z głównych dostawców usług internetowych. Już wcześniej były z nim pewne problemy i pierwszą godzinę administratorzy spędzili na usuwaniu znanych usterek. Nikt nie przypuszczał, że Yahoo! właśnie w szybkim tempie stawał się pierwszą ofiarą największego w historii ataku typu denial-of-service[13].

W końcu administratorzy zostali zmuszeni do zablokowania całego ruchu wpływającego od dostawcy usług internetowych. Pozwoliło to na ponowne uruchomienie podstawowego routingu sieciowego, ale nadal nie było jasne, co się właściwie stało. Administratorzy Yahoo! mogli jedynie stwierdzić, że system załamał się w wyniku przeciążenia nadmiernym ruchem pakietów ICMP[14] (Internet Control Message Protocol). Sieci komputerowe używają komunikatów ICMP do wykrywania przyczyn problemów, na przykład w sytuacji, gdy router nie może transmitować pakietów równie szybko, jak je otrzymuje. Komunikaty te są automatycznie wymieniane między systemami. I wówczas administratorzy Yahoo! zrozumieli, że kłopoty, które dotknęły ich sieć, nie są wynikiem przypadkowej usterki. Był to przemyślany atak.

Natychmiast rozpoczęli filtrowanie wszystkich komunikatów ICMP, lecz wówczas cały zablokowany ruch zaczął zalewać serwery Yahoo!. Jeden z głównych dostawców usług internetowych przechwycił część danych i technicy stwierdzili, że bezpośrednie łącza do dostawców usług, w tym do głównego dostawcy krajowego, z którym współużytkowano dane, nieświadomie biorą udział w ataku. Znaleźli ślad, który doprowadził do jednego z własnych komputerów Yahoo!; jedne systemy Yahoo! atakowały inne systemy własnej sieci. Był to szeroko zakrojony atak, w którym wiele komputerów posłużyło jako zombi[15]. Według ekspertów broniących Yahoo!, tego rodzaju skomplikowany atak musiał był dziełem najwyższej klasy hakera lub grupy hakerów. Kto inny mógłby przeprowadzić tak zmasowany atak typu odmowy usług?

[12] Urządzenie, które po otrzymaniu przesyłanego pakietu odczytuje jego nagłówek i ustala najlepszą trasę transmisji. Jest również odpowiedzialne za podział pakietu na fragmenty, jeżeli tego wymagają parametry transmitującej sieci — *przyp. tłum.*

[13] Odmowa usługi — patrz przypis we Wstępie — *przyp. tłum.*

[14] Internetowy protokół komunikatów kontrolnych — *przyp. tłum.*

[15] Komputer opanowany przez hakera w celu przeprowadzenia ataku, np. typu *denial-of-service*. Legalny właściciel komputera może nie zdawać sobie sprawy z jego działania jako zombi — *przyp. tłum.*

„Wyglądało na to, że haker (lub hakerzy) znał topologię naszej sieci i wszystko zaplanował z wyprzedzeniem" — napisał administrator Yahoo! w kilka dni po napływie pierwszej fali blokujących pakietów. „Wydaje się, że był to zdecydowanie atak typu DDoS[16], w którym wiedza i umiejętności atakującego znacznie przewyższały poziom przeciętnego hakera. Atakujący musiał doskonale znać zarówno Unix, jak i technologię oraz organizację sieci".

Była to szczegółowa analiza dokonana przez pierwszą, jak się potem okazało, z szeregu atakowanych firm. Było jasne, że Yahoo! dotknął atak wytrawnego hakera, który wiedział, co robi i poświęcił wiele czasu na poznanie celu ataku. To, czego świadkami byli administratorzy Yahoo!, z całą pewnością nie było dziełem dzieciaka, który ściągnął z Internetu parę skryptów hakerskich do ataku typu DDoS i chciał się przekonać, jak działają. Był to atak przeprowadzony przez profesjonalistę, który prawdopodobnie korzystał z dodatkowej pomocy. Przynajmniej tego administratorzy Yahoo! byli pewni. Dane, którymi zaatakowano Yahoo!, wydrukowane na papierze, wypełniłyby 630 półciężarówek.

Późną nocą Swallow nalał sobie filiżankę kawy i zasiadł przed komputerem, przygotowując się do kolejnej długiej nocy wypełnionej w większości nieistotnymi czatami z nic nieznaczącymi nastoletnimi hakerami. Nocne dyżury wydłużały się, żaden z rzeczywistych hakerów nie wyściubił wirtualnego nosa przed nastaniem wczesnych godzin porannych. Ale tej nocy Swallow, działając jako administrator jednego z odwiedzanych przez hakerów kanałów IRC-a, zauważył, że pojawił się nowy uczestnik o pseudonimie Mafiaboy. Zauważył go już wcześniej, a przynajmniej kogoś, kto używał tego pseudonimu (nie było sposobu, by się przekonać, czy to ta sama osoba). Ale wszelkie wątpliwości dotyczące tożsamości Mafiaboya wkrótce się rozwiały. Chłopak idealnie pasował do znanych już cech osobowości. Był tym samym hałaśliwym, piszącym skrypty nastolatkiem, z którym Swallow i inni już poprzednio wymienili parę zdań.

Tej nocy Mafiaboy przechwalał się swoimi umiejętnościami. Inni hakerzy na IRC-u wkrótce znudzili się tymi przechwałkami. Czat rychło zamienił się w wymianę wyzwisk i przekleństw. Przeklinanie było jedną z pokazowych umiejętności Mafiaboya, ale nie o tym myślał Swallow przez resztę wieczoru. Chełpienie się dokonaniem „włamu, jakiego jeszcze nikt nie widział" tak bardzo zmęczyło innych uczestników czatu, że Swallow usunął go z pokoju dyskusyjnego.

8 maja o 9.00 *Buy.com* — internetowa firma sprzedaży detalicznej jak zwykle rozesłała wstępną ofertę towarów. Przyszłość rysowała się w różowych barwach, gdyż firma trafiła na okres mody na dotcomy[17]. Ale już o 10.50 administratorzy musieli podjąć walkę ze zmasowanym atakiem typu „denial-of service", podczas którego dane napływały z prędkością 800 megabitów na sekundę, co ponad dwukrotnie przekraczało normalne obciążenie serwera. Atak groził całkowitym odcięciem dostępu do firmy. Tego samego dnia po południu najpopularniejszy w sieci portal aukcyjny eBay również zgłosił zablokowanie

[16] *DDoS* (*Distributed Denial of Service* — rozproszony atak odmowy usług) — atak typu DoS, w którym wiele komputerów atakuje komputer-ofiarę — *przyp. tłum.*

[17] *Dotcom* (lub *dot-com*) — taką nazwą określono firmy, które w latach 90. oparły swą działalność rynkową na Internecie. Słowo pochodzi od nazw tych firm, których większość zawierała *.com* („dot" — kropka). Przykładem jest znana księgarnia internetowa *Amazon.com* — *przyp. tłum.*

usług, a zaraz potem to samo przydarzyło się popularnej księgarni wysyłkowej *Amazon.com*. Dla zarządzających startującą dopiero firmą *Buy.com* pocieszeniem mógł być fakt, że atak dotknął nie tylko ich. Nie były to też ostatnie ofiary.

Gdy tego dnia Swallow rozpoczął pracę, od razu natknął się bezczelnego młodocianego hakera używającego pseudonimu Mafiaboy. Ale tym razem Swallow wiedział, co się zdarzyło w Internecie, i miał nadzieję na znalezienie tropu w IRC-u. Mafiaboy ponownie sobie przypisał ataki, ale ani Swallow, ani żaden z hakerów na IRC-u nie potraktowali tego poważnie. To tylko chwalipięta Mafiaboy, robiący wokół siebie dużo szumu, irytujący innych hakerski szczeniak. Takie jawne lekceważenie zdenerwowało go i potraktował je jako wyzwanie.

Spytał uczestników czatu, co ma teraz zaatakować. Zignorowali go i odpowiedzieli, że na „chwalipiętomierzu" dotarł do końca skali, że jest durniem i idiotą bez żadnych rzeczywistych umiejętności. Ktoś rzucił mimochodem, że CNN byłoby równie dobrym obiektem jak witryny E-Trade.

„Niech będzie" — zgodził się.

W ciągu kilku minut zostało zablokowane działanie globalnego systemu przesyłania informacji i 1200 innych miejsc w rozciągającej się na cały świat sieci CNN. Następnego dnia dwie internetowe firmy handlowe, Datek i E-Trade dotknęły sporadyczne ataki zagrażające stabilności rynków finansowych. Z wolna, w miarę składania w całość okruchów informacji o źródłach ataków, stało się jasne, że użyto kilkudziesięciu komputerów, nad którymi ktoś zdołał przejąć kontrolę. Niezbyt dobrze zabezpieczone komputery Uniwersytetu Kalifornijskiego w Santa Barbara, Uniwersytetu Alberta w Kanadzie oraz uczelni w Atlancie i Massachusetts stały się „zombi". Ten sam los spotkał 75 komputerów rozsianych po świecie. Włamywacz zainstalował w ich systemach złośliwe programy, które zamieniły je w autonomiczne jednostki służące do przeprowadzenia ataków typy „denial-of-service".

Był to prawdziwy kryzys, przed którym od lat przestrzegali eksperci. Wokół zapanował strach, że jest to początek czegoś, co specjaliści od spraw bezpieczeństwa sieci nazwali elektronicznym Pearl Harbour, czyli niespodziewanego ataku mającego na celu okaleczenie całej internetowej struktury Stanów Zjednoczonych. Internet stanął na skraju załamania. Media rzuciły się na sprawę, jakby to był prawdziwy koniec świata. Gdyby ataki miały być kontynuowane, gospodarka światowa mogła rzeczywiście wpaść w spiralę śmierci. Ale, czy miały być kontynuowane? Ile systemów zostało zarażonych, ile zamienionych w „zombi", w ilu umieszczono bomby z opóźnionym zapłonem, czekające na zdalne zdetonowanie? To były najważniejsze pytania, na które należało odpowiedzieć jak najszybciej. Stawką było załamanie się wiary społeczeństwa w przyszłość internetowej ekonomii.

FBI musiało znaleźć hakera o pseudonimie Mafiaboy. I musiało to zrobić szybko.

^()<[]>()*^*

Gdy zadzwonił telefon, Knesek siedziała w pokoju hotelowym w wiejskiej części stanu Alabama, gdzie prowadziła dochodzenie w prawie innego hakera wykrytego podczas ogólnej obławy na podziemie. To był Neal.

„Mamy bardzo poważny problem" — wiedział. — Haker uderza we wszystkich głównych dostawców usług i centra komercyjne w Internecie, od Yahoo! do Amazon i CNN. Wstępne dowody wskazują, że dla kamuflażu korzysta z telnetu[18] przez Wingate proxy[19]. Większość z maszyn, do których się włamał i zamienił w „launching pads[20]", była komputerami uniwersyteckimi zarządzanymi prze Red Hat Linux 6.1.

Knesek weszła do Internetu, starając się znaleźć jakiś ślad. Ona także jeszcze kilka miesięcy wcześniej, zanim została koordynatorem operacji przeczesywania podziemia, wyrobiła sobie pozycję fałszywego nastoletniego hakera. Ale z Alabamy niewiele mogła zdziałać. Tropy były nadal trudne do wykrycia. Z końcem tygodnia wróciła do biura w Los Angeles.

Neal zdecydował, że biuro w Los Angeles będzie centrum operacji wywiadowczej, zaś zadaniem biur lokalnych, np. z San Francisco, będą sprawy penetracji technicznej. Wiedział, że to właśnie on dysponuje w podziemiu najlepszymi kontaktami wywiadowczymi. Mógł także korzystać z efektów rocznego udawania nastoletniego hakera. Akordem końcowym miało być połączenie obu rodzajów działań, co powinno w końcu doprowadzić FBI i policję kanadyjską do drzwi Mafiaboya.

Znalezienie rzeczywistego Mafiaboya było niełatwym zadaniem. W ciągu kilku dni od pierwszego ataku zaczęły napływać fałszywe zeznania. Trzeba było odbierać dziennie dziesiątki telefonów, a jeszcze więcej zgłoszeń pojawiało się przez Internet w IRC-owych pokojach pogawędek. Każdy twierdził, że to on jest odpowiedzialny za największy wyczyn hakerski od czasu działania grupy MOD i jej włamań do systemów telefonicznych rozmów zamiejscowych w roku 1990. Konieczność sprawdzenia tych przechwałek wydłużyła tydzień pracy całej grupy do 80 godzin. Spośród dziesiątków hakerów przyznających się do ataków FBI udało się odsiać trzech używających pseudonimu Mafiaboy i teraz należało wyłuskać właściwego.

Do FBI napływał strumień informacji od poszkodowanych firm. Exodus Communications, Inc., wielki dostawca usług internetowych, którego klienci — firmy z rejonu Los Angeles — również ucierpieli w wyniku ataków, oraz inne pomniejsze firmy — rozpoczęły żmudne sprawdzanie plików nadzoru swoich routerów i składanie mozaiki połączeń w czasie ataku. Powoli zaczął się wyłaniać rzeczywisty portret hakera.

Neal delegował kilku agentów do centrum operacyjnego sieci Exodusa w celu zbadania komputerów, które brały udział w ataku. Jednak nie zostali oni dopuszczeni do urządzeń przez straż firmową. Exodus wymagał czegoś więcej niż zwykłe zlecenie z FBI. Neal dostał po nosie, ale natychmiast zadzwonił do Exodusa. Zaczął od głównego numeru, ale pracownicy odsyłali go od Annasza do Kaifasza. Wściekły, gdyż

[18] *Telnet* — protokół internetowy pozwalający na logowanie się na innym komputerze podłączonym do Internetu. Również program pozwalający na korzystanie z tego protokołu — *przyp. tłum.*

[19] Wyspecjalizowany komputer, obsługujący komunikację między siecią wewnętrzną i Internetem. Jego zadaniem jest ochrona sieci lokalnej przed nieautoryzowanymi próbami dostępu oraz zmniejszanie ruchu na łączach poprzez buforowanie najczęściej pobieranych plików. W tym przypadku chodzi o serwer zarządzany oprogramowaniem opartym na technologii Windows — *przyp. tłum.*

[20] *Launching pad* (platforma wyrzutni rakietowej) — tu: miejsce, skąd jest dokonany atak, czyli mniej więcej to samo co „zombi" (patrz w poprzednich przypisach) — *przyp. tłum.*

zwłoka w tak krytycznym okresie, groziła utratą możliwości kontynuowania śledztwa, powtarzał żądania i wędrował w górę hierarchii służbowej Exodusa. W końcu dotarł do Billa Hancocka, nowego szefa działu bezpieczeństwa firmy. Dzień, w którym Neal zadzwonił, był dosłownie pierwszym dniem pracy Hancocka. Zaprzyjaźnieni od lat, ze zdumieniem spotkali się w tak zdumiewających okolicznościach. Po bardzo krótkiej wymianie zdań Neal uzyskał to, czego potrzebował — współpracę ze strony Exodusa. Dane otrzymane z systemu tej firmy stały się bardzo ważnym elementem śledztwa.

12 lutego koncern Dell Computer Corporation poinformował, że jego system został dosłownie zalany potokiem danych płynących z Internetu. Mafiaboy ponownie pojawił się w sieci, kontynuując kampanię autoreklamową i biorąc na siebie odpowiedzialność za atak na Della i wszystkie poprzednie. Kilku agentów bezpieczeństwa z prywatnych firm oraz inni hakerzy przechwycili i przesłali do FBI następującą sesję czatową. Oto przechwycony z hakerskiego kanału IRC-owego #!tnt zapis rozmowy Mafiaboya, który przybrał tu pseudonim ANON (od anonimowy), z kilkoma innymi hakerami używającymi imion T3, Mshadow i swinger:

ANON: FBI, WYNIUCHAJ MNIE!!

ANON: t3, możesz się połączyć z dellem? Jedni mówią, że tak, inni, że nie

T3: nie mogę przejrzeć sieci

ANON: idioci nie wiedzą co to cache[21]. telnetuj na port 80

T3: spoko, mój modem jest całkiem [f***ed][22]. Wszystko jest time out[23]. Nie, dzięki

SWINGER: anon. Chodzi, ale wolno

SWINGER: no, rzeczywiście opóźnia

MSHADOW: puszczasz na niego streama[24]?

ANON: mshadow, nie, mój własny atak

MSHADOW: hehe, jaki rodzaj pakietów?

ANON: spoofed[25] ++

ANON: to taka mieszanka. Nowy typ i syn[26]

[21] Pamięć buforująca, pamięć podręczna — *przyp. tłum.*

[22] *Fucked* lub *fucked-up* — (wulg.) ze względu na ustawę o ochronie języka polskiego pozostawiam domyślności Czytelników, podobnie jak następne wyrażenia `[f***it]` i `[f***]` — *przyp. tłum.*

[23] Przekracza czas, np. czas, w którym modem oczekuje na odpowiedź serwera — *przyp. tłum.*

[24] *Stream attack* — atak strumieniowy — istota ataku została opisana w następnych przypisach — *przyp. tłum.*

[25] Z podrobionym adresem IP — *przyp. tłum.*

[26] Komunikacja TCP jest inicjowana przez przesłanie do stacji docelowej pakietu SYN. Wysłanie dużej liczby pakietów z podrobionymi adresami IP wiąże zasoby systemu docelowego, który alokuje zasoby do obsługi i śledzenia nowej sesji komunikacyjnej i wysyła odpowiedź, która w przypadku fałszywego adresu IP trafia w próżnię. Wysłanie wielu fałszywych pakietów SYN łatwo doprowadza do przekroczenia limitu połączeń i wyłączenia komputera z sieci — *przyp. tłum.*

T3: spoofed ++, lol[27]

T3: spoofed, nie spoofed, nie są idealne, a nawet podmienione można śledzić, jak je złapiesz, gdy wypływają.

MSHADOW: muszą chodzić od routera do routera, aby wyśledzić. to jakieś 20 min.

T3: mafiaboy, kto po dell?

MSHADOW: poczekajcie na wiadomości na msnbc[28]

SWINGER: ms powinno być następne i wrzuć coś na czacie

ANON: t3, wieczorem wsadzę komputer do kominka

SWINGER: ehe

MSHADOW: haha

ANON: to nie żart

MSHADOW: dlaczego nie wyciągniesz i nie rozwalisz hd[29] i nie wsadzisz nowego

ANON: mshadow nie chce im dać ŻADNEJ szansy

MSHADOW: tak. a gadanie na IRC-u to nie szansa?

ANON: a co irc pokaże?

T3: mafia

ANON: aha [f***it][30], [f***] do kominka albo młotem i do jeziora

T3: wszystko podmienione, nie mogą cię złapać. Muszę zwiewać zanim wrobią mnie w twojego wspólnika lub wdepnę w inne g...

ANON: t3, nie [f***]

MSHADOW: haha

T3: a co

ANON: nie łap się za to

T3: chcesz zrobić wielki huk?

ANON: tak

MSHADOW: trzepnąć 10 routerów sieci szkieletowej:\

---

[27] *Laughing out loud lub lots of laughs* — slang internetowy, tutaj mniej więcej tyle co „ha ha ha" lub „śmiechu warte" — *przyp. tłum.*

[28] *MSNBC* — portal informacyjny, korzystający z informacji kanału NBC, joint-venture MS i NBC — *przyp. tłum.*

[29] *Hard disk* — dysk twardy — *przyp. tłum.*

[30] Aby nie podpaść pod ustawę o ochronie języka polskiego, zostawiam w wersji oryginalnej i pozostawiam domyślności czytelników — *przyp. tłum.*

ANON: nie

T3: to co planujesz

ANON: Microsoft

ANON: Microsoft będzie leżał na kilka tygodni

T3: HAHAHAHAHAHAHAHAHA

T3: człowieku, to źle

ANOAN: MOŻE, myślę o czymś większym. może *www.nasa.gov* lub *www.whitehouse.gov*, a może to blef

T3: zwiewam zanim mnie przymkną jako wspólnika lub wdepnę w gorsze g...

ANON: t3, trzepnij router

ANON: całą listę routerów

ANON: wiem, co robię

ANON: Yahoo!.com

T3: haha

T3: ten mafiaboy co trzasnął to wszystko co w wiadomościach, to rzeczywiście ty? buy.com, etrade, eBay, cały ten chłam?

ANON: pingnij je porządnie. nawet nie przekierują

ANON: t3 może. kto wie. mógłbym odpowiedzieć tylko pod ssh2 [bezpieczne, szyfrowane połączenie]

T3: haha

ANON: mógłbym wyciągnąć hd, trzepnąć młotkiem i wrzucić do jeziora

T3: mówią, że kosztujesz ich miliony

ANON: dziwisz się, że jeszcze mnie nie capnęli, t3, to durnie

Pomimo tego, że jeden z rozmówców się przyznał, agenci FBI i inni doświadczeni członkowie hakerskiej społeczności nie mogli uwierzyć, że chłopak, który przyjął pseudonim Mafiaboy, był w stanie przeprowadzić ataki tak skomplikowane, dokładnie przemyślane i tak rozległe. Przecież był tylko nastolatkiem i czeladnikiem w hakerskim rzemiośle. Ponadto eksperci ze służby bezpieczeństwa prywatnego sektora gospodarki poinformowali FBI, że atak na Yahoo! z 7 lutego różnił się znacznie od ataków, które miały miejsce w tydzień później, co wskazywałoby na udział grupy hakerów.

Patrząc wstecz, FBI i reszta hakerskiej społeczności zrozumieli, że przegapiono pierwsze poszlaki. Mafiaboy, którego już znali, rzeczywiście był osobą odpowiedzialną za ataki. Nie można udowodnić, że Swallow i jego agenci, uwierzywszy od razu w przechwałki o pierwszym ataku, byliby w stanie zapobiec następnym, ale trzeba przyznać, że pierwsze sygnały nie dotarły do ich świadomości; dzwonki alarmowe nie zadzwoniły na czas. Założono, że arogancki Mafiaboy nie nadaje się do czegoś

takiego. Przechwalał się, że nigdy go nie złapią. Ważniejsze było to, że jego zapowiedź wrzucenia komputera do ognia nie była czczą groźbą. Mógł w końcu wrzucić dyski twarde do jeziora i nikt by ich nie znalazł.

Przez następne dwa dni Neal i jego grupa ekspertów przeczesywali Internet, poszukując wskazówek pozwalających na ustalenie prawdziwej tożsamości Mafiaboya. 14 lutego znaleźli stronę:

```
www.dsupernet.net/~mafiaboy
```

Strona należała do użytkownika korzystającego z usług Delphi Supernet w Kanadzie. Wkrótce potem znaleziono coś, co nadawałoby się na dowód sądowy. Rzecz dotyczyła ataku na Della, a ślad prowadził do TOTALNET-u, dostawcy usług internetowych w Montrealu. FBI miało teraz dwie poszlaki łączące Mafiaboya z Kanadą. Było to istotne, gdyż istnieli przynajmniej dwaj inni uczestnicy czatów internetowych używający tego samego pseudonimu wystarczająco często, by zmusić FBI do ich szukania. Bardziej podejrzany z tych dwóch okazał się potem studentem jednej z uczelni w Nowym Jorku. Ale choć agenci z Nowego Jorku byli przekonani, że to oni namierzyli właściwą osobę, Neal święcie wierzył, że właściwy sprawca siedzi po drugiej stronie granicy, w Kanadzie.

Trzecim dowodem wspierającym tezę Neala, że należy się zająć Mafiaboyem z Kanady, były dane dotyczące pierwszego ataku i zarejestrowane przez administratorów systemu Uniwersytetu Kalifornijskiego w Santa Barbara. Oprócz kompletnych plików nadzoru, pokazujących dokładnie wszystkie działania hakera w systemie, skopiowali narzędzia, które posłużyły do przeprowadzenia ataku. Oprogramowanie było zarejestrowane na dwóch użytkowników: pierwszym był Mafiaboy, a drugim Short. Potem okazało się, że była to jedna i ta sama osoba. Jednakże dla późniejszego sformułowania oskarżenia i wydania wyroku istotniejszy był komunikat, który autor hakerskiego programu dołączył do niego, ku oświeceniu wszystkich, którzy ten program ściągną i zaczną używać:

```
UWAGA: używanie tego programu w sieci publicznej jest ABSOLUTNIE nielegalne i grozi
wsadzeniem do więzienia. Autor w żaden sposób nie odpowiada za twoje działania.
Ogranicz się do stosowania go wyłącznie w sieci wewnętrznej.
```

Wśród znalezionych narzędzi, przeznaczonych do wykonania ataku typu „denial-of-service", był Staheldracht, niemiecka wersja Barbed Wire, wariantu Tribal Flood Network (TFN), który wysyłając masę zapytań, paraliżował atakowany system. Jak większość nastoletnich hakerów, Mafiaboy nie stworzył samodzielnie narzędzi użytych do ataku. Przypuszcza się, że ich autorem był bardziej doświadczony niemiecki haker, znany jako Randomizer. Twórcą oryginalnego hakerskiego oprogramowania TFN był inny 20-letni haker niemiecki nazywany Mixterem. FBI natychmiast wysłało agentów do odszukania i sprawdzenia Mixtera. Po krótkiej rozmowie Mixter został wykreślony z listy podejrzanych. Później potępił ataki jako działania kryminalne i szkodliwe.

^()<[]>()*^*

14 lutego Waszyngton telefonicznie zawiadomił, że FBI potrzebuje pomocy Królewskiej Konnej Policji Kanadyjskiej, aby schwytać hakera o pseudonimie Mafiaboy,

który prawdopodobnie działa gdzieś w okolicach Montrealu. FBI i RCMP[31] miały za sobą długą historię wspólnych działań, więc strona kanadyjska natychmiast wyraziła chęć pomocy. Tak rozpoczęła się Operacja Claymore.

Od czasu ataku na szkolnego dostawcę usług internetowych w Oregonie agent RCMP Gosselin zajmował się wieloma innymi sprawami. Sprawa skończyła się fiaskiem i teraz była tylko odległym wspomnieniem. Ale po telefonie z FBI Gosselinowi powierzono śledztwo, którego celem było wyśledzenie Mafiaboya. Wybór Gosselina okazał się bardzo istotną dla toku śledztwa decyzją RCMP.

Następnego dnia, 15 lutego, Gosselin przystąpił do realizacji nakazu rewizji systemów Delphi Supernet i TOTALNET w biurach tych firm w Montrealu. Znalazł trzy konta e-mailowe przypisane do Mafiaboya:

mafiaboy@dsupe.net

mafiaboy@total.net

pirated_account@total.net

Choć konta te należały do osoby noszącej pseudonim Mafiaboy, nie oznaczało to, że jest nią poszukiwany haker. Jedno z kont okazało się być legalnym kontem pewnego brokera nieruchomości. Późniejsze dochodzenie, liczne telefony wyjaśniające i tropienie doprowadziły do miejsca zamieszkania Mafiaboya. Uzyskał on hasło konta niczego niepodejrzewającego małżeństwa i łączył się z nim, telefonując z domu.

Gosselin ponownie przystąpił do żmudnego przedzierania się przez góry informacji i dopasowywania numerów telefonów, kart kredytowych, adresów IP i nazw kont e-mailowych. Nic nie pasowało, za wyjątkiem pewnego numeru telefonu. Był to numer kontaktowy jednego konta. Większość firm telekomunikacyjnych i dostawców usług internetowych prosi klientów o podanie takiego numeru jako alternatywnego sposobu komunikacji. Z niewiadomych powodów numer ten wydawał się Gosselinowi znajomy. Zaczął szukać odpowiadającego mu adresu i znalazł Rue de Golf. Teraz informacje zaczęły się układać w całość. Przypomniał sobie ten adres.

Pomocne stały się lata doświadczeń zdobytych w pracy tradycyjnego detektywa. Pomimo postępu technologii i całego gadania o trudnościach znalezienia przestępcy komputerowego Gosselin i jemu podobni doskonale wiedzą, jakie znaczenia ma dobry policyjny nos węszący wokół. Szukając wskazówki, zaczął grzebać w starych teczkach. Jedna z pierwszych dotyczyła włamania do serwera Outlawnet, dostawcy usług internetowych w Oregonie. Znaleziony adres i numer telefonu pasowały jak ulał do adresu i numeru podejrzanego w tamtej sprawie. Mafiaboy wciąż działał. Gosselin poczuł, że tym razem go ma lub przynajmniej że ma prawdziwy adres Mafiaboya. „Zdaje się, że pasuje. Wygląda obiecująco" — powiedział. Jego podejrzenia zostały poparte długą listą skarg, które klienci dostawców usług internetowych składali na użytkownika tego konta. Wydawało się, że wielu z nich padło ofiarą hakera, którego konto udało się znaleźć w Delphi Supernet.

[31] *Royal Canadian Mounted Police* — Królewska Konna Policja Kanadyjska — *przyp. tłum.*

Kilka miesięcy wcześniej Gosselin nie zamknął go jedynie z powodu braku dowodów; być może zdobyłby je, gdyby w grudniu założył podsłuch telefoniczny tej linii. Trudno przewidzieć, co mogłoby się zdarzyć, gdyby Gosselin nie był przydzielony do biura RCMP w Montrealu w czasie, gdy nastąpiła seria ataków typu DDoS. Inny śledczy mógłby nie skojarzyć szczegółów. Tak ważna informacja mogłaby zostać przeoczona w krytycznym momencie.

W Waszyngtonie prezydent Bill Clinton wezwał na pilną konferencję w Białym Domu dziesiątki doświadczonych specjalistów odpowiedzialnych za sprawy bezpieczeństwa w przemyśle prywatnym i instytucjach narodowych. „Ostatnia fala ataków typu „denial-of-service" skierowanych przeciw największym firmom internetowym stanowi groźbę dla całego amerykańskiego stylu życia. Nie jest to Pearl Harbour, bo tam straciliśmy całą naszą Flotę Pacyfiku. Obecne straty nie są tak wielkie. Są ceną, jaką płacimy za sukces Internetu" — powiedział do zebranych w gabinecie na pierwszym piętrze.

Rozpoczął spotkanie od żądania, aby kilku ekspertów wyjaśniło mu, w jaki sposób doszło do ataków oraz jak mogło dojść do tak wielkiego zamieszania i tak wielkich strat w Internecie. Z wyjaśnieniami pierwszy wystąpił Rich Pethia, ekspert z Computer Emergency Response Team[32] w Mellon University. Po nim wystąpili Tom Noonan, szef Internet Security Systems[33], Inc. i Vint Cerf, główny wiceprezes MCI Worldcom. Wszyscy stwierdzili istnienie wielu błędów i niedociągnięć systemów, które w taki czy inny sposób przyczyniły się do powodzenia ataków. Ale najbardziej intrygujące wyjaśnienie podał Witt Diffie z Sun Microsystems. Siedząc naprzeciw prezydenta przy wielkim, wypolerowanym stole, zwykle używanym do rozmów nad sprawami najwyższej wagi, Diffie powiedział: „To tak, jakby prezydent przegrał wybory nie dlatego, że ludzie na niego nie głosowali, lecz dlatego, że ktoś ukradł głosy i oddał je przeciwnikowi". Była to analogia, którą Clinton był w stanie zrozumieć, ale jak później twierdziło wielu ekspertów, prezydent nie potrzebował takich wyjaśnień, by pojąć znaczenie ataków. Nie były one „elektronicznym Pearl Harbour", ale miały większe znaczenie, niż wielu ludzi chciało przyznać.

Prezydent i inni uczestnicy spotkania mieli istotne problemy, by zrozumieć wyjaśnienia Peitera „Mudge" Zatko, byłego członka hakerskiej grupy L0pht Heavy Industries, a obecnie konsultanta od spraw bezpieczeństwa. Wielu uznało jego wystąpienie za skrajny przejaw ironii. Grupa L0pht była odpowiedzialna za stworzenie L0phtCrack, jednego z potężniejszych internetowych narzędzi przeznaczonych do łamania haseł. Były członek grupy hakerskiej, którą oficjalni przedstawiciele rządu uznali za groźną, siedział teraz w Białym Domu, doradzając prezydentowi, w jaki sposób należy chronić systemy rządowe. Siedząc między Sandym Bergerem, Doradcą do Spraw Bezpieczeństwa Narodowego i Janet Reno, Prokuratorem Generalnym — swoimi długimi włosami i sposobem bycia cyberpunka zakłócał harmonię sztywnych garniturów i starannie ułożonych fryzur zebranych wokół oficjeli. Ku zaskoczeniu i zgorszeniu wielu, argumentował, aby odstąpić od uznania za przestępstwo tworzenia ofensywnych narzędzi hakerskich. Według niego, penalizacja takich działań spowoduje odcięcie zajmujących się sprawami bezpieczeństwa od możliwości efektywnego tworzenia narzędzi obronnych.

[32] Grupy do działań w komputerowym stanie wyjątkowym — *przyp. tłum.*

[33] Systemy bezpieczeństwa internetowego — *przyp. tłum.*

Argumenty Mudge'a zostały puszczone mimo uszu, co nie było zaskoczeniem, gdyż dostojnicy ze sfery rządu i zarządów udają, że wiedzą, czym jest hakerstwo, gdy tymczasem naprawdę nic do nich nie dociera. Nie rozumieją, że dbanie o bezpieczeństwo nie jest sprawą hakerów. Jeszcze trudniej im pojąć, że hakerzy nie są kryminalistami i ich działania nie mają znamion przestępstwa. Oczywiście, wielu z dawnych kolegów Mudge'a z podziemia znacznie się przyczyniło do takiego postrzegania ich środowiska. Teraz hakerzy sami do siebie mogą mieć pretensję za to, co o nich wypisują.

Choć doradcy prezydenta nie przedstawili jednolitej opinii na temat hakerstwa i spraw bezpieczeństwa, Clinton zrozumiał istotę sprawy i fakt, jak poważne konsekwencje dla gospodarki może mieć powtórzenie lutowych ataków. Jego postawa kontrastowała z niefrasobliwym podejściem do sprawy kilku szefów do spraw bezpieczeństwa przemysłu, którzy przysłali na konferencję swoich młodszych rangą przedstawicieli, niemających upoważnienia do podejmowania decyzji określających politykę bezpieczeństwa firm. Choć Clinton zaprosił osoby stojące na czele zarządów firm, wiele z nich wolało pozostać na boku, starając się uniknąć konfrontacji z prezydentem, gdyż obawiali się jego pytań dotyczących polityki bezpieczeństwa w nowej dziedzinie, jaką był Internet. Był to sygnał, że sektor prywatny nie zrozumiał groźby, jaką stanowiły ataki przeprowadzone w lutym. Koszty wynikające z utraty zysków i wypłaconych odszkodowań eksperci wycenili później na 1,7 mld dolarów.

W tym czasie zbierano dowody obciążające winą chuderlawego, buntowniczego i złośliwego 14-latka z okolic Montrealu. Wyobraźcie to sobie. Patrząc wstecz, nie należy się dziwić, że 14-latek był w stanie przeprowadzić atak, który rozłożył na łopatki największe firmy internetowe. Technika atakowania strumieniem pakietów jest szeroko znana w społeczności hakerskiej, a narzędzia do przeprowadzenia tego rodzaju ataku są dostępne w wielu miejscach Internetu. Niegdyś haker musiał włamywać się do każdej maszyny z osobna i uruchamiać indywidualne wersje narzędzi do ataku „denial-of-service". Teraz, za pomocą automatycznie działających skryptów, nawet niezbyt utalentowany nastolatek może przeprowadzić szeroko zakrojone przeczesanie sieci w celu znalezienia źle zabezpieczonych komputerów, zainstalować w nich oprogramowanie do ataku DDoS, po czym nakazać im wykonanie zmasowanego ataku na wybrany serwer.

Gdy dochodzi do ataku typu DDoS, przepustowość łącza jest sprawą równie istotną jak liczba komputerów użytych do ataku. Bardzo szybkie łącza 25 uniwersytetów, wykorzystane przez Mafiaboya do przeprowadzenia ataków, świetnie się nadawały do tego celu. Systemy uniwersyteckie ze względu na stosunkowo słabe zabezpieczenia były poligonem doświadczalnym dla różnej maści złośliwych hakerów. Ostatecznie ofiarą ataków DDoS padały liczne w sieci serwery sterowane systemami mającymi znane luki, wśród nich serwery rządu i wielkich korporacji. Gdyby komputery, których Mafiaboy użył do swoich ataków, były odpowiednio zabezpieczone przez administratorów, nigdy by nie doszło do tak bezkarnego, tygodniowego hulania po Internecie.

A była cała seria ostrzeżeń. Pod koniec 1999 roku NIPC[34] przy FBI zaczęło otrzymywać raporty o istnieniu narzędzi umożliwiających przeprowadzenie w Internecie zmasowanych ataków DDoS. Były to te same narzędzia, które później Mafiaboy ściągnął

[34] *National Infrastructure Protection Center* — narodowe centrum ochrony infrastruktury — *przyp. tłum.*

z sieci i których użył do ataków. Z powodu powstania nowej groźby w grudniu 1999 roku NIPC wysłało ostrzeżenie do agencji rządowych, firm prywatnych i instytucji publicznych. Ale nikt się tym nie przejął.

W tym samym czasie, gdy NIPC rozsyłał ostrzeżenia, agencja stworzyła narzędzie, za pomocą którego administratorzy sieci mogli wyśledzić w swoich systemach obecność programów przeznaczonych do przeprowadzenia ataku typu DDoS. Wtedy było to jedyne oprogramowanie służące do tego celu. Dlatego NIPC podjął kroki w celu udostępnienia go, co miało zmniejszyć groźbę ewentualnego ataku. Pierwszą wersję umieszczono na stronie NIPC w grudniu 1999 roku. Informacje o tym podano w prasie, jednocześnie tworząc trzy uaktualnione wersje, które przystosowano do pracy w różnych systemach operacyjnych i oczyszczono z zauważonych błędów.

FBI ze swoim oddziałem do ochrony przed przestępstwami komputerowymi, czyli NIPC, wykonało pracę, której wszyscy oczekiwali. Niestety, ani firmy, ani uniwersytety nie ściągnęły tego programu i nie użyły go do sprawdzenia, czy w ich systemach nie zostało ukryte złośliwe oprogramowanie. Żadne ostrzeżenia nie były w stanie zabezpieczyć ich przed atakiem.

Do 16 lutego informacje o znalezieniu przez Gosselina istotnego śladu dotarły do FBI. Zaplanowano uzyskanie zgody na założenie rejestratorów wykręcanych numerów na wszystkich liniach telefonicznych łączących rezydencję na Rue de Golf ze światem zewnętrznym. Rejestrator notuje wszystkie numery, z którymi nastąpiło połączenie, i jest stosowany do śledzenie kontaktów osób podejrzanych ze światem przestępczym, a w tym przypadku chodziło o śledzenie połączeń z dostawcami usług internetowych. Rejestratory są narzędziem o dużym znaczeniu w przypadku poszukiwania wspólników przestępcy i dowodów wystarczających do uzyskania zgody na założenie pełnego podsłuchu. Były szeroko wykorzystywane w roku 1990 podczas śledztwa przeciwko grupie MOD (Masters of Deception) i pomogły przedstawicielom prawa odkryć grupę elektronicznych włamywaczy, którzy zabawiali się uszkadzaniem systemów central zamiejscowych połączeń telefonicznych firmy AT&T.

Na liniach telefonicznych domu, w którym mieszkał Mafiaboy, rejestratory założono 18 lutego. Tego dna Jill Knesek przyjechała do Montrealu. Niestety, rejestratory miały swoje ograniczenia. Nie pozwalały na uchwycenie głosu, a tylko numerów, z którymi się łączono oraz daty i czasu rozmowy. Ale RCMP zmieniła taktykę dalszego postępowania, dzięki czemu powstała możliwość zastosowania pełnego podsłuchu. Teraz prowadzący śledztwo mieli dostęp do takich szczegółów z życia Mafiaboya i jego rodziny, które mogły posłużyć do oskarżenia młodocianego hakera oraz zmienić sposób myślenia wielu ludzi o jemu podobnych nastolatkach.

^()<[]>()*^*

Knesek od razu po przybyciu do Montrealu stała się pośrednikiem między kwaterą główną FBI w Waszyngtonie, Departamentem Sprawiedliwości i prowadzącym śledztwo z ramienia RCMP, czyli Gosselinem. Płynące z Waszyngtonu żądania informacji każdego mogły przyprawić o ból głowy i powoli wywoływały wściekłość w RCMP, której funkcjonariusze coraz niechętniej zaczęli przekazywać zdobyte dane.

Tak czy inaczej, w tej chwili sprawa bezapelacyjnie podlegała jurysdykcji kanadyjskiej. RCMP była główną jednostką odpowiedzialną za pierwszą w historii systemu prawnego Kanady operację przechwycenia danych tego rodzaju.

Knesek była pod wrażeniem informacji zdobytych na temat Mafiaboya do czasu jej przybycia do Kanady. Była również zaskoczona, że dopiero teraz spotyka Gosselina. Choć to nazwisko zrazu nic jej nie powiedziało, wkrótce dwaj agenci, z którymi się zetknęła, uświadomili jej, że oboje brali udział w organizowanych przez oddział FBI w Baltimore kursach specjalistycznych dotyczących śledzenia hakerów i przestępstw komputerowych. W ciągu kilku następnych tygodni Knesek i Gosselin stworzyli „bardzo dobry raport", który okazał się niezwykle istotny dla dalszego przebiegu śledztwa.

Po czterech dniach od zainstalowania rejestratorów numerów prowadzący śledztwo odkryli w TOTALNET-cie jeszcze jedno konto zarejestrowane na Mafiaboya. Tym razem konto należało do przedsiębiorstwa transportowego, którego właścicielem i zarządzającym był jego ojciec. Stało się jasne, że pomimo skasowania przed dwoma laty jego poprzednich kont Mafiaboy miał obecnie wiele możliwości łączenia się z Internetem i podszywania się pod kogoś innego. Były to konta, do których się włamywał i które oficjalnie należały do rodziny. Choć śledztwo skupiło się na śledzeniu jednego budynku, główne zadanie pozostawało jeszcze niewykonane. Należało stwierdzić, kto siedział przy komputerze i dokonywał ataków. Ponownie Gosselin i FBI stanęli przed pytaniem, co robić, gdyż zbyt wczesne wkroczenie do akcji mogło zaprzepaścić dotychczasowe wysiłki. Wówczas Mafiaboy, kimkolwiek był, mógłby umknąć bezkarnie.

W przypadku domu zamieszkanego przez pięć osób, w tym trzech nastolatków, w jeden tylko sposób można było zidentyfikować Mafiaboya i sprawdzić, czy miał wspólników. 25 lutego FBI i RCMP otrzymały sądowe zezwolenie na pełny podsłuch wszystkich rozmów prowadzonych z domu przez podejrzanego i jego najbliższą rodzinę. Pełny podsłuch oznaczał duże ilości informacji, przede wszystkim z rozmów telefonicznych i połączeń internetowych. Mieli 60 dni na zebranie dowodów wystarczających, by zwrócić się o ponowne wydanie nakazu sądowego.

Ale na tym etapie śledztwa zdarzyło się jeszcze coś, co stało się przyczyną późniejszych pytań, jak właściwie doszło do schwytania Mafiaboya. Choć szczegóły są nadal pilnie strzeżoną tajemnicą, FBI i RCMP przyznają, że w ostatecznej identyfikacji pomógł informator, dzięki któremu agenci wiedzieli, kiedy haker był w sieci. Pozostaje pytanie, kto był źródłem informacji i w jaki sposób potrafił stwierdzić, że to Mafiaboy jest na linii. W tej sprawie FBI i RCMP zgodnie milczą. Agenci policji kanadyjskiej ujawnili jedynie, że w tym okresie śledztwa udało im się ustalić, iż jeden z braci hakera używał wcześniej pseudonimu Mafiaboy. Zgodnie z opinią sierżanta sztabowego RCMP Roberta Currie, szefa Computer Investigative Support Unit[35], fakt ten okazał się pomocny dla dalszego przebiegu śledztwa. Czy informatorem był jeden z przyjaciół, niegdyś również zamieszany w działania hakerskie, czy też ktoś z domowników? Być może tego nie dowiemy się nigdy i Mafiaboy też się tego nie dowie. Tak czy inaczej, FBI i RCMP dysponowały już wieloma informacjami o osobie, przeciw której toczyło się śledztwo mające przygotować materiały dowodowe dla sądu, a która mieszkała w tym eleganckim domu z założonym podsłuchem.

[35] Oddziału komputerowego wsparcia śledczego — *przyp. tłum.*

Podsłuch rozpoczął się 27 lutego. TOTALNET przygotował zestaw adresów IP przeznaczonych jedynie do użytku przez konta, z których, jak podejrzewano, korzystał Mafiaboy. Dzięki temu prowadzący śledztwo mogli się skupić tylko na jego poczynaniach. Serwery do przechwytywania danych zostały zainstalowane również u dostawcy usług internetowych. Informacje zaczęły napływać natychmiast. Każdego dnia przechwycone dane były rekonstruowane za pomocą specjalnego oprogramowania przygotowanego przez FBI. Zadanie zbierania danych, zarządzania i sterowania nimi spadło na sierżanta Currie.

Jako szef Computer Investigative Support Unit, Currie aktywnie monitorował wszystkie połączenia internetowe wychodzące z domu Mafiaboya i przesiewał uzyskane informacje, starając się znaleźć dane, które pozwoliłyby na sformułowanie aktu oskarżenia. Wkrótce zauważył, że samo przechwytywanie danych jest najłatwiejszą częścią zadania. Trudniejsze było podzielenie ich na różne typy działania, np. surfowanie po stronach WWW, granie w dostępne w sieci gry komputerowe, wysyłanie i odbieranie e-maili — dzięki czemu można było ustalić, z kim Mafiaboy kontaktował się.

Zdarzały się dni bardzo aktywne i inne, nieco senne. Jeśli był aktywny, sesje trwały do trzeciej lub czwartej nad ranem, kiedy to wreszcie szedł spać. Zanim podsłuch po 43 dniach zakończył się, Currie zdołał zebrać 7,6 gigabajta surowych danych.

W większości przypadków Mafiaboy zajmował się w sieci przeglądaniem stron WWW, grami komputerowymi i prowadzeniem buńczucznych sesji na czacie IRC-a. Ale radził sobie świetnie, dobrze wykorzystując swój dwusystemowy (dual boot) komputer sterowany zamiennie przez Windows NT lub Unix. Ściągnął z Internetu Back Oriface Scanner, konia trojańskiego[36] (tylne drzwi) napisanego przez niesławnej pamięci grupę hakerską Cult of Dead Cow[37] (cDc). Niedoświadczony nastoletni haker pracował także nad zrozumieniem programu Netcat, „podsłuchiwacza portów" sterowanego wierszem poleceń. Jego zmagania z Netcatem świadczyły, że nie był biegłym hakerem, gdyż ten program powinien już mieć opanowany w początkach kariery. Mafiaboy dopiero się uczył, ale był zdolnym uczniem.

Agenci obserwujący jego działania w czasie rzeczywistym widzieli, jak podczas sesji telnetowej, podczas której starał się włamać do komputera, pewne polecenia wpisywał kilkakrotnie w różnych formach, zanim trafił na poprawną. Ponadto wydawało się, że zawsze korzysta z kont, do których login i hasło otrzymał od innych hakerów. Jeden z nich przesłał mu plik zawierający dane o 20 różnych systemach uniwersyteckich.

Poza rozpaczliwymi próbami rozwikłania zawiłości Netcata i wprawianiem się w używaniu różnych poleceń hakerskich Mafiaboy zakładał nielegalne miejsca sieciowe FTP (File Transfer Protocol[38]) na serwerach, do których wcześniej uzyskał dostęp podczas przygotowywania lutowych DDoS-owych ataków. Miejsc tych używał do handlowania nagraniami Sony Playstation i japońskimi animacjami wideo Dra-

[36] Koń trojański — program, który pozornie wykonuje istotne funkcje, ale w tle prowadzi działania niszczące. W odróżnieniu od wirusów, konie trojańskie nie rozmnażają się — *przyp. tłum.*

[37] Kult zdechłej krowy — *przyp. tłum.*

[38] Protokół transmisji plików — internetowy standard przesyłania plików. Do przesyłania plików służy program nazywany klientem FTP — *przyp. tłum.*

gonBallZ. Ściągnął uniksowe skanery, żeby łamać konta internetowe. Często grzebał w systemach 25 uniwersytetów rozsianych w USA i w Kanadzie, do których udało mu się zdobyć dostęp.

Ponadto był rodzajem internetowego łobuza rozrabiającego z bandą podobnych mu młodocianych hakerów. Miał w sieci wielu przyjaciół tego rodzaju. IRC stał się centrum jego internetowej egzystencji. Często „przesiadywał" na kanałach czatowych : #exceed, #shells i #carding oraz należał do grupy hakerskiej TNT, czego dowodem była sesja powitalna w oddzielnym pokoju, która jednak nie była kontynuowana. Ostatecznie porzucił TNT, uważając, że dzięki zdobytemu tam doświadczeniu jest w stanie założyć własną grupę hakerską, która rozprawi się ze wszystkimi witrynami internetowymi. Sprawiała mu przyjemność zdobyta sława hakerska, ale problemem, przed którym stanął, był fakt, że jego umiejętności nie dorównywały jakości oprogramowania, którego używał.

^()<[]>()*^*

W marcu jego ojciec założył DSL (digital subscriber line) w Sympatico-Lycos, Inc. U tego wielkiego (jednego z największych w Kanadzie) dostawcy usług internetowych i gospodarza stron WWW 16 marca zaczął działać podsłuch na linii DSL.

Przejmowano tyle danych, że Currie założył we własnym domu małe laboratorium, dzięki czemu również stamtąd mógł sterować podsłuchem, zaś będąc w biurze RCMP, mógł przez cyfrową kamerę wideo pilnować swoich dzieci. Pewnej nocy po przyjęciu, które wraz z żoną wydał dla kolegów z FBI, wraz z jednym z agentów zdecydował się zejść do przyziemia, by spojrzeć na ostatnie wyniki śledztwa.

Zobaczył wówczas istny potop informacji wchodzących do domu Mafiaboya i zeń wychodzących. Od razu skojarzył, że to kolejny atak „denial-of-service". Było to coś, na co agenci długo czekali. Ustalanie, w jaki sposób prowadzić dochodzenie, i jednocześnie zabezpieczać innych przed atakami, było wielkim wyzwaniem.

Currie wyszarpnął z bieżącego strumienia danych kilka pakietów i rozpoczął ich analizę. Z surowych danych zawartych w pakietach można się wiele dowiedzieć, pod warunkiem, że wie się, czego szukać. Łatwiej stwierdzić, czy to pakiety HTML, czy inne z sieci Web, nieco trudniej odróżnić dane z e-maili. Po dziesięciu minutach napięcie Curriego osiągnęło szczyt. Nagle zauważył pakiety zawierające komunikaty: „I'm going to kill ya[39]", „Death God[40]" i inne podobne. Nie był to następny atak „denial-of-service" na kolejną witrynę handlu internetowego, lecz komputerowa gra strategiczna Starcraft, w której w czasie rzeczywistym walczą ze sobą w wojnie galaktycznej trzy rasy.

Currie zauważył wówczas, że Mafiaboy czasem robi doświadczenia z narzędziami, które posłużyły mu do ataków w lutym. Gdy już się zdawało, że zrezygnował z działań hakerskich i wziął za naukę, 21 marca przeprowadził ograniczony atak na samego siebie za pomocą pakietów ICMP. Ach, te szczeniaki. Wydaje się, że nigdy się niczego nie nauczą.

[39] Slang.: zamierzam cię zabić — *przyp. tłum.*

[40] Bóg śmierci — *przyp. tłum.*

Nieudolność Mafiaboya nie zaskoczyła prowadzących śledztwo. Szkoła nigdy go nie pociągała. Koledzy z klasy i nauczyciele opisywali komputerowe cudowne dziecko jako chłopaka, którego wciąż zawieszano w prawach ucznia z powodów dyscyplinarnych. W rzeczywistości przed aresztowaniem Mafiaboy był w Riverdale High School dwukrotnie zawieszony w prawach ucznia. Po aresztowaniu złamał nawet warunki umożliwiające powrót do szkoły po zakończeniu zawieszenia. Koledzy z klasy i nauczycieli wspominają, że zdarzało mu się pyskować nauczycielom angielskiego i matematyki oraz walić pięściami w ławkę na znak frustracji. Rzadko zjawiał się w szkole z kompletem podręczników i odrobioną pracą domową. Po jego aresztowaniu jeden z kolegów wspominał, że miał problemy z odnalezieniem się w świecie rzeczywistym.

Takie problemy z dopasowaniem zdarzały się rzadko w etnicznie wielorakiej, liczącej 1200 uczniów Riverdale High School. Mafiaboy lubił ubierać się w workowate spodnie, bluzy i tenisówki. Często go widziano z czapeczką baseballową noszoną daszkiem do tyłu — zgodnie z modą punków. W przeciwieństwie do tych, którzy uważali go za normalnego chłopaka, część twierdziła, że przestawał głównie z łobuzami, paląc papierosy, zaczepiając dziewczyny i pakując się w różne kłopoty.

W szkole, której motto brzmiało „Rozwijaj się i odnoś sukcesy" czuł się jak ryba wyjęta z wody. Nie była to, oczywiście, jego pierwsza szkoła. Z poprzedniej wyrzucono go z powodów dyscyplinarnych. W przeciwieństwie do niej, w Riverdale wymagano, by uczniowie nosili mundurki. Kolorami szkoły były ciemna lesista zieleń i czerń. Do wyboru były: białe klasyczne koszule, białe golfy, zielone rozpinane swetry, pulowery z wycięciem w serek i blezery. Żadnych tenisówek, butów sportowych, czarnych dżinsów, spodni palazzo, swetrów i butów z cholewami.

Te szczegóły wyszły na jaw dopiero po aresztowaniu Mafiaboya. Przedtem jednak policja kanadyjska dowiedziała się pewnych niezbyt chwalebnych szczegółów o życiu domowym Mafiaboya. Knesek potem zauważyła: „Jego pseudonim nie był przypadkiem i nie wziął się z powietrza".

^()<[]>()*^*

Pełny obraz Mafiaboya ukazał się 15 kwietnia 43 dni od założenia podsłuchu. Okazało się, że podsłuch telefoniczny jest doskonałym narzędziem zbierania dowodów pozwalających postawić nastoletniego hakera przed sądem. Udało się ustalić i udowodnić zarówno jego winę, jak i fakt, że działał samodzielnie. RCMP chciała jednak niepodważalnego dowodu, że to on siedział przed komputerem.

W tym czasie Mafiaboy skończył 15 lat, a jego starszy brat świętował ukończenie 18. Dla Gosselina była to dobra wiadomość, gdyż w przypadku, gdyby się okazało, że starszy brat byłby zamieszany w przestępstwo, mógłby już być sądzony jako dorosły. Gosselin i Knesek mieli zdjęcia członków rodziny, ale różnica wieku między braćmi nie była na tyle duża, by można było bez kłopotu odróżnić, kto rozmawia przez telefon. Czasami agenci musieli się dokładnie wsłuchiwać w treść rozmowy, by poznać, który z braci rozmawia. Obaj mieli podobne gusta, to samo lubili, tego samego nie lubili i obaj gadali o dziewczynach.

Tematem rozmów był także Mafiaboy i stało się to kluczowym dowodem wskazującym na winę młodszego. Poza jego opowiadaniami, gdzie i do czego się włamał, podsłuchano także rozmowę, w której starszy chwalił się kolegom hakerskimi wyczynami młodszego. Pewnego razu opowiadał, jak to o jego młodszym bracie mówili i pisali we wszystkich wiadomościach. Była to wyraźna aluzja do lutowych ataków „denial-of-service".

John Calce, ojciec Mafiaboya, również uważał hakerskie osiągnięcia syna za godne podziwu, ale jako biznesmen nie był zadowolony z uwagi, jaką na siebie ściąga, spodziewając się kłopotów. 45-letni szef firmy transportowej miał na głowie inne problemy i na pewno nie było mu potrzebne dodatkowe zainteresowanie przedstawicieli prawa.

Rozważał wynajęcie kogoś do napadu na wspólnika. Spór dotyczył transakcji wartej 1,5 mln dolarów. Został pociągnięty do odpowiedzialności za coś, co według Gosselina i Knesek, można było uznać za spisek w celu dokonania morderstwa.

Przez 43 dni Gosselin walczył z pokusą, by wtargnąć do domu i skonfiskować komputery młodocianego hakera — dążył do wykorzystanie pełnych 60 dni podsłuchu, na które otrzymał zgodę sądu. Ale teraz RCMP miała dowody, że jego ojciec planuje spisek, którego ofiarą może paść człowiek. Działanie już zaplanowano. Tego dnia wieczorem podsłuchano dwóch mężczyzn dochodzących do porozumienia przez telefon. Prowadzący śledztwo musieli działać. Jak wspomina Gosselin „Nie chcieliśmy, aby ktokolwiek został zabity".

Policja wtargnęła do domu 15 lipca o trzeciej nad ranem. Jednakże znaleźli jedynie zaskoczonego i zmieszanego ojca, macochę Mafiaboya i jego dwóch braci. Jego samego nigdzie nie było widać. Po zabraniu ojca do aresztu dowiedzieli się, że tego dnia Mafiaboy był u przyjaciela. Gdy agenci RCMP pojawili się przed jego domem, Mafiaboy stał na zewnątrz, przy krawężniku — w pełni ubrany i wypoczęty. Wyglądał, jakby czekał na autobus lub taksówkę. Na jego twarzy było dokładnie to, czego można było oczekiwać: nadszedł jego czas i wiedział o tym.

Knesek nie była obecna podczas akcji zajmowania domu, ale pozostały jej w pamięci podsłuchane rozmowy i obraz patologicznej rodziny. Wszyscy bracia zamykali swe pokoje na kłódki. Mafiaboy „wiele widział, z wieloma rzeczami miał do czynienia i wiele rzeczy sobie przyswoił" — wspomina Knesek. „Ani on, ani jego ojciec nie uważali, że to, co robi, jest nielegalne i szkodliwe. Takie po prostu było życie tej rodziny". Mafiaboy zdobył nieco respektu innych hakerów, ale trwało to jedynie do chwili, gdy zaczęli się oni obawiać kontaktów z nim.

^()<[]>()*^*

Osadzenie Mafiaboya oznaczało zamknięcie śledztwa prowadzonego przez pięciu agentów RCMP przez 60 do 80 godzin tygodniowo, co kosztowało 60 tys. dolarów amerykańskich. Mounties[41] mieli wreszcie swego chłopca. Ale gdy przystąpiono do badania dysków twardych z zarekwirowanych komputerów, nie znaleziono żadnego

[41] Konni, popularna nazwa policjantów i agentów RCMP (*Royal Canadian Mounted Police* — Królewskiej Konnej Policji Kanadyjskiej) — *przyp. tłum.*

technicznego dowodu, który pozwoliłby na powiązanie oskarżenia z atakami z lutego. Dyski twarde Mafiaboya i inne techniczne dowody leżały zapewne na dnie Lake of Two Mountains lub jednego z wielu innych okolicznych jezior, rzek i ich dopływów tworzących całą sieć w okolicach Montrealu. Bez podsłuchu i dowodów przechwyconych przez administratorów z uniwersytetu w Santa Barbara Mounties nie mieliby nic pozwalającego na sporządzenie aktu oskarżenia.

W sądzie dla nieletnich Mafiaboy przyznał się do dziesiątków przestępstw związanych z atakami dokonanymi w lutym. Odrzucił jedynie oskarżenie o atak na Outlawnet, szkolnego dostawcę usług internetowych w Oregonie. RCMP cofnęła oskarżenie i do dziś podejrzewa, że za ten atak odpowiedzialny jest jeden z braci Mafiaboya.

Ale przyznanie się do winy było jedynym, co zrobił. Nie chciał rozmawiać. Gosselin próbował wielokrotnie nawiązać z nim rozmowę, by dowiedzieć się, dlaczego zrobił to, co zrobił, jakie były motywy jego działania i czy cokolwiek pchnęło go lub zmusiło do dokonania ataków. Ale chłopak i jego prawnik, Yan Romanowski, wielokrotnie odmawiali odpowiedzi na pytania. Jedyny raz, gdy Gosselin i inni agenci mieli okazję przeprowadzić wywiad z oskarżonym, był również obecny Romanowski. Montrealski haker uznał, że jego szansą jest przekonanie sądu, że 7, 8, 9, 10 i 12 lutego po prostu przeprowadzał testy, które miały być pomocne w pracy nad nowym, ulepszonym firewallem[42].

Ale w jego historyjce było kilka niezgodności. Pierwsza i najważniejsza to fakt, że jego tzw. testy trwały aż sześć dni. Ponadto narzędzia hakerskie, które ściągnął i wykorzystał, zawierały ostrzeżenia, że ich użycie przeciw innemu komputerowi lub sieci jest nielegalne i nie mogą one służyć do zbierania danych statystycznych i innych, które można by spożytkować do konstrukcji firewalla. Jego historia była całkowicie nieprzekonująca i dowodziła, że nie stać go na bardziej finezyjne myślenie. Gosselin wspomina: „było jasne, że chciał rozłożyć te wielkie firmy. Dowody wykazywały to bez cienia wątpliwości. Nie było dla niego żadnego wyjścia".

Na rozprawie wstępnej w czerwcu roku 2001 pojawił się w swych workowatych spodniach, niebieskiej dżinsowej koszuli wyrzuconej na spodnie i niechlujnej. Ostatnim ciosem rozbijającym jego obronę była opinia zatrudnionego przez sąd biegłego, który przeprowadził wywiad rodzinny. Przed sądem stwierdził, że: „oskarżony nie tylko nie przyjmuje na siebie odpowiedzialności za popełnione czyny, lecz również przekonuje, że miał prawo tak postąpić". W 16-stronicowym raporcie przedłożonym sądowi biegły dochodził do wniosku, że Mafiaboy kłamie, twierdząc, że zamierzał jedynie wypróbować jakość systemów ochrony atakowanych stron. Gdyby to była prawda, ataki nie trwałyby tak długo.

Sąd zgodził się z opinią biegłego, że oskarżonego należy na pięć miesięcy osadzić w zamkniętym areszcie, gdyż istnieje niebezpieczeństwo, że powróci do włamań komputerowych. Jego matka powiedziała przed sądem, że czuje, iż była za surowa dla chłopca, gdy wykazał pierwsze zainteresowanie komputerami, ale ojciec był zbyt pobłażliwy i nie nadzorował jego poczynań, a przecież — dodała — rodzice są odpowiedzialni za wychowanie dzieci.

[42] Zapora (ściana) ogniowa — specjalnie oprogramowany komputer lub system odgraniczający sieć wewnętrzną od Internetu. Jego zadaniem jest ochrona sieci wewnętrznej — *przyp. tłum.*

Choć biegły powołany przez obronę stwierdził, że Mafiaboy w pełni świadomie przyjął na siebie odpowiedzialność za popełnione przestępstwa i uznał winę, oskarżyciel Louis Miville-Deschenes użył opinii nauczycieli i innych pracowników szkoły do przedstawienia sądowi obrazu chłopca nieokazującego innym szacunku, krnąbrnego, sprawiającego kłopoty i żądnego podziwu. To był Mafiaboy, którego znali Swallow, Gosselin i Knesek. A któż znał go lepiej od agentów, którzy śledzili i podsłuchiwali wszystkie jego poczynania?

12 września 2001 roku sąd kanadyjski skazał Mafiaboya na ośmiomiesięczny pobyt w ośrodku odosobnienia dla młodzieży. Maksymalny wyrok, który mógł otrzymać, wynosił dwa lata. Sędzia zakazał również skazanemu posiadania jakiegokolwiek oprogramowania niedostępnego komercyjnie i zabronił używania Internetu do rozmów z innymi hakerami oraz włamywania się do jakichkolwiek miejsc w sieci. Nakazał również ujawnianie władzom nazwy dostawcy usług internetowych.

^()<[]>()*^*

Od tego dnia tajemnicza sprawa Mafiaboya ucichła w Internecie, przestała „być na topie". W mniej niż trzy miesiące z władcy cyberprzestrzeni, rzucającego wyzwanie potęgom rządowym i ekonomicznym, spadł do roli chłopaka, którego chuderlawa postać i niewymyślne umiejętności hakerskie nie były w stanie wygrać z siłami prawa. Wielu może twierdzić, że był zaledwie napuszonym amatorem, niewartym uwagi, którą mu poświęcono. Ale jego historia jest znacząca.

Poprzednim hakerem, który w pojedynkę zmusił FBI do użycia swoich ogólnokrajowych technicznych i ludzkich zasobów był Kevin Mitnick hulający w sieci w latach 80. i na początku lat 90. Jest znakiem czasu, że do śledztwa w sprawie Mafiaboya wciągnięto ponad stu agentów z dwóch krajów, co trudno porównać z trzema agentami na pełnym etacie, którzy ścigali Mitnicka.

Podobieństwa między oboma hakerami są uderzające. Żaden z nich nie był zbyt dobry w tym, co robił. Mitnick był daleko lepszym specjalistą od „inżynierii socjalnej" niż hakerem, choć w tamtych czasach można było uznać jego wiedzę za dość zaawansowaną. Mafiaboy potrafił rozreklamować swoje osiągnięcia, ale w atakach korzystał z narzędzi i technik dawno temu wymyślonych przez innych. Ale w tej chwili żaden haker nie musi być wybitnie sprawny i uzdolniony. Osiągnięcia Mitnicka były pochodną numerów telefonicznych, numerów kont i haseł, które potrafił wydobyć od ogłupionych i nieostrożnych ludzi. Sukcesy hakerskie Mafiaboya opierały się na korzystaniu z gotowych programów-narzędzi, które ściągał ze wszystkich możliwych miejsc Internetu. Nie była to wielka sztuka; zwykłe znalezienie obiektu i naciśnięcie klawisza Enter. Nie interesował go finezja programowania ani odkrycia technologiczne. Interesowały go przestępstwa.

Ironią losu jest fakt, że Neal opuścił FBI i zatrudnił się w Exodusie, firmie, która z początku odmówiła jego agentom dostępu do urządzeń — co było tak istotne w śledztwie dotyczącym Mafiaboya. W końcu ściągnął do współpracy Swallowa oraz Knesek i stworzył w Exodusie wyspecjalizowaną grupę Cyber Attack Tiger Team[43]. W czasie pisania tej książki Gosselin i Currie pozostawali na swych stanowiskach w RCMP w Montrealu.

[43] Grupa tygrysów do spraw ataków komputerowych — *przyp. tłum.*

Wszyscy agenci biorący udział w polowaniu na Mafiaboya stwierdzili, iż nie wątpią, że nastolatek z Montrealu działał sam. Twierdzą, że to jednoznacznie wynika z danych uzyskanych dzięki podsłuchowi. Jednakże eksperci od spraw bezpieczeństwa z firm prywatnych i inni członkowie hakerskiego podziemia uważają, że jeszcze nie znaleziono prawdziwych „mózgów" ataków „denial-of-service" z lutego 2000 roku. Twierdzą, że umiejętności Mafiaboya nie były wystarczały do przeprowadzenia tak przemyślanych i skoordynowanych działań. A co ważniejsze, część ekspertów zatrudnionych wówczas do analizowania danych uważa, że taktyka zastosowana w ataku na Yahoo! różniła się od taktyki w pozostałych atakach. A jeżeli ten argument nie wystarcza, należy się zastanowić nad istnieniem sporej liczby fałszywych zeznań i ujawnieniem faktu, że niektórzy hakerzy podczas sesji IRC-a podszywali się pod Mafiaboya i mogli oszukać innych.

Neal jest jednak nadal przekonany, że Monties złapali właściwego chłopaka. „Byłem w środku tego wszystkiego" — mówi. Twierdzenia, że Mafiaboy nie działał samodzielnie uważa za „absolutnie fałszywe". Według niego „jest całkowicie pewne, że tylko on jest winien".