Rozdział 3.
Złoczyńcy

Elita hakerska początkowo była kodem słownym używanym w podziemnych komputerowych biuletynach (np. magazyn 2600). „Złota era" hakingu trwa jednak dalej. Elita jest pewnym stanem, zaszczytem, który trzeba nabywać sukcesywnie, stopniowo i powoli. Jest wiedzą i techniczną sprawnością, która musi być ciągle udowadniana i udoskonalana. Haker ze zdobywanej wiedzy buduje swoistą bazę danych, którą później udostępnia dla innej zaufanej generacji ludzi młodych. Przez lata elita hakerska wypracowała na swój własny użytek swoisty kodeks postępowania. Główne jego założenia to:

- Nigdy nie uszkadzaj systemu, bo możesz przysporzyć sobie kłopotów;
- Nigdy nie zmieniaj plików systemowych oprócz tych, które powinieneś zabezpieczyć, ażeby nie zostać wykrytym i tych, które sam zabezpieczyłeś, aby zyskać bezpieczny dostęp do systemu w przyszłości;
- Nie mów nikomu o swoich wyczynach, projektach z wyjątkiem tych osób, którym ufasz;
- Kiedy korespondujesz przez BBS, nie używaj konkretów, ponieważ BBS może być kontrolowany przez siły rządowe;
- Nigdy nie używaj prawdziwego imienia i nazwiska, numeru telefonu kiedy konwersujesz przez BBS;
- Zostaw system w takim stanie, jak go zastałeś;
- Nie włamuj się do komputerów i systemów rządowych;
- Nie rozmawiaj z nikim o swoich planach przez telefon domowy;
- Bądź przezorny aż do przesady, a wszystkie swoje materiały trzymaj zakodowane w bezpiecznym miejscu;
- Aby stać się prawdziwym hakerem musisz hakować;
- Haker nie posługuje się wirusami, a jedynym powodem eksperymentowania z nimi jest chęć poznania sposobu ich działania;

- Haker nie włamuje się dla osiągnięcia korzyści innych niż poszerzenie swojej wiedzy;
- Haker nie modyfikuje danych w systemach, do których się włamał (dopuszczalne są wyjątki: zmiana zapisów systemowych, aby wejście do systemu pozostało nie zauważone, naprawy uszkodzonych plików, korekty w plikach użytkownika w celu zapewnienia sobie dostępu w przyszłości);
- Haker dzieli się swoją wiedzą, chce, aby ludzie poznawali luki w systemach zabezpieczeń i mogli je naprawiać (a nie wykorzystać); haker pomaga tym, którzy pomagają sobie, tzn. jeżeli ktoś ciężko się napracował i nadal sobie nie radzi, haker wyciągnie do niego pomocną dłoń, bo chociaż haker może łamać ustawowe prawo, nie złamie nigdy zasady etyki;
- Haker płaci za oprogramowanie komercyjne i nie korzysta z pirackich kopii;
- Haker wie, że informacja powinna być powszechnie dostępna, ale respektuje prawo do poufności informacji prywatnych.

Znani i nieznani

Hakerzy, których znamy nie są tak naprawdę zbyt dobrymi hakerami. Ci najlepsi po prostu nie dają się złapać. Pracują w cieniu, kontrolując być może wszystkie działające wokół nas systemy komputerowe. Pracują za bardzo poważne pieniądze dla wywiadów światowych mocarstw i — zamiast niszczyć — wyszukują cenne informacje strategiczne. Są to „faceci w czerni", których być może nigdy nie poznamy, zaś efekty ich działań pozostaną dla niewidoczne. To są właśnie najlepsi hakerzy, którzy tworzą hakerską elitę.

„Gabinet Cieni"

Poniżej przedstawione zostały sylwetki i losy najbardziej znamienitych hakerów.

Dennis Ritchie, Ken Thompson, Brian Kernighan


Ritchie, Thompson i Kernighan to programiści firmy Bell Labs, którym zawdzięczamy istnienie systemu Unix i języka C. Bez tej trójki nie byłoby Internetu (albo byłby dużo mniej funkcjonalny). Ciągle są aktywni. Na przykład Ritchie pracuje nad systemem Plan 9, który być może zajmie miejsce Uniksa jako standardowego systemu dla sieci komputerowych.

Paul Baran, Rand Corporation

Paul Baran to prawdopodobnie najznakomitszy haker w historii, który zajmował się Internetem jeszcze zanim ten zaczął istnieć! Rozpracowywał samą ideę sieci globalnej i stworzył podstawy, na których oparli się jego następcy.

Eugene Spafford

Spafford jest znanym i cenionym profesorem informatyki Uniwersytetu Purdue. Miał ogromny wkład w powstanie systemu bezpieczeństwa COPS (*Computer Oracle Password and Security System*), półautomatycznej procedury zabezpieczania sieci. Spafford wykształcił niejednego wybitnego specjalistę i jest figurą bardzo poważaną w kręgach informatycznych.

Dan Farmer

Powiedziano kiedyś, że bezpieczeństwo w Internecie to pojęcie wewnętrznie sprzeczne. Zachowanie strefy prywatności, odpowiedzialność i ograniczenia w dostępie do informacji — jak się uważa — są technicznie niezgodne z gwałtownie rosnącą siecią publiczną i skomplikowanym oprogramowaniem. Skoro tak jest, to nic dziwnego, że 37-letniego Dana Farmera uważa się powszechnie za czołowego przedstawiciela elitarnego kręgu specjalistów do spraw bezpieczeństwa w Internecie. Jest prawdziwym guru. Za konsultacje pobiera honorarium dochodzące nawet do 5 000 dolarów dziennie i często jest powoływany w charakterze eksperta doradzającego komisjom senackim w sprawie zabezpieczenia federalnych systemów komputerowych. Ale kiedy pojawia się na konferencjach, natychmiast wtapia się w grono hakerów, którzy tłoczą się wokół niego, jakby był gwiazdą rocka. Bo Farmer czuje się najlepiej w tej wąskiej szarej strefie, gdzie spotykają się przeciwności.

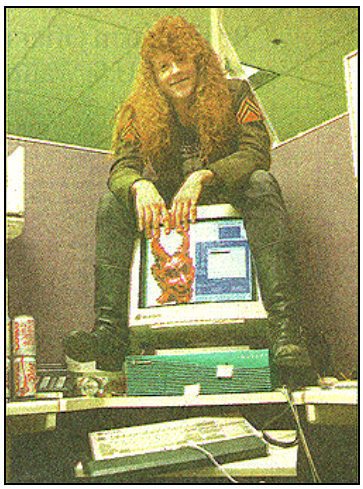
Potwierdza to jego barwna biografia. Wychowany w Bloomington (Indiana) Farmer rozpoczął studia na tamtejszym uniwersytecie. Uczęszczał przez jakiś czas na zajęcia z informatyki prowadzone przez znakomitego matematyka (także byłego felietonisty „Scientific American”) Douglasa R. Hofstadtera, ale rozczarowany (a może znudzony) przeniósł się do Purdue University, gdzie — zanim powrócił do studiów informatycznych — próbował kolejno swoich sił w dziedzinie astronautyki i matematyki. Mimo tych urozmaiceń zwykle wspomina studia jako bezbarwny okres swojego życia, tak bardzo pozbawiony fantazji, że tłumione pragnienie przygody pchnęło go dalej i... zaciągnął się do piechoty morskiej. Ale przygoda skończyła się, gdy w czasie wojny w Zatoce Perskiej dostał kartę powołania. Wówczas oświadczył, że używanie broni jest niezgodne z jego przekonaniami i został zwolniony ze służby. Powrócił do Purdue. Jego oceny okazały się za słabe, aby mógł podjąć studia doktoranckie. Kolejne ograniczenie. Cóż zrobić mógł Dan w takiej sytuacji? Otóż przekonał informatyka Eugenea H. Spafforda z Computer Emergency Response Team w Carnegie Mellon University, by powierzył mu pracę nad Cops, programem, który stanowił jedno z pierwszych — więc nie dość dobrych — narzędzi do analizowania reguł bezpieczeństwa w Internecie. Od tego wszystko się zaczęło.

Aktualnie Farmer mieszka w skromnym domu w Berkeley w Kalifornii. Rzadko się goli, chodzi w czarnych podartych skórzanych spodniach. Jego rude kręcone włosy zaczepiają o srebrny kolczyk wkłuty w prawą brew i zwisając z obu stron grubych, niemodnych okularów, przesłaniają na jego podkoszulce pastelowy napis. *Pride* — duma. I jeszcze — niezależność, wolność. Właśnie tak, bo Dan jest prawdziwym hakerem, który włamuje się do systemów komputerowych po to, by przełamać ich fatalną siłę. By pozbyć się przeszkód. Przekroczyć granice. I wreszcie gdzieś daleko odkryć ten lepszy świat. A jest na dobrej drodze... W jego domu — obok niezasłanego materaca, wciąż włączonego komputera i dziwacznego słupka, którym w chwilach błogości pieszczotliwie drapie swojego kota Flame’a — piętrzą się puste butelki po winie. Jest bowiem namiętnym kolekcjonerem markowych win. Podobno często puszcza kompakt z U2 i krąży po pokoju z na wpół wypalonym papierosem w ustach. Z butelki popija caberneta... Ale wyobrażam go sobie inaczej. Jak ścieli materac i wprowadza ład w swojej kalifornijskiej samotni, jak związuje niesforne loki, zmienia ubranie na bardziej uroczyste, na stole rozkłada biały obrus. Porusza się elegancko, swobodny, ale opanowany, uważa, by nie potrącić przypadkiem Flama’e, który snuje się wokół niego. Jeszcze tylko świeca, jedna, jedyna. I z szafy wyjmuje skrywany przed światem kieliszek firmy Riedel. Dopiero wtedy nadchodzi czas właściwy dla wina. Nalewa ostrożnie, z wyczuciem porusza kieliszkiem... Tajemniczo milczy. Chwilę wpatruje się w jakiś punkt za oknem... A potem — może zbyt gwałtownie — wstaje i zmierza w stronę szklanego monitora.

Chyba tak to wygląda. Inaczej nie stworzyłby przecież tak wyrafinowanego programu, aktualnie jednego z najgroźniejszych narzędzi hakerskich, który podważa sens hermetycznych systemów i sieciowych zabezpieczeń, z pełnym sarkazmem nazwany Satanem.

Prowokacyjna nazwa, jak sugeruje Wietse Venema, informatyk z Eindhoven University of Technology i współautor programu, była bardzo ważna. Opinie prasy europejskiej okazały się przychylne. Satan przyniósł Farmerowi międzynarodowy rozgłos.

Działanie programu jest równie przewrotne, co jego nazwa. Na czym polega? To proste — aby włamać się do systemu, trzeba znać luki tkwiące w jego zabezpieczeniach. Poznał je Farmer pracując nad Cops i w bazie danych Satana umieścił listę tych usterek. Z jednej strony pozwala ona badać i wynajdować słabe miejsca Sieci, których ochronę należałoby wzmocnić, z drugiej jednak — umożliwia bezproblemowe włamanie. Satan działa bowiem jak tradycyjny miecz obosieczny czy może lepiej — wąż pożerający własny ogon. Pozornie wzmacniając system, *de facto* obnaża jego słabość.



Mimo że program ten nie wpłynął zdecydowanie na poziom bezpieczeństwa Sieci, Farmer narobił sporo zamieszania, kiedy za pomocą nowej wersji Satana przejrzał bez pozwolenia około dwóch tysięcy stron WWW należących do banków, organizacji przydzielających kredyty, czasopism, agend rządowych oraz firm rozpowszechniających pornografię (ostatnie prześwietlił, gdyż ich działalność opierała się na pewnej i dyskretnej wymianie informacji) i w raporcie, który ukazał się w Internecie, doniósł, że w dwóch trzecich przypadków używano oprogramowania z wieloma usterkami, co mogło pozwolić hakerom amatorom na uszkodzenie danego miejsca w WWW. Nie opublikował wszakże listy adresów podatnych na atak, jednak podane informacje pozwalały na snucie domysłów co do adresów, o których pisał. Ponadto zastrzeżenia może budzić fakt, że testował zabezpieczenia cudzych serwerów bez zgody ich właścicieli. Jako że robił to w słusznym (załóżmy) celu, obyło się bez konsekwencji prawnych.

Oczywiście Dan jest jedyny w swoim rodzaju. Wciąż pełen entuzjazmu i zapału robi rzeczy, na które eksperci się nie ważą. Aktualnie pracuje nad nowym programem, który będzie poszukiwał słabych miejsc programów zabezpieczających i automatycznie ściągał odpowiednie poprawki. Przygotowując coraz doskonalsze metody obrony Internetu przed nieproszonymi gośćmi, Farmer daje tym samym wyraz niemal fatalistycznemu pragmatyzmowi. Jak mówi: „większość ludzi nie przywiązuje wagi do bezpieczeństwa systemu. Do pewnego stopnia nawet i o mnie można to powiedzieć. Stosuję standardowe zabezpieczenia, więc ciągle ktoś próbuje się włamać do mojej systemu. Ale takie jest życie i nawet jak wychodzę w nocy z domu, nie

zamykam drzwi na klucz, bo szkoda mi na to czasu. Wolę napić się wina. A system... Jeśli jest dobry, niech broni się sam!". Może dlatego jego ostatni raport podpisany został nowym adresem internetowym, symbolicznie schowanym za wirującym kołem yin/yang.

Wietse Venema

Venema jest pracownikiem Instytutu Technologicznego w Eindhoven w Holandii. To niezwykle utalentowany programista, który stworzył niejedno narzędzie określone mianem standardu przemysłowego. Był współautorem Satana i napisał program TCP Wrapper, stosowany do monitorowania przychodzących pakietów danych.

Linus Torvalds

We wczesnych latach dziewięćdziesiątych Torvalds zapisał się na zajęcia szkoleniowe obejmujące przybliżające działanie systemu Unix i języka C. Rok później sam zaczął tworzyć system na analogiczny do Uniksa, opublikowany nieco później w Internecie pod nazwą Linux. Dziś wokół Linuksa wytworzyło się coś w rodzaju kultu. Jest to jedyny system w historii napisany przez niezależnych programistów z całego świata — wielu z nich nigdy się nawet nie widziało. Linuksa nie chronią prawa autorskie w zakresie takim, jak w przypadku innych systemów operacyjnych.

Bill Gates i Paul Allen

Ci starsi panowie dwaj z Waszyngtonu programowali od lat licealnych, o czym już wcześniej wspomniałem. Posiadają ogromny talent i zaczynając w roku 1980, zbudowali największe imperium programistyczne na kuli ziemskiej. Do komercyjnych osiągnięć Microsoftu należą: MS-DOS, Windows, Windows 95 i Windows NT.

Robert Tappan Morris

Uczęszczał na studia doktoranckie na Wydziale Informatyki Uniwersytetu Cornell. Spokojny, sympatyczny młody człowiek ze stopniem magistra Uniwersytetu Harvarda nigdy nie miał nic wspólnego z przestępstwami czy z hakingiem. Ale nie był tak całkowicie wolny od słabości. Lubił bowiem wykrywać błędy w systemach operacyjnych...

Jesienią 1988 roku Morris zaczął pracować nad programem mającym na celu ukazanie wykrytych błędów w zabezpieczeniach systemu 4 BSD UNIX. Program, po „wpuszczeniu" w Sieć, miał wykazać możliwość uzyskania dostępu do dowolnego innego komputera i zainfekowania go wirusem. Czerw (*worm*), jak nazwano później program Morrisa, miał mniej niż 100 linii kodu. A jednak Robert pisząc go, popełnił drobny błąd, który kosztował bardzo wiele.

Czerw po uruchomieniu zajmował bardzo mało czasu procesora. Miał on pozostawać w ukryciu i być niezauważalnym nawet dla administratora. Morrisowi chodziło jedynie o udowodnienie, że może on się przenosić z komputera na komputer. „Rozmnażanie" możliwe było poprzez wykorzystanie błędów w kilku elementach systemu Unix oraz poprzez odkrywanie łatwych do odgadnięcia haseł użytkowników.

Morris przewidział, że nieskończone rozmnażanie się programu spowoduje zablokowanie komputerów. Dlatego też czerw „pytał się", czy infekowany serwer zawiera już kopię programu czy nie. To jednak mogłoby ułatwić administratorom pozbycie się programu, więc Robert zdecydował się, że mimo odpowiedzi „tak" w jednym na siedem przypadków czerw i tak będzie uruchamiał się na komputerze jako nowy proces. Miało to ograniczyć prędkość rozmnażania się programu i uniknąć blokady systemu. Obliczenia okazały się jednak błędne.

Mimo że czerw wymagał jeszcze kilku poprawek, niecierpliwy Robert zdecydował się wprowadzić go do Internetu 2 listopada 1988 roku około godziny 20:00. Aby ukryć fakt, że program jest jego autorstwa, uruchomił go z jednego z serwerów na uniwersytecie Harvarda.

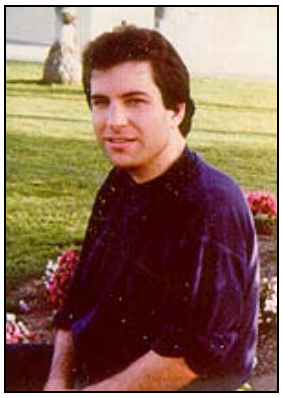
Czerw rozmnażał się powoli, ale sukcesywnie. Już w kilkanaście minut po uruchomieniu wiele komputerów zaczęło dotkliwie odczuwać jego obecność, a dwie godziny później, czerw uniemożliwił uruchomienie większości maszyn. Nie mogli sobie z tym poradzić nawet administratorzy. 3 listopada o godzinie 00:34 (czyli parę godzin później) obecność wirusopodobnego programu odkrył Andy Sudduth z Harvardu.

Kiedy Morris zorientował się, co się dzieje, wraz z kolegą opracował odpowiednie antidotum i rozesłał anonimowo po Sieci. Ale było już za późno. Czerw działał skutecznie. Nawet odebranie i przeczytanie listu nie było już możliwe.

Nad zwalczeniem złośliwego programu pracowali specjaliści z tysięcy placówek w USA. Już w 12 godzin od infekcji informatycy z Uniwersytetu Kalifornijskiego w Berkeley i z Massachussetts Institute of Technology odkryli metodę likwidacji. Ze względu na odłączenie wielu komputerów od Sieci dopiero 10 listopada udało się całkowicie przywrócić normalną pracę Internetu. Zainfekowanych zostało ponad 6000 komputerów klasy Sun 3 i VAX. Straty w każdej lokalizacji sięgały nierzadko 50 000 dolarów, a łączne oceniono je na około 10 000 000 dolarów.

Robert przyznał się do popełnionego błędu. Skazano go na 3 lata obserwacji sądowej, 400 godzin prac społecznych i grzywnę w wysokości 10 000 dolarów. Obecnie pracuje jako informatyk, ale nie zajmuje się kwestią bezpieczeństwa systemów. Wpadka kosztowała go zbyt wiele.

Kevin Mitnick — Condor



Kevin to bardzo ciekawa postać, o czym była już mowa wcześniej. Jego życie nie wygląda jednak zachwycająco, choć wciąż budzi on grozę. Strażnicy więzienni boją się dać mu do ręki jakiekolwiek urządzenie elektroniczne w obawie, że zrobi z niego bombę lub spróbuje za jego pomocą uciec. Sąd odmówił mu już kilkakrotnie zwolnienia za kaucją. Ma ograniczony dostęp nawet do biblioteki więziennej. Tak skończyła się hakerska kariera pewnego człowieka, który chciał lepiej żyć.

Jego ojciec Alan wychowywał się na przedmieściach Detroit w dość licznej, ubogiej rodzinie. Kilka lat później, podczas służby w wojsku został przeniesiony do Kalifornii, gdzie spotkał swą przyszłą żonę Rochelle. Po narodzinach potomka,

który otrzymał imię Kevin, państwo Mitnick przenieśli się do wielorodzinnego domu niedaleko Hollywood. Ale nawet blisko tej krainy snów, dzieciństwo Kevina nie przypominało filmu z happy endem. Gdy skończył trzy lata, jego rodzice rozwiedli się. Został z matką, która w tym czasie zaczęła pracować jako kelnerka. Dwa lata później znów wyszła za mąż na rok i jeszcze raz... W sumie burzliwe życie matki, źle wpływało na rozwój Kevina — został uznany za nadpobudliwego chłopca i zaczął zażywać lekarstwa — ritalinę i deksedrynę, które lekarz przepisywał mu do jedenastego roku życia. Poza tym cierpiał na chroniczne alergie, skarżył się na palpitację serca. Ale był to tylko efekt stresu i ciągłego niepokoju.

W miarę jak stawał się coraz starszy, coraz bardziej zamykał się w sobie. Nie pił, ani nie zażywał narkotyków. Z bólem egzystencjalnym radził sobie inaczej. Jadł. Jadł coraz więcej aż stał się otyłym, zakompleksionym nastolatkiem, który źle skrywał gniew. Oddalał się od świata. Rzucił szkołę średnią. Oddał się całkowicie życiu w wirtualnej przestrzeni.

Punktem zwrotnym w życiu Kevina był dzień 9 grudnia 1988 roku, kiedy to Lenny DiCicco doniósł na niego agentom federalnym. DiCicco dobrze go znał. Wiedział o niezwykłym talencie, ale przerażała go „ciemna strona księżyca" — podłość, mściwość, żądza odwetu, arogancja, nieopanowanie i przedziwna skłonność do kłamstwa przy jednoczesnym wymaganiu prawdomówności od innych. Kevin wydał mu się niebezpieczny.

Wcześniej całymi miesiącami „przesiadywali" w Easynet — wewnętrznej sieci komputerowej Digital Equipment. Chcieli dostać się do kodu systemu operacyjnego VMS, który był zainstalowany w milionach komputerów na całym świecie. Działając we dwójkę, włamali się do firmy DEC w Massachusetts. W tym czasie Mitnick pracował na dwóch komputerach jednocześnie (z jednego się włamywał, a drugiego używał dla zmylenia pogoni).

Długo próbowano ich namierzyć. Bezskutecznie. Może dlatego chłopcy stawali się coraz odważniejsi. Czytali pocztę specjalistów do spraw zabezpieczeń, włamywali się do coraz to nowszych systemów, słowem — zabawa była przednia. Jednak Kevin zaczynał popadać w coraz większą obsesję. Narzucał się kompanowi podczas pracy, stale pożyczał od niego pieniądze, żądał, by DiCicco wpuszczał go do biura, w którym pracował. Aż pewnego dnia DiCicco sprzeciwił się i zabronił Kevinowi korzystać z firmowych komputerów. Co zrobił Mitnick? Zadzwonił do szefa i przedstawiając się jako pracownik Służby Dochodów Państwa poprosił o wstrzymanie wypłaty dla DiCicco. Tego już było za dużo. DiCicco skontaktował się z kilkoma osobami z Digital, te zaś — z FBI i wszyscy razem stworzyli system obserwacji.

Scena ujęcia Mitnicka przypominała była dokładnie wyreżyserowana. DiCicco, zaopatrzony w miniaturowy przekaźnik radiowy, zaczął podczas hakowania rozmowę z Kevinem, a następnego wieczora zwabił Kevina do swojego samochodu, odczekał, aż wyjmie on swoją czerwoną torbę, w której miał niezbędne do „pracy" narzędzia i dał znać agentom, by przystąpili do aresztowania. Zjawili się natychmiast i po chwili podarowali Kevinowi „srebrną bransoletkę z łańcuszkiem".

Zaskoczony Mitnick spytał przyjaciela o powód. „Bo chciałeś mnie załatwić", odpowiedział krótko DiCicco. Kevina zabrano do Zakładu Karnego Terminal Island w San Pedro. Zatrzymano go w celi o szczególnym nadzorze, bez możliwości zwolnienia za kaucją. Sędzia określił go jako „wielkie, ale to wielkie zagrożenie dla społeczeństwa". Miał rację — firma DEC ogłosiła, że Kevin Mitnick naraził ją na straty w wysokości 4 000 000 dolarów.

Od typowego więzienia Kevin ustrzegł się dzięki adwokatowi, który wymyślił na jego potrzebę nową jednostkę chorobową: uzależnienie od komputera. Skazany na rok przesiedział więc połowę wyroku w Federalnym Obozie dla Więźniów w Lompoc, a resztę spędził w domu przejściowym.

Gdy przybył do Lompoc, był on pełen przestępców. Trzymał się z dala od innych. 8 grudnia 1989 roku (dokładnie w rok po aresztowaniu) Kevin wylądował w Beit T'Shuvah (z hebrajskiego „dom pokuty") znajdującym się w dzielnicy narkomanów i prostytutek — Ecgo Park w Los Angeles. Proponował on klasyczny program 12 kroków stosowanych przez anonimowych alkoholików. Rossetto, licencjonowana pracownica socjalna otwierała drzwi przed wszystkimi narkomanami, alkoholikami, nałogowymi hazardzistami. Tu właśnie Kevin miał się wyrzec swej potęgi przy klawiaturze i stać się zwykłym, przestrzegającym prawa człowiekiem. Czas wypełniał mu sztywny rozkład dnia, którego musiał rygorystycznie przestrzegać. Spotykał się z Rossetto, uczestniczył w sesjach grupowych. Chodził również na zebrania anonimowych łasuchów, przestrzegał diety, dużo czasu spędzał przy hantlach i rowerze treningowym. W tym czasie stracił 40 kilogramów.

Wszystko układało się dobrze aż do czasu, gdy zjawił się wuj Kevina — Mitchell Mitnick, człowiek o bardzo barwnej przeszłości, który zaczynając od handlu nieruchomościami, dzięki czemu zbił majątek, skończył na uzależnieniu od heroiny i kilku wyrokach. Przypływ nagłych uczuć rodzinnych odizolował ich od reszty grupy.

W ostatnim miesiącu półrocznego pobytu Kevina w domu przejściowym Rossetto skoncentrowała się na pomocy w znalezieniu mu pracy. Nie było to łatwe. Udało się co prawda, uzyskać zmianę warunków nadzoru policyjnego w sprawie używania komputera (nie mógł używać jedynie modemu), ale i tak żadna firma nie chciała zatrudnić człowieka pokroju Mitnicka. Złą sława wyprzedziła jego zdolności.

W tej sytuacji Kevin wraz z wujem zaczął pracować w firmie budowlanej swego ojca. Ale pracy starczyło tylko na kilka miesięcy. Przeniósł się więc wraz z matką do Las Vegas, chodził na kursy żywienia, tenisa i poradnictwa dietetycznego. Dostał pracę w przedsiębiorstwie Passkey Industries, gdzie wykonywał niezbyt skomplikowane prace na komputerze.

Sielanka nie trwała długo. Nadszedł zły okres w życiu Kevina. Znowu zaczęła prześladować go własna przeszłość. Stało się tak za sprawą książki „Cyberpunk", która opisywała wcześniejsze wyczyny Kevina i skutecznie likwidowała szansę na normalne życie. Z drugiej jednak strony, cały ten zamęt spowodował, że stał się znany. Jakieś pół roku po ukazaniu się książki Kevin wziął udział w konferencji zorganizowanej przez Digital Equipment Users Socjety, wpływową organizację skupiającą około 110 000 użytkowników na całym świecie.

Idąc na tę konferencję zamiary, miał jak najbardziej uczciwe. Znał system i wiedzą którą posiadał, chciał się podzielić ze specjalistami do spraw zabezpieczeń firmy Digital. Wypełnił więc kartę rejestracyjną używając swego prawdziwego nazwiska. Kiedy już wypełnił formularz okazało się, że nie podpisał „zasad zachowania się", które powinni byli podpisać wszyscy uczestnicy. Wychodząc wpadł na zaprzyjaźnionego konsultanta do spraw zabezpieczeń — Raya Kaplana, który zaproponował, że przedstawi go paru osobom. Następnego ranka wrócił do South Hall. Kiedy zgłosił się do rejestracji, czekało na niego trzech przedstawicieli DECUS-a. Jeden z nich poprosił Mitnicka o przedstawienie się, co ten uczynił bez oporu. Jak wspomina Kevin:

„Następnie poprosił o jakiś dowód tożsamości, więc wyciągnąłem kalifornijskie prawo jazdy. Popatrzył na mnie i powiedział:

— *Nie możesz w tym uczestniczyć.*
— *Dlaczego?*
— *Wiesz dlaczego — usłyszałem.*
— *Nie, nie wiem.*
— *Wiesz dlaczego".*

W tym momencie akredytacja Kevina na DECUS-ie została skonfiskowana. Choć Ray Kaplan próbował później interweniować u organizatorów, nie przyniosło to skutku. Kevin nie mógł wrócić. Nikt mu nie ufał.

Niecały miesiąc później Kevina dotknął następny cios. 7 stycznia 1992 roku jego dwudziestojednoletniego brata Adama znaleziono martwego w zaparkowanym samochodzie. Przyczyną śmierci było przedawkowanie heroiny. Kilka dni po pogrzebie spotkał Harriet Rossetto. Przyznał się jej, że wrócił do włamywania się. Ale na powrót do Beit T'Shuvah było już za późno.

Następnie za rekomendacją ojca zaczął pracować jako pracownik badawczy w firmie TelTec w Kalifornii, gdzie wykonywał nieskomplikowane i nudne prace na komputerze.

FBI wpadło na pomysł, aby do łapania hakerów wykorzystywać... hakerów. Zwerbowano Justina Petersona, który był ścigany za oszustwa pocztowe, komputerowe, kradzieże, ale posiadał również sporą wiedzę techniczną. Pomysł wypalił. Peterson pomógł złapać i odnaleźć komputer, na którym znajdowały się tajne informacje Kevina Poulsena. Kolejnym celem był Mitnicka. Kiedy latem 1992 roku Peterson zaczął namierzać Kevina, ten jeszcze nie otrząsnął się po śmierci Adama. Jako że nie udało się jeszcze ustalić, kto przyczynił się do tego, Kevin próbował sam odpowiedzieć na kilka pytań dzięki hakingowi. W tym czasie utrzymywał bliski kontakt z przyjaciółmi z dawnych lat. Peterson próbował się wkręcić w ich towarzystwo, ale nie trzeba było dużo czasu, by Kevin i Lewis zorientowali się, co jest grane. Bardziej ich to jednak rozbawiło, niż zaniepokoiło. We wrześniu 1992 roku FBI opierając się przede wszystkim na informacjach Petersona, zrobiło nalot na mieszkanie Kevina i DePayne'a. Albo Kevin miał szczęście, albo dostęp do bardzo tajnych informacji — nie było go w domu. W listopadzie wydano nakaz aresztowania pod zarzutem złamania postanowień warunkowego zwolnienia, polegającym na nielegalnym podłączeniu się do komputerów Pac Ball.

Śledztwo FBI skomplikowało się. Kevin nie tylko wywinął się z zastawionej na niego pułapki, ale ośmieszył biuro, demaskując ich współpracownika jako przestępcę. Nie skończył na tym. Prowadził dochodzenie, włamał się do komputerów DMV i poprosił o przesłanie dokumentów do punktu kserograficznego Kinko w Studio City.

We wrześniu 1985 roku Kevin zapisał się na zajęcia w centrum Kształcenia Komputerowego w Los Angeles. Wyglądało na to, że chce rozstać się z przeszłością i w jakiś sposób ukierunkować swą fascynację komputerami. Na zajęciach nauczył się nie tylko sprawności technicznych. Pewnego wieczoru podczas w pracowni komputerowej wdał się w e-mailową rozmowę z niewysoką, atrakcyjną brunetką, siedzącą po drugiej stronie sali. Zaprosił ją na kolację. Chociaż była już zaręczona, po miesiącu spotykali się już regularnie. Bonnie Vitello, była dwa lata starsza od Kevina, miała za sobą jedno małżeństwo i była o krok od drugiego. A jednak otyły i mrukowaty Kevin zaintrygował ją. Wydawał się całkiem miły, inteligentny. Roześmiał się głośno, gdy powiedziała mu, że pracuje w GTE, jednym z miejscowych przedsiębiorstw telefonicznych. A potem było jak w bajce — Bonnie zerwała zaręczyny i zamieszkała z Kevinem-„Claydem" w małym miasteczku Thousand Oaks. Ale on dale hakował. Wszedł nawet do systemu Narodowego Centrum Bezpieczeństwa Komputerowego, udając pracownika technicznego. To nie mogło pozostać bez echa.

Na tydzień przed planowanym małżeństwem mieszkanie Bonnie zostało przeszukane przez policję. Zajęty został komputer, modem, dyskietki i wszystkie podręczniki komputerowe. Kevin znowu narozrabiał — zabawił się oprogramowaniem przedsiębiorstwa programistycznego Santa Cruz Operation, które wyprodukowało jedną z wersji systemu operacyjnego Unix, dostosowaną do pracy na komputerach osobistych. Administratorzy systemu obawiali się, że mógł ukraść należącą do nich niekomercyjną wersję programu. Z punktu widzenia Santa Cruz Operation sytuacja

była poważna, gdyż w grę wchodziły setki tysięcy dolarów, nie mówiąc już o reputacji przedsiębiorstwa. SCO próbowała więc dogadać się z Mitnickiem, przyznano mu nawet własne hasło i postanowiono nie podawać sprawy do sądu, a wszystkp to w zamian za informacje o metodzie włamania. Targ się nie udał. W końcu powiadomiono o poczynaniach Mitnicka policję. Odszukanie w Thousand Oaks adresu Bonnie, skąd dokonywano połączeń telefonicznych nie było trudne.

Aż do tej chwili Kevin miał czystą „dorosłą" kartotekę. Jednak został oskarżony o bezprawne wejście do komputera i za karę otrzymał 36 miesięcy nadzoru sądowego. Musiał też zgodzić się na spotkanie z operatorem systemu Santa Cruz Operation, który poznać znalezione przez Kevina „dziury" w ich systemie zabezpieczeń. Tak to się skończyło.

Kevin i Bonnie pobrali się 9 czerwca 1987 roku w Woodland Hills. Aby trochę zaoszczędzić, przeprowadzili się do małego mieszkania jej matki. Bonnie pracowała w GTE, a Kevin spędzał całe dnie na poszukiwaniu odpowiedniego zajęcia. Wydawało się, że chce zbudować sobie przyszłość. Wysyłał dziesiątki listów z pytaniami o pracę, a w załączonym życiorysie wyszczególniał, jak i gdzie zdobywał doświadczenie, wymieniał całą masę systemów operacyjnych, którymi potrafił się posługiwać (VM/CMS, OS/VS1/DOS/VSE, MS-DOS, RSTS/E, VAX/VMS, Unix), a w rubryce cele wpisywał „kariera programisty komputerowego". Z pomocą Bonnie został w październiku 1987 roku przyjęty do GTE, ale już po tygodniu znana była jego przeszłość i stracił pracę. Kilka miesięcy później szczęście znów uśmiechnęło się do niego. Złożył podanie o pracę w charakterze konsultanta do spraw elektronicznych przelewów bankowych w Security Pacifik Bank. Zgodnie z poleceniem wypełnił formularz swoim wielkim, niestarannym pismem, przypominającym bazgroły dziecka. Czy zrobił to z rozpaczy czy chciał wprowadzić w błąd ewentualnych pracodawców nie wiadomo, dość że w rubryce z pytaniem o to, czy był karany, odhaczył odpowiedź — nie. Ku swojemu zaskoczeniu otrzymał z sekcji osobowej banku list z wiadomością, iż otrzymał pracę. Był szczęśliwy. Miał zarabiać 34 000 dolarów rocznie! I miała to być pierwsza dobrze płatna praca w jego życiu. Ale wyprzedziła go zła sława. Donn Parker, konsultant do spraw zabezpieczeń w SRI dowiedział się, że Kevin ma zostać przyjęty do pracy w banku i złożył stosowne oświadczenie. Jim Black detektyw z wydziału policyjnego Los Angeles zajmujący się przestępstwami komputerowymi, zrobił to samo. Dzień po rozpoczęciu pracy, oferta zatrudnienia została wycofana. Ale sprawa nie była zakończona. Przynajmniej nie dla Mitnicka.

Któregoś dnia Donn Parker podniósł słuchawkę telefonu w swoim biurze w SRI i usłyszał: „cześć Donn, mówi Kevin Mitnick". Zaniemówił z wrażenia, ale po paru minutach rozmowy zdał sobie sprawę, że Kevin szuka nie zemsty, ale zatrudnienia. Kevin mówił tonem profesjonalisty, był uprzejmy i tryskał humorem. Wiele wiedział o pracy, którą Parker wykonywał — o kontroli zabezpieczeń informacji wykonywanych na zlecenie różnych przedsiębiorstw i o badaniach nad przestępczością komputerową prowadzonych na zlecenie Departamentu Sprawiedliwości. I nie było nic dziwnego w tym, że Kevin zadzwonił. Parkera był swego rodzaju patronem młodych hakerów i jeśli kogoś polubił, mógł mu znaleźć posadę wysokopłatnego konsultanta do spraw zabezpieczeń. Ta reputacja w większości okazała się mitem.

Czasami zatrudniał dzieciaki o niezwykłych zdolnościach komputerowych, ale wymagał czegoś więcej od fantazji i pustych słów. I kiedy Kevin zapytał, czy pomoże mu znaleźć pracę w SRI w charakterze konsultanta do spraw bezpieczeństwa danych, odmówił. W zamian doradził mu powrót do szkoły i zdobycie dyplomu z nauk komputerowych albo administracji handlowej.

Kevin wysłuchał tego bez protestów, podziękował Parkerowi za radę, a potem pożegnał się i odłożył słuchawkę.

Trzeba było wrócić do przeszłości. Jeszcze w 1978 roku Lewis DePayne (pseudonim „Roscoe") skontaktował się z Kevinem za pomocą amatorskiego radia, gdyż usłyszał, jak ktoś przechwala się, że wykonał nielegalne połączenie międzymiastowe, używając wykradzionych kodów przedsiębiorstwa telefonicznego MCI. Spotkali się wtedy i zaczęli wymieniać informacje. Kevin miał 14 lat, ale jego umiejętności budziły respekt. W tamtych czasach nikt nie strzegł dostępu do sieci telefonicznych. Można było dzwonić za darmo w dowolne miejsce na świecie. W tych wczesnych latach Kevin i Lewis razem z Susan Headly i Rhoadesem planowali swe przygody w pizzeri Shakeya w Hollywood. Później Mitnick często używał swych phreakerskich umiejętności, gdyż pozwalały mu one na swobodne korzystanie z dostępu do komputerów przez modem. Swobodne, czyli nie tylko darmowe, ale i bezpieczne, bo wielokrotnie sprawdzano, skąd dzwoni włamywacz i znajdowano jedynie puste mieszkania, nieczynne biuro, lub Bogu ducha winną rodzinę. Kevin zacierał ślady zmieniając numer telefonu, z którego się łączył.

Kiedy około 1980 roku przedsiębiorstwa telefoniczne zaczęły wymieniać mechaniczne łącznice telefoniczne na centrale komputerowe, Kevin ze znajomymi, również przeszli na systemy cyfrowe. Wymagało to wielkiego skoku jakościowego, ale i przyjemności rosły kilkakrotnie. A później odkryli Arpanet..

Jednak to potyczki z Tsutomu doprowadziły do trwałego zatrzymania hakerskiej działalności Kevina Mitnicka. Pod wieloma względami byli do siebie podobni — łatwiej nawiązywali kontakt z maszyną niż z innym człowiekiem, byli inteligentni, zarozumiali i — co najbardziej znamienne — obydwaj mieli wyraźne tendencje do popadania w obsesję.

Tsutomu Shimomura w Boże Narodzenie nie było w domu. Jego zastępca w San Diego Supercomputer Center Andre Gross, który spędzał święta z rodziną w domu w Tennessee, w pewnym momencie postanowił sprawdzić swoją pocztę elektroniczną, gdzie rutynowo otrzymywał pliki raportowe zapisujące wszystko, co się działo w komputerze Tsutomu. Zaskoczyło go, że zamiast się wydłużać, raporty były coraz krótsze.

Zaniepokojony Gross natychmiast zadzwonił do Tsutomu. Obaj wiedzieli, co to znaczy — ktoś włamał się do komputera.

Tymczasem Kevin zmienił miejsce zamieszkania. Wynajęte mieszkanie składało się z jednego pokoju z małą łazienką i kuchnią, ale było ładnie wyposażone, jasne, czyste i przytulne. Jak widać, nie przykuwało całej uwagi Kevina.

Po rozpoznaniu ataku Tsutomu powiadomił kolegów. Wydarzenie to nie przysporzyło mu chwały jako specowi od zabezpieczeń komputerowych. Ale przypuszczał, kto się za tym kryje.

Jego wściekłość wzrosła, gdy odkrył, że intruz wykradł mu setki megabajtów plików osobistych i poczty elektronicznej, narzędzia zabezpieczające dostęp do danych, programy obsługujące telefony komórkowe oraz kopię napisanego przez Tsutomu programu Berkley Packet Filter — narzędzia do prowadzenia komputerowej obserwacji napisanego na zamówienie Narodowej Agencji Bezpieczeństwa. Następnego ranka Tsutomu był już w samolocie do San Diego, gdzie próbując odtworzyć przebieg ataku, rozpoczął trudny proces analizy rejestrów komputerowych. W swoim domu zastał elektronicznie zniekształconą pocztę głosową (ktoś groził mu i wyśmiewał się z niego i jego narodowości, nazywając mistrzem kung-fu). Tsutomu zminiał nagranie na plik i udostępnił w Internecie. Podziałało! Za kilka dni tajemniczy głos odezwał się ponownie: „niełądnie mój synu... jestem bardzo rozczarowany".

Początek stycznia Tsutomu spędził na wyjaśnieniu metody, jaką posłużył się włamywacz. Był to IP — spoofing — znany już wcześniej, ale tu po raz pierwszy wykorzystany w praktyce. Tsutomu „pozatykał" luki w systemie bezpieczeństwa i wrócił w góry. Nie na długo. W „New York Times" ukazał się bowiem artykuł Markoffa poświęcony włamaniom. Przedstawiał Tsutomu jako nowego bohatera, który wreszcie złapie hakera. Zdjęcie Shimomury opublikował także „Newsweek". Tsutomu jawił się jak ktoś niezwykły — długowłosy, opalony, wysportowany facet z wykształceniem neurochirurga, genialny fizyk i haker stojący po stronie prawa. A przecież nie był bohaterem, lecz ofiarą ataku.

27 stycznia w czasie rutynowej kontroli systemu w WELL zauważono duży przyrost plików na jednym z kont. Znaleziono na nim dane, które pochodziły z komputera Tsutomu. ponadto była tam jeszcze lista 20 000 numerów kart kredytowych.

Zdecydowano tymczasem nie zatykać dziur w systemie bezpieczeństwa. Bowiem Tsutomu postanowił zmienić reguły gry i złapać Kevina Mitnicka. Tak rozpoczęło się elektroniczne polowanie. Pracownicy FBI byli przekonani, że Kevin znajduje się w okolicach Denver, ale kiedy sprawdzali, skąd się loguje odkryli, że z kontem, którego użył do włamania się do komputera Tsutomu o nazwie „gkremen" łączy się z telefonów rozsianych po całym kraju. Niektóre z połączeń pochodziły z Minneapolis, inne z Denver, ale większość była realizowana z Raleigh. Obszar poszukiwań zawężył się więc. Udało się określić numer, z którego korzystał Mitnick, ale po jego wykręceniu słychać było słychać jedynie trzaski.

Zaczęło się więc monitorowanie wszystkich połączeń z NetCom i WELL, zapisywanie podejrzanych rozmów na IRC-u. Tsutomu analizował połączenia do NetComu. Kiedy wiadomo już było, skąd dzwonił Mitnick, Tsutomu wraz z Markoffem wsiedli do minivana wypełnionego elektroniką. Mieli do dyspozycji antenę kierunkową, która zastępowała używany do tej pory przez Tsutomu nielegalnie przerobiony telefon komórkowy z możliwością podsłuchu. Zlokalizowany został dom, w którym ukrywał się uciekinier. Sporo czasu zajęło ustalenie numeru mieszkania. Nawet wydany nakaz przesłuchania nie posiadał wpisanych numerów domu i ulicy.

Tymczasem napięcie rosło coraz bardziej, na miejscu znajdowało się pięciu wezwanych wcześniej funkcjonariuszy Oddziału Specjalnego do Walki z Groźnymi Przestępcami na Okręg Wschodni Karoliny Północnej (w tym zastępca szeryfa federalnego Mark Chapman). Chcieli oni dokonać aresztowania, ale nikt z zespołu monitorringu elektronicznego nie potrafił wykryć jakiejkolwiek aktywności telefonu Kevina. Nie zdarzyło się coś takiego ani razu, gdy prowadzili nasłuch. Czyżby Mitnick wyczuł, co się dzieje i zniknął?

Spekulacji nie przerwał nawet powrót Kevina, który u bram swojego domostwa stanął tuż po północy. Przyznał się później znajomemu, że poszedł po prostu zjeść kolację na mieście. Ale jak udało mu się wyjść z mieszkania będącego pod obserwacją sześciu policjantów, pozostanie na zawsze tajemnicą. Więcej — wrócił też niezauważony i dopiero, kiedy przystąpił do „pracy" niedługo po północy, technicy znowu próbowali za pomocą ręcznego detektora ustalić, w którym mieszkaniu się znajduje. Dwóch z nich jakimś trafem znalazło się na parterze budynku 4504 w tej chwili, gdy na piętrze ktoś otworzył drzwi. Twierdzili później, że u góry zobaczyli osobę odpowiadająca rysopisowi Kevina, wychodzącą z mieszkania i rozglądająca się wokół. Kevin stanowczo temu zaprzeczał, ale policjanci nie mieli już żadnych wątpliwości. Wiedzieli, które mieszkanie zajmował. Kilku ludzi z FBI i Oddziału Specjalnego zebrało się przed drzwiami. Kevin wspomina:

„Ktoś zastukał.

— Kto tam? — zapytałem.
— FBI — brzmiała odpowiedź".

Mimo, iż w serce Kevina musiał uderzyć piorun strachu, wydawał się całkiem spokojny i przez kilka minut rozmawiał z agentami przez zamknięte drzwi. Upierał się, że nie jest Kevinem Mitnickiem i nie wie, o czym mówią. W pewnej chwili uchylił drzwi. Miał przy uchu telefon komórkowy i najwidoczniej z kimś rozmawiał. Gdy

funkcjonariusz zapytał, czy może wejść, Kevin zażądał okazania nakazu rewizji. Dalej zeznania na temat tego, co zdarzyło się dalej są znowu niezgodne. Kevin twierdzi, że próbował zamknąć drzwi, które jeden z agentów zastawił mu nogą, ten natomiast mówi, że Kevin wpuścił ich bez oporu. W środku zobaczyli komputer. Sprawdzili, czy w mieszkaniu nie ma broni, a następnie zrewidowali gospodarza. Miał na sobie sportowy dres i adidasy. Poproszono go o podanie imienia i nazwiska. „Thomas Case" — usłyszeli w odpowiedzi.

Pokazał im wydane w Kalifornii Północnej prawo jazdy, kartę kredytową i książeczkę czekową, wszystkie na to samo fałszywe nazwisko. Kiedy szukał czegoś w portfelu, policjanci zauważyli, że znajduje się tam parę innych dowodów tożsamości. Kevin odłożył portfel na stolik, jeden z nich podniósł go i zajrzał do środka. Kevin twierdzi, że policjanci zaczęli przeszukiwać mieszkanie, chociaż działo się to wbrew jego woli. Pozwolono mu jednak zadzwonić do adwokata. Kilku policjantów zostało jednak na miejscu, by mieć Kevina na oku. Chciał zadzwonić do mamy, ale agenci odmówili. Poprosił o lekarstwo — jego odwieczne problemy z żołądkiem nasiliły się. Przyniesiono mu je. Kilka minut później jeden z agentów wrócił z nakazem aresztowania. Ale Kevin nadal utrzymywał, że nazywa się Thomas Case, więc nakaz jeszcze ciągle nie miał mocy. Dopiero, kiedy Burns zadzwonił do sędziego Dixona, otrzymał ustne upoważnienie do przeprowadzenia przeszukania. Poprawny adres i numer mieszkania zostały dopisane ręcznie w górnym rogu.

Przeszukanie mieszkania zajęło agentom godzinę. Zajęli około 80 przedmiotów, w tym laptop Toshiby, telefony komórkowe i różne urządzenia do ich obsługi. Dopiero po trzeciej nad ranem przewieziono Kevina Mitnicka do Centrum Bezpieczeństwa Publicznego, znajdującego się w centrum Raleigh. Jadąc tam, wielokrotnie prosił o możliwość skontaktowania się z matką. Nie chciał podać agentom jej nazwiska, ani powiedzieć, jakie nazwisko podać, gdy spyta, kto dzwoni. W dalszym ciągu upierał się, że aresztowali nie tego kogo szukają, gdyż nazywa się Thomas Case i nie ma pojęcia dlaczego zabierają go do aresztu. Dopiero po wielu godzinach zaprzeczeń, dotarło do niego, że tym razem nie uda mu się wywinąć. Przyznał się.

Media były bardzo szczęśliwe, mogąc dostarczyć żądanego symbolu cybernetycznego bandyty.... Trafiło na żydowskiego chłopaka o skomplikowanym życiorysie z Panorama City. Ci, którzy go ścigali, zostali milionerami (Markoff i Tsutomu mieli szczególne powody do radości, bo otrzymali po 750 000 dolarów zaliczki za napisanie książki o Mitnicku, która miała okazać się bestsellerem oraz prawie 2 000 000 dolarów za scenariusz do filmu na ten sam temat). Bohater tych zdarzeń natomiast ubrany w pomarańczowy kombinezon skończył za kratkami. Był oskarżony o popełnienie 23 przestępstw.

Jednak w czerwcu 1995 roku w zamian za przyznanie się do pojedynczego przypadku oszustwa popełnionego w Karolinie Północnej za pomocą urządzenia łącznościowego, sąd odstąpił od ścigania go za pozostałe 22 wykroczenia. Otrzymał karę ośmiu miesięcy więzienia i zesłany został do Centralnego Aresztu Miejskiego w Los Angeles. Czekają go jeszcze procesy z oskarżeń wytoczonych przeciwko niemu w Seattle, San Jose i Denver.

Z więzienia wyszedł po niecałych pięciu latach. Od razu udzielił wywiadu magazynowi „Y-LIFE". Ale nie zaczął się jeszcze dla niego czas przyjemności. Nie wolno mu dotknąć ani użyć klawiatury, aż do 20 stycznia 2003 roku ma zakaz konsultowania czy doradzania jakiejkolwiek grupie lub osobie prywatnej w sprawach komputerowych. Nie wolno mu też podjąć jakiejkolwiek pracy w firmie telekomunikacyjnej piszącej oprogramowania. To chyba gorsze niż więzienie, bowiem Kevin ma zakaz wykonywania pracy, do której jest stworzony.

W wywiadzie udzielonym „Y-LIFE" wspomina jak na początku lat 90. musiał stworzyć sobie nową tożsamość, próbując ominąć pułapki. Przyznaje, że nie było to trudne, gdyż wystarczyło znać numer ubezpieczenia, który zawiera ogromną liczbę danych. Teraz ludzie dzielą się nimi na stronach internetowych, czyli dostęp do tego typu informacji jest jeszcze łatwiejszy. Swoją przestępczą działalnością Kevin Mitnick ukazywał niebezpieczeństwa płynące z dostępu do informacji, wskazywał luki, które należałoby zabezpieczyć przed naprawdę groźnymi przestępcami.

Kevin Mitnick przedstawia siebie jako człowieka, któremu nigdy nie ufano i nie dano szansy na to, by wykorzystał swoją wiedzę i doświadczenie we właściwym kierunku. Zawsze bowiem borykał się z brakiem pracy, a jeśli już udało mu się znaleźć zatrudnienie, to i tak po bardzo krótkim czasie był postrzegany jako przestępca. Teraz jednak wyobrażenie o nim uległozmianie i duża część młodych hakerów podziwia go. Otrzymuje ogromną ilość e-maili przesyłanych na e-konto, sponsorowane przez stronę *2600.com*. Firma drukuje te wiadomości i przesyła Kevinowi normalną pocztą (nie wolno mu zbliżać się do klawiatury).

Kevin Mitnick wyjawił także sekrety hakowania, opowiadając o nich na konferencji Giga Research. Właśnie wtedy postanowił podzielić się swoją wiedzą na temat sposobów włamań do komputerów. Tłumaczył więc informatykom i menadżerom odpowiedzialnym za bezpieczeństwo wielkich korporacji, jak złapać intruza próbującego wtargnąć do firmowej sieci.

Parę miesięcy po jego wyjściu z więzienia sąd zapoznał się z mnóstwem ofert pracy skierowanych do byłego hakera i wyraził zgodę na przyjęcie niektórych z nich. Mitnick otrzymał ponadto prawo wypowiadania się w programach telewizyjnych na temat bezpieczeństwa Sieci, może pracować jako konsultant do spraw technicznych, a także pisać artykuły do czasopism zajmujących się problematyką Internetu.

Kevin Poulsen

Niepozorny pracownik supermarketu Hugh's w Van Nuys w Kalifornii był wielkim fanem amerykańskiego odpowiednika programu telewizyjnego „997" — „Unsolved Mysteries". 11 kwietnia 1991 roku rozpoznał przedstawianego kilka dni wcześniej w programie przestępcę. Rzucił się więc na 24-letniego mężczyznę, który kupował prezerwatywy. Obezwładnił go i zawołał powiadomionych wcześniej, czekających już przed sklepem agentów federalnych. Tak wyglądało ujęcie Poulsena.

Podobnie jak Kevin Mitnick, uwielbiał on zabawiać się centralami telefonicznymi i robić dowcipy niczego nie spodziewającym się, przypadkowym ludziom. Zapytany o to, czy żałuje swoich czynów odpowiadał, że żałuje jedynie tego, iż pewnej nocy wybrał się do supermarketu po prezerwatywy.

Dysponujący nieprzeciętnymi umiejętnościami Poulsen był określany jako „24-godzinny haker". Pracował jako asystent programisty, włamując się w celu przetestowania bezpieczeństwa do systemów Pentagonu. Ale po godzinach szalał już na własną rękę — podsłuchiwał prywatne rozmowy aktorek, włamywał się do komputerów wojskowych, podglądał akta procesu FBI przeciwko Ferdynandowi Marcosowi (byłemu prezydentowi Filipin).

Po raz pierwszy został oskarżony w 1989 roku. Zarzuty dotyczyły 19 przypadków oszustw, włamań do systemów telefonicznych i wyłudzenia pieniędzy. Głównym argumentem było jednak... szpiegostwo. W czasie hakerskich eskapad po komputerowych łączach Poulsen niechcący dobrał się bowiem do planów bojowych sił lotniczych USA.

Jednak uniknął aresztowania i ukrywał się przez 18 miesięcy, rozwijając stale hakerskie umiejętności. Jego największym popisem było... wygranie dwóch Porsche 944 w konkursie radiowym. A wyglądało to tak.

Stacja radiowa KIIS-FM w Los Angeles, która słynęła z prowadzenia konkursu „Win a Porsche by Friday", w każdy piątkowy poranek informowała słuchaczy o sekwencji piosenek, po usłyszeniu której należy zadzwonić pod wyznaczony numer. Aby wygrać samochód wystarczyło być 102-gą z kolei osobą dzwoniącą do stacji.

Poulsen z kolegami zablokowali centrale Pacific Bell tak, że dzwonić do niej nie mógł nikt inny tylko oni. Udało im się to zrobić aż cztery razy pod rząd. W dwóch przypadkach wygraną był samochód Porsche 944, raz spora suma pieniędzy, a kiedy indziej wycieczka na Hawaje, na którą Kevin wysłał swoją siostrę.

Całe oszustwo było perfekcyjnie zaaranżowane — posługujący się fałszywymi dokumentami Kevin — znany także jako Walter Kovacs, John Osterman — był tak przekonywujący, gdy po raz któryś z kolei cieszył się z wygranej, że kierownictwo stacji dowiedziało się o oszustwie dopiero od policji...

Nie mogąc odnaleźć Poulsena, FBI pokusiło się o pomoc telewidzów. Wykroczenia Kevina zostały przedstawione w bardzo mrocznym świetle w programie „Unsolved Mysteries". Określono go jako maniakalnego przestępcę, potrafiącego dokonywać cudów za pomocą komputera.

Po aresztowaniu znalezione zostały dowody w postaci urządzeń przypominających akcesoria Jamesa Bonda, a także wydruków tajnych dokumentów schowanych w wykupionej skrzynce pocztowej. Nawet będąc już pod obserwacją policji, Kevin nie próżnował. Kilkukrotnie próbował dostać się do systemu komputerowego i skasować wszystkie materiały dowodowe, jakie FBI zgromadziło przeciwko niemu. Jak widać — bez powodzenia.

W czerwcu 1994 roku Poulsen przyznał się do siedmiu wykroczeń (oszustwa komputerowe, pocztowe i telefoniczne, wyłudzenia pieniędzy i zakłócania porządku publicznego), a rok później został skazany na 51 miesięcy pozbawienia wolności i ponad 56 000 dolarów grzywny. Była to największa dotychczas kara za przestępstwa tego rodzaju.

Christopher Matthew Lamprecht

Minor Threat, czyli Niewielkie Zagrożenie, to pseudonim, który mówi sam za siebie. Bo tak postrzegał swoją działalność ten 24-letni, mizerny i fajtłapowaty młodzieniec, który wylądował w 1995 roku za kratkami wbrew pozorom nie za hakowanie, lecz za wyłudzanie pieniędzy. W rzeczywistości był winny wykradania, wywożenia do innego stanu i sprzedawania układów elektronicznych dla central telekomunikacyjnych.

Kiedy dowiedział się, że spędzi w więzieniu 5 lat, a przez następne trzy nie wolno mu będzie korzystać z komputera z modemem, rozpłakał się. Parę miesięcy później zażył 99 tabletek nasennych i zemdlał podczas rozmowy telefonicznej ze swoją matką. Został odratowany. Ale...

Hakerska kariera Lamprechta rozpoczęła się we wczesnej młodości. Już wtedy świat cyberprzestrzeni wydawał mu się bardziej rzeczywisty od realnego. Wyrósł w mieście wielkich firm komputerowych (Austin), gdzie swoje biura mają tacy giganci jak IBM, AMD, Motorola czy Dell. Stał się handlarzem części elektronicznych, zamiast stać się handlarzem narkotyków. Bo innych perspektyw nie miał. Pochodził z rozbitej rodziny, był synem alkoholika, który wychowywany wraz z młodszą siostrą przez samotną matkę, szybko musiał dorosnąć.

Jak dla wielu zagubionych młodych ludzi, świat komputerów był dla niego ucieczką od smutnej rzeczywistości. Pierwsze próby podejmował usiłując zmienić swoje stopnie w szkolnych systemach komputerowych. Potem zajął się piractwem, uczestnicząc w dystrybucji nielegalnych kopii gier wraz z grupą znaną jako Public Enemy. Następnie przyszły dni phreakingu, kiedy wraz z siostrą dzwonił za darmo po całym świecie — do Watykanu, do pałacu Buckingham w Anglii i rozmawiał ze strażnikami. W tym też czasie napisał jeden z bardziej znanych na świecie programów do testowania możliwości połączenia się z innym modemem (tzw. war-dialer) o nazwie ToneLoc. Zmieniał nagrania na prywatnych automatach zgłoszeniowych, a nawet groził prezydentowi USA na linii konferencyjnej. Te większe i mniejsze przewinienia uchodziły mu na sucho.

Kłopoty zaczęły się, kiedy Chrisowi przestały wystarczyć dawki adrenaliny, jakie powodowało włamywanie się do systemów komputerowych w cyberprzestrzeni. Po nocach wkradał się więc do laboratoriów komputerowych, aby pograć w niewydane jeszcze wersje gier czy przetestować nowoczesny sprzęt komputerowy. Jego częstym celem były laboratoria firmy telekomunikacyjnej Southwestern Bell.

Lamprecht łatwo ulegał wpływom. W BBS-ie o nazwie Pentavia poznał złodzieja z talentami hakerskimi — Jasona Copsona, stosującego pseudonim Scott Berry. Traktował go jak najwyższy autorytet. I to właśnie Jason namówił go na kradzież sprzętu elektronicznego z odwiedzanych laboratoriów, a następnie sprzedaż poza granicami stanu. We czwórkę — Lamprecht, Copson oraz David Querin i Mike Dailey okradali centrale telefoniczne i — jako „Berry Associates" — sprzedawali części firmom handlującym urządzeniami elektronicznymi. W lipcu 1992 roku Lamprecht i Copson zostali złapani, kiedy próbowali sprzedać skradzione układy handlarzowi z Austin. Copsona odesłano do stanu Virginia, gdzie był poszukiwany za inne wykroczenia, zaś Lamprecht odsiedział pięć miesięcy w więzieniu i znalazł się pod nadzorem kuratora. To jednak nie zraziło Chrisa i kolegów — firma „Berry Associates" nadal działała, wspomagana przesyłanymi przez Copsona instrukcjami (przekazywanymi za pomocą kodu lub samodzielnie montowanych przez Jasona urządzeń blokujących podsłuch). Za to po opublikowaniu na kilku BBS-ach nazwiska, adresu i numeru ubezpieczenia społecznego człowieka odpowiedzialnego za ujawnienie „Berry Associates" policji, Massengale przez dłuższy czas musiał borykać się z dziwnymi kwotami obciążającymi jego karty kredytowe. W lutym 1994 roku mieszkający z Chrisem David Querin włamał się dla zabawy do komputerów Texas Racing Commision. Jako, że jego talenty hakerskie nie były zbyt rozwinięte, policja odkryła fakt, że włamania dokonano z mieszkania Lamprechta. Znaleziono tam ponadto torby wypełnione skradzionymi częściami. I Lamprecht trafił znów przed oblicze sądu, gdzie tym razem postawiono mu zarzut o wyłudzanie pieniędzy i skazano na 70 miesięcy pozbawienia wolności oraz 3 lata obserwacji bez możliwości dostępu do Internetu.

Decyzja ta spotkała się z ogromną krytyką opinii publicznej. Zarzucano wymiarowi sprawiedliwości bezsensowne postępowanie, uniemożliwiające więźniom rehabilitację. Przy dzisiejszym tempie rozwoju technologii Lamprecht po wyjściu z więzienia może nie dostać nawet pracy w McDonalds, bo i tam będą już komputery z modemami. Ale wszystko wskazuje na to, że decyzji sądu nie uda się zmienić. Mimo wielokrotnych prób Chrisa i jego adwokatów listy wysyłane do różnych instytucji i organizacji nie przyniosły na razie zamierzonego efektu. Nawet próby współpracy, polegające na ujawnieniu tajników dokonywanych włamań (co pomogło lepiej zabezpieczyć systemy w atakowanych firmach), spełzły na niczym.

Tak więc wszystko wskazuje na to, że Niewielkie Zagrożenie wyjdzie na wolność za niecałe dwa lata, lecz na prawdziwą dla niego wolność, wolność w świecie cyberprzestrzeni, przyjdzie mu czekać jeszcze pięć lat.

Ehud Tanennaum

Wydawałoby się, że na Bliskim Wschodzie kryminaliści traktowani są bardziej brutalnie i surowo niż w USA. A jednak izraelscy hakerzy zamiast przesiadywać latami w więzieniach, ukazują się w reklamach, podpisują kontrakty książkowe i filmowe. Przykładem tego może być „Analyzer". Ten wybitnie uzdolniony w branży komputerowej osiemnastolatek jest częściowym dyslektykiem. Interesuje się naukami ścisłymi i większość wolnego czasu spędza przy komputerze.

Gdy go zatrzymano, w mediach rozpętała się prawdziwa burza. Ale nie trafił do więzienia, ponieważ nałożono na niego jedynie areszt domowy. Niedługo potem zaczął jednak na swojej sławie zarabiać pieniądze, gdy „Yiedioth Ahronoth" (największy dziennik Izraela) opublikował reklamę firmy komputerowej EIM z jego udziałem. Następnie EIM podpisało z Tenenbaumem długoterminowy kontrakt, na mocy którego w przyszłości również będzie występował w ich reklamach. Zaoferowano mu także możliwość wystąpienia w wywiadach w USA oraz sprzedaż swojej historii na potrzeby książki lub filmu. Z tego powodu warto pokrótce przedstawić dzieje Analizera.

Krótka kariera

Ehud zajmował się hakingiem przez dwa lata. Miał dostęp do ponad 1000 serwerów. Ale większość włamań kończyła się jedynie na uzyskaniu dostępu, gdyż nie interesowała go nigdy zawartość hakowanych wojskowych serwerów. Wybierał je tylko dlatego, że były dobrze chronione. Udało mu się nawet włamać do witryn parlamentu izraelskiego. Jedynym celem było publiczne ogłoszenie wsparcia dla ówczesnego prezydenta Ezera Weizmana oraz sugestia, aby witryna była częściej aktualizowana.

Cała trójka (bo działał wraz z przyjaciółmi) wpadła po tym, jak Makaveli i TooShort, korzystając z haseł odkrytych przez Analyzera, włamali się do kilku serwerów w domenach .mil i .gov. Reakcja FBI była oczywista. Do walki z hakerami zaangażowano ponad czterdziestu agentów. W rezultacie złapano wystraszonych nastolatków. Analyzer, który także włamywał się do serwerów Pentagonu, nie krył się ze swoimi wyczynami.

Walka o słuszną sprawę

W przeciwieństwie do większości hakerów, których popisy można określić jako chęć szpanowania, Analyzer to „haker z przesłaniem". Jego celem były wielokrotnie witryny organizacji terrorystycznych oraz strony z materiałami ocierającymi się o pedofilię. To właśnie niszczeniu takich serwerów poświęcał najwięcej czasu. W jednym z wywiadów oświadczył, że:

„Neonaziści grożą Żydom, zaś pedofile podniecają się zdjęciami dzieci. Są bardzo dumni ze swoich witryn, więc najlepszym sposobem na odwet jest ich niszczenie. (...) Nadal będę walczył z neonazistami, pedofilami, Hizbollah czy Hamasem. Sądzę, że każdy powinien z nimi walczyć na swój sposób".

Tenenbaum należy do organizacji hakerskiej znanej jako Enforcers. Właśnie ona skłoniła go do działalności antypornograficznej, gdyż statut organizacji zakładał wolę walki z pedofilami i rasistami. mimo to Enforcers niedługo po aresztowaniu Analyzera zaprzestała swojej działalności ze względu na fakt, iż przez wybryki Tennenbauma media zwróciły na nią zbyt dużą uwagę.

Nicholas Whiteley — czyli szalony haker

W Wielkiej Brytanii pierwszego hakera aresztowano w 1988 roku. Był to Nicholas Whiteley, który stał się praktycznie ofiarą nowego systemu prawnego. Bowiem dopiero w 1988 roku haking uznano tam za przestępstwo i kiedy Whiteley włamał się do systemu komputerowego Uniwersytetu Bath and Hull, stał się oczekiwanym celem. Skończyło się jednak tylko rokiem pobytu za kratkami.

Whiteley zaczął interesować się komputerami w wieku 12 lat, gdy w jego szkole pojawiła się maszyna Acorn Atom z pamięcią 4 KB i starym czarno-białym monitorem. Z upływem czasu szkoła wzbogaciła się o komputery Sinclair ZX80 i ZX81, a później w maszynę obliczeniową RMZ80.

Wtedy nie myślał jeszcze o włamaniach, ale w głębi duszy marzył, by zostać informatykiem. Kiedy pojawiła się okazja wybrał tę specjalność jako dalszy kierunek nauki. Pierwszy duży komputer DEC 10 spotkał na politechnice w Middlesex.

W 1984 roku w wieku 15 lat kupił swój pierwszy komputer Commodore VIC20 PC, który później przerobił na Commodore 64. Spędzał czas programując gry, z zamiarem opanowania tego rzemiosła w sposób profesjonalny. Posiadał certyfikat drugiego stopnia z informatyki, matematyki, fizyki, angielskiego i arytmetyki.

W 1985 roku podjął pracę, a jego nowym zadaniem było przygotowywanie danych dla lokalnej rady, co okazało się bardzo nudnym zajęciem. Szef jednak dostrzegł jego zainteresowania i przesunął go na stanowisko operatora.

Wtedy Whiteley zajął się komputerami ICL i systemem operacyjnym VME. W firmie zainstalowano właśnie nowy sprzęt i dzień po dniu mógł zdobywać wiedzę na temat jednego z najbardziej skomplikowanych systemów operacyjnych. Nocami przesiadywał przy swoim nowym nabytku, komputerze Amiga 1000, w którym gromadził wszystkie zdobyte informacje na temat ICL.

System operacyjny VME traktował bardzo poważnie. I w takich okolicznościach po raz pierwszy się włamał. Odbyło się to na oczach wszystkich, w czasie, gdy operatorzy zmieniali hasła i kodowali je, jemu udało się złamać kod.

Ale prawdziwą działalność Whiteley rozpoczął dopiero po podjęciu pracy operatora w firmie Bush Boake Allen, produkującej kompozyty aromatyczne.

Jakkolwiek nigdy nie włamał się ani do, ani za pośrednictwem komputerów firmy, to układ zmian pozwalał mu na ciągłe doskonalenie umiejętności. Nawet popołudniową zmianę trwającą od czternastej do dwudziestej drugiej wykorzystywał do tego celu. W domu natomiast całymi godzinami patrzył w ekran. Jak wspomina:

„Najlepsze były weekendy. Piłem kawę i colę, paliłem mnóstwo papierosów i potrafiłem pracować przez 24 godziny. Rodzice patrzyli na to z niepokojem. Uważali, że taki tryb życia, może się odbić na zdrowiu.

Rachunek telefoniczny za kwartał wynosił 460 funtów, z czego ja płaciłem 400. Myślę, że był to całkiem tani sposób spędzania czasu. To tylko 25 funtów tygodniowo. Zresztą zarabiałem nieźle w BBA, a nie miałem czasu na wydawanie pieniędzy. Na koncie uzbierała mi się niezła sumka.

Czas uciekał niezauważalnie. Nieraz ze zdumieniem stwierdzałem, że jest już druga nad ranem. Obiecywałem sobie, że jeszcze tylko jedna rundka i koniec. Kiedy spojrzałem na zegarek ponownie była ósma rano.

Mój brat zwykł wpadać do pokoju i pytać: I co u Ciebie?. Po paru godzinach znów zaglądał i zadawał to samo pytanie. Kiedy chciałem pochwalić się jakimś sukcesem i wyjaśnić mu szczegóły włamania, odpowiadał: Słuchaj, Nick, ja i tak nic z tego nie rozumiem!”.

Sieć Janet stała się ulubionym miejscem wędrówek Whiteleya dzięki informacjom, jakie przyniosła mu lektura „Haker’s Handbook”.

Potrafił też napisać program, który wyszukiwał wszystkie komputery ICL zainstalowane w Sieci. W swych nocnych wypadach najczęściej zatrzymywał się przy Queen Mary College i Uniwersytecie Glasgow. Dostawał się tam za pomocą programu, któremu z racji szybkości działania nadał nazwę — „królik”. Wyznaje:

„Napisałem program, który uruchamiał komputer. Przypuszczałem, że operator może to zauważyć. Nadałem informację o tym. W Glasgow przyjęli ją, ale w Queen Mary nie było nikogo. To było w piątek w nocy. Dopiero w poniedziałek rano zwrócili na to uwagę. Plan pracy komputera został całkowicie zakłócony. Musieli usunąć wiele zbiorów".

Na uniwersytecie zorientowano się, że ich obawy dotyczące penetracji systemu nie były bezpodstawne, ale dopiero atak na komputer w Queen Mary College spowodował rzeczywiste przeciwdziałanie. Świadomość, że włamywacz ma dostęp do zbiorów i może robić z nimi wszystko, co tylko zechce, zmobilizowała uczelnię do wyśledzenia drogi połączeń.

Wkrótce policja zapukała do drzwi włamywacza. Ambicje Whiteleya zostały powstrzymane 6 lipca 1988 roku. Siedział wówczas w swej sypialni w domu rodziców w Enfield i stukał zawzięcie w klawiaturę komputera. do drzwi ktoś zapukał. Za oknem stało trzech albo czterech facetów. Ojciec Whiteleya otworzył im drzwi, usłyszał coś o nakazie rewizji. Whiteley był oszołomiony, kiedy ktoś powiedział, że jest aresztowany za włamanie do komputera Queen mary College. Wszystko to przypominało scenę z filmu sensacyjnego.

Policja przeszukiwała dom przez następne trzy godziny. Zapakowano komputer, dyskietki i wydruki. Około jedenastej w nocy, Whiteley został zabrany na posterunek Holborn w centralnym Londynie i osadzony w areszcie. Następnego dnia po spotkaniu z obrońcą wyznaczonym z urzędu, a detektyw Austin przesłuchiwał go przez 6 godzin.

Został w areszcie, a policja zajęła się sprawdzaniem informacji zgromadzonych na skonfiskowanych dyskietkach. Rodzice dostarczyli mu trochę smakołyków. W końcu po zdjęciu odcisków palców i zrobieniu zdjęć zwolniono go. Wcześniej musiał jednak oddać kartę identyfikacyjną i przepustkę wystawioną przez firmę BBA, w której pracował. Oznaczało to, że stracił pracę.

Trzy lata ciągnęły się procedury prawne, wyroki, apelacje, dyskusje w prasie, zanim zapadł wyrok. Whiteley powołał do życia agencję konsultacyjną Andromeda, która miała pomagać użytkownikom komputerów personalnych w ochronie ich zbiorów. Zdobył nawet parę kontaktów, ale przeciągający się proces uniemożliwił dalszą działalność. Komputery osobiste nie były zresztą jego pasją. Wciąż interesował go sprzęt ICL, ale przypuszczał, że nikt nie będzie chciał zatrudnić człowieka z przeszłością kryminalną.

Whiteley nadal uważa, że jego motywacją byłą chęć nauki, a nie włamania. Próbował znów zająć się komputerami ICL, ale w końcu zdał sobie sprawę z tego, że nie można żyć przeszłością. Musiałby od nowa uczyć się tysięcy komend. Po wyjściu z więzienia policja zwróciła mu sprzęt, ale wciąż uważa się za pokrzywdzonego. Gdyby odpowiednie przepisy funkcjonowały wcześniej, nie został włamywaczem i nie musiał siedzieć w więzieniu. Rzeczy które robił nie były wcześniej opatrzone sankcjami prawnymi. A tak... złamał sobie karierę.

Edward Austin Singh

Wśród brytyjskich włamywaczy zmuszonych do publicznego ujawnienia się Edward Singh był jednym z najbardziej utalentowanych i aktywnych zarazem. Wiadomość o aresztowaniu go przez Wydział Kryminalny została natychmiast podana przez magazyn „Computing", ale nikt nie zwrócił na to uwagi aż do chwili, gdy dwa tygodnie później policja ujawniła szczegóły jego działalności.

Singh opracował bowiem program, który pozwalał mu na dostęp do zastrzeżonych, komercjalnych i wojskowych informacji. Przyznał, że mógł nie tylko poznać stan cudzego konta w banku, ale jeszcze przesłać pieniądze na dowolne konto.

Singh był wówczas dwudziestotrzyletnim, poważnym, pełnym entuzjazmu młodym człowiekiem, pewnym swej intelektualnej pozycji. Ale kiedy mówił wpatrywał się w stół lub w podłogę, skrywając wyraz swych oczu za ciemną grzywką. Może czegoś się wstydził?... Miał wyjątkowy talent do niedotrzymywania umówionych spotkań. Często nosił ze sobą postrzępione egzemplarze rozpraw filozoficznych Kanta. Ubrany w dżinsy, tenisówki i luźną, bawełnianą koszulkę spędzał cały czas w pubach grając na ustawionych tam automatach i popijając godzinami jeden kufel piwa. Po przedwczesnym opuszczeniu uniwersytetu rozkład jego dnia był składanką wolnego czasu i dezorientacji w typowo studenckim stylu. Jego historia jest pod wieloma względami przykładem na to, w jaki sposób fascynacja elektroniką i komputerami może doprowadzić do obsesji.

Urodził się w Boże Narodzenie w 1964 roku, w londyńskiej dzielnicy Kingston nad Tamizą. Od dziecka interesowały go wszelkie maszyny i zasady ich działania. Pierwszy komputer zobaczył mając 8 lat w czasie wycieczki do muzeum techniki w Kensington. „Widziałem tam program demonstracyjny zatytułowany «Zgadnij jakie to zwierzę» — wspomina Singh — i już wtedy myślałem o włamaniu. Byłem strasznie ciekaw, jak to działa". Później w szkole średniej miał okazję korzystać z teleksowego łącza komputerowego z Uniwersytetem Surrey.

W szkole, do której chodził, było około 1500 uczniów, ale tylko dwóch lub trzech interesowało się informatyką. Programowali trochę w Basicu i oczywiście grali w różne gry. W domu zajmował się elektroniką. Kupował stare radia i telewizory i próbował przywracać je do życia. Wszystkie wolne dni spędzał w swym warsztacie urządzonym w piwnicy. Bardzo lubił grzebać w starociach. Dzięki nim mógł słuchać dziwnych, normalnie niedostępnych stacji, jak np. Radio Moskwa. Chciał wtedy zostać oficerem radiowym w marynarce handlowej.

W wieku 14 lat Singh został adoptowany i przeniósł się do Dorking, a jego brat i siostra pozostali z matką. W tym samym roku wysłano go do szkoły w Niemczech. Radził sobie dobrze, ale nie był zbyt zadowolony z przenosin i reżimu, jakiemu został poddany. Przymusowa służba kościelna i wojskowa nie pasowała do jego charakteru. Na dodatek nie miał regularnego dostępu do komputera. Po powrocie do Surrey został wysłany do szkoły technicznej Brooklands w Weybridge, gdzie zaczął studiować informatykę. Tam właśnie w wieku 16 lat rozpoczął swoją karierę włamywacza.

Był zafascynowany, gdyż mógł spędzać całe dnie przy terminalu. Przedzierał się przez zakamarki szkolnego komputera Prime. Trudno określić ówczesne próby jego włamania, ponieważ większość z nich nie zakończyła się sukcesem. Ale jedno udało się zrobić — napisał program przechwytujący cudze hasła. Ten eksperyment był powodem pierwszego starcia z przełożonymi, gdyż wykładowca dowiedział się o wszystkim i zabronił komukolwiek używać programu. Incydent nie powstrzymał jednak Singha.

Nie czując się dobrze w Brooklands Singh, przeniósł się do innej uczelni w Redhill. Kontynuował studia informatyczne i dalej prowadził swoje poszukiwania. Komputer uczelni nie był podłączony do żadnej sieci zewnętrznej, ale też stanowił wyzwanie. Singh penetrował system dopóty, dopóki nie odkrył wszystkich stosowanych w nim haseł. Został przyłapany w chwili, w której drukował pełną ich listę. Tym razem nie udało mu się zdać egzaminów i opuścił uczelnię bez dyplomu. Znalazł sobie pracę w towarzystwie ubezpieczeniowym jako urzędnik nadzorujący realizację zleceń i opłat składek. Komputer, który miał do dyspozycji w swej filii, włączony był w ogólną sieć firmy. Hasło potrzebne do wejścia w system, napisane na karteczce, przyklejano do monitora na wypadek, gdyby ktoś je zapomniał. Dostęp do komputera umieszczonego w głównym biurze firmy był jednak utrudniony. Po roku zniechęcony Singh opuścił firmę. Wiosną 1984 roku wybrał się z kolegą w podróż do południowej Afryki. Po tygodniu pobytu pod upalnym niebem Tangeru zdecydowali się na powrót do Europy. Przejechali przez Hiszpanię, Francję i Włochy aż do Grecji. W końcu wyczerpały się pieniądze i trzeba było wracać. Za resztę drobniaków Singh kupił w Atenach książkę o systemach operacyjnych. Przeczytał ją w pociągu w czasie drogi powrotnej.

W Dorking mieszkał we wspólnym mieszkaniu wraz z dwoma kolegami z uczelni. Jeden z nich miał własny komputer. Drugi postarał się o modem, za pomocą którego Singh podłączył komputer do Sieci. Telecom wydał mu pozwolenie na korzystanie z systemu. Jako że było ono drogie, trzeba było znaleźć sposób na unikanie opłat. Singh szybko odkrył, że łącząc się z miejscowym uniwersytetem w Guildford jest w stanie, za cenę lokalnej rozmowy, osiągnąć połączenie z dowolnym miejscem w świecie. Nie podejmował żadnej pracy, korzystając z pieniędzy otrzymywanych od przybranych rodziców.

W tym właśnie czasie Singh nawiązał pierwszy kontakt z włamywaczami. Dostał numer biuletynu redagowanego przez kogoś w Leicester. Jak wspomina:

„To było moje pierwsze doświadczenie. Biuletyn zawierał mnóstwo informacji dla hakerów i w ten sposób trafiłem na faceta na Uniwersytecie Surrey, który nauczył mnie, jak włamać się do systemu elektronicznej poczty i odczytać przesyłane wiadomości. Od niego też dostałem hasło wykładowcy wydziału matematyki, które było wciąż aktualne, mimo że człowiek ten opuścił uczelnię trzy lata wcześniej".

Na początku 1985 roku dwudziestoletni wówczas Singh zaproponował jednemu z uniwersyteckich analityków systemów udział w pracach nad wzajemną translacją różnych języków komputerowych. Od czasu do czasu zaglądał również na wykłady w szkole technicznej w Guildford. Ale zła sława się rozeszła szybko i musiał opuścić uczelnię.

W tym czasie Singh najczęściej penetrował instalacje komputerów Prime. Procentowały tu wcześniejsze doświadczenia z badań nad systemem operacyjnym Primos. Na Uniwersytecie Surrey znajdowała się jedna z największych sieci tych komputerów w Europie. Potrafił dostać się do każdego z nich. Przeglądał głównie rejestry uczelni, zbiory administracyjne i pocztę.

W końcu postanowił dokończyć studia. W odróżnieniu od normalnie przyjętych kryteriów nie wybrał uczelni ze względu na jej reputację czy też położenie, lecz zdecydował się na Politechnikę Teesside posiadającą komputery Prime. Został przyjęty na czteroletni kurs informatyki. W Middlesbrough szybko znalazł sobie miejsce w centrum komputerowym, co pozwoliło mu na swobodny dostęp do Sieci.

„Wędrował" po komercyjnych systemach na całym świecie, głównie — po instalacjach komputerów Prime i wraz z innymi studentami stworzył grupę „Dot Abuse Kids".

Zdarzało się, że włamania były bardzo szybko wychwytywane. Po drugim wejściu w sieć szkoły rolniczej w Edynburgu, przeczytał wiadomość: „Wiem, że jesteś włamywaczem. Zostaw naszą sieć w spokoju w okolicy są lepsze kąski". Dość szybko jego działalność została zauważona przez władze uczelni. Już w czasie pierwszego semestru Uniwersytet Surrey skontaktował się z Teesside skarżąc się na włamywaczy. Singh został wezwany na rozmowę.

Nieco później włamał się wraz z kolegami do komputera Uniwersytetu Sussex i nawiązał kontakt, jak się potem okazało, z administratorem, który kazał mu się rozłączyć i zadzwonić pod wskazany numer. Singh usłyszał, że został zlokalizowany i o jego działalności zostanie powiadomiony szef centrum komputerowego Teesside. Po dłuższej rozmowie administrator systemu Sussex dał się przeprosić i obiecał zapomnieć o zdarzeniu. Faktycznie ten incydent nie pociągnął za sobą żadnych konsekwencji. Ale Singh został przyłapany ponownie, tym razem przez pracowników Teesside, którzy zaczęli poważnie obawiać się, że działalność ludzi pokroju Singha przyniesie im prędzej czy później kłopoty. Dr. John Wilford, starszy wykładowca z ich kursu, próbował powstrzymać go. Jego zdaniem Singh:

„był bardzo zdolny, ale miał w sobie coś takiego, co czyniło go włamywaczem niejako automatycznie. Rozmawiałem z nim i zachęcałem do studiowania zgodnie z programem kursu. W zasadzie zgadzał się, ale po pewnym czasie wracał na swoje stare ścieżki. To było coś w rodzaju narkotycznego uzależnienia. Chciałem, żeby zdobył kwalifikacje i dobry zawód, ale on ciągle wracał do przełamywania kodów. Udało mu się dostać do Janet, głównej sieci akademickiej, ale został kilkakrotnie przyłapany. Był naprawdę dobry, znał doskonale komputery Prime".

Wilford wierzył, że Singh mógł bez problemu ukończyć studia.

„Nie wiem dlaczego nie próbował — ciągnie swój wywód — czyniłem zabiegi aby go przekonać, wszystko na próżno. Miał całkiem ugodowy charakter, ale nie potrafił robić nic, co go nie interesowało. Wymagaliśmy od naszych studentów pewnego, określonego zasobu wiedzy. Nie wyrzuciliśmy go za włamania. Spędzał całe godziny w laboratorium, ale jedyne, czego szukał, to były sposoby na wędrówki po sieciach.

Mieliśmy bardzo słabo rozwinięty system zabezpieczeń. On powinien pracować w jakiejś firmie zajmującej się metodami ochrony danych i może wtedy zacząłby myśleć o włamaniach w innych kategoriach".

Singh zignorował rady Wilforda, nie zaliczył paru wykładów, w końcu nie zdał egzaminów i musiał opuścić uczelnię. Był już wtedy człowiekiem całkowicie uzależnionym od komputera. Teoretycznie nie powinienem mieć żadnych problemów z dostaniem odpowiedniej pracy, ale nikt nie dałby mi referencji.

W tym czasie zaczął występować pod pseudonimem „Średni Vashtar". Pomysł zaczerpnął z autobiograficznej książki Richarda Hillary'ego „Ostatni przeciwnik", opowiadającej o przeżyciach pilota w czasie bitwy o Anglię. Po powrocie do Surrey, tym razem bez komputera, Singh cały czas myślał o metodach swobodnego dostępu do sieci. Poszedł w końcu na uniwersytet i odegrał rolę słuchacza informatycznych studiów doktoranckich. Nie było to trudne. Bez problemu przekonał innych studentów. Udało mu się nawet zdobyć legitymację studencką. Miał przyjaciół wśród studentów i czasami nocował w domu studenckim. W ciągu dnia, a potem nocami siedział przy terminalu, który wkrótce należał tylko do niego. Zaczął być znany. Czasami pytał o coś pracowników uczelni, ale nie dlatego, że nie znał odpowiedzi, lecz po to, by zaistnieć w środowisku. Ci, którzy wcześniej go znali już tam nie pracowali.

Wykorzystując te same hasła, które poznał kiedyś, bez problemu uzyskał dostęp do sieci Janet. Pracował systematycznie. Zbierał informacje i starannie je analizował. Zanim został aresztowany, miał dostęp do 250 systemów na całym świecie. Granice geograficzne nie miały żadnego znaczenia w pojęciu włamywacza.

W połowie roku akademickiego w centrum komputerowym zorientowano się, że ktoś systematycznie penetruje system. Ostrzegano więc potencjalnych włamywaczy przed ewentualnymi konsekwencjami.

Pomimo to Singh nie zaprzestał prób, ani nawet nie zwolnił tempa. Nawiązywał coraz więcej kontaktów i wymieniał informacje z innymi włamywaczami rozrzuconymi po całym świecie. Niektóre z prywatnych biuletynów pracowały w sieci po 24 godziny na dobę, inne dostępne były w tych porach, kiedy firmy nie wykorzystywały swoich do bieżącej komercyjnej działalności. Ulubionym miejscem elektronicznych spotkań hakerów był w tym czasie niemiecki system Altos. Tam właśnie Singh poznał najbliższych mu potem towarzyszy elektronicznych wędrówek. Jednym z nich był Scott Klein z Filadelfii. Już jako uczeń dysponował swym własnym komputerem. Chcąc mieć dostęp do większej ilości gier, kupił modem i zaczął wymieniać informacje z innymi zapaleńcami. O systemie Altos dowiedział się za pośrednictwem biuletynu redagowanego w USA. Podobnie jak Singh specjalizował się w komputerach Prime.

Klein posługiwał się pseudonimem „Szando". Pod tajemniczym pseudonimem „MH" pracował natomiast siedemnastoletni kompan Kleina z Nowej Anglii. Przy końcu 1987 roku za pośrednictwem Kleina Singh poznał „MH". W ciągu następnych miesięcy nawiązali intensywną współpracę i wymieniali informacje na temat sposobów penetrowania różnych systemów operacyjnych. Singh wymyślił dla nich wspólną nazwę „Triada".

Ich metody nie miały oczywiście nic wspólnego z potężną mafią o tej samej nazwie. Scott i „MH" czasami łączyli się z Singhem poprzez sieć Surrey, ale najczęściej spotykali się na gruncie Altos. Pod koniec współpracowali bardzo ściśle. Można powiedzieć, że utrzymywali transatlantycką łączność, planując wspólne operacje obejmujące swym zasięgiem cały świat. Rozmawiali po 4 czy 5 godzin, chociaż nigdy nie spotkali się wszyscy razem. W styczniu 1988 roku Singh miał co prawda okazję widzieć „MH", który udawał się na kurs w Oxfordzie. Klein natomiast nie miał pojęcia, jak wyglądają współtowarzysze jego wędrówek. Dopiero rok po aresztowaniu udało mu się zobaczyć Singha.

Kolejnym kompanem, którego Singh poznał za pośrednictwem Altos był Hans Hubner. W Niemczech zjawisko komputerowych włamań rozwijało się w atmosferze współpracy, której przykładem był Klub Komputerowego Chaosu. Dziewiętnastoletni Hans pozostawał w tym momencie poza głównym nurtem klubu, uczestnicząc okazjonalnie w corocznych konferencjach. Kiedy jako kilkunastoletni chłopak przeprowadził się do Berlina Zachodniego, zajmował się elektronicznymi zabawkami, składając najróżniejsze układy z lutownicą w ręku.

Potem pojawił się na rynku komputer Sinclar ZX81, który kupił jeden z jego kolegów. Przesiadywali przy nim całymi godzinami. Sam zaprojektowałem komputer, ale nigdy go nie zbudował. Ogólnie rzecz biorąc, znacznie więcej czasu poświęcał oprogramowaniu niż oprzyrządowaniu. W Berlinie Zachodnim połączenie z dowolnym miejscem z Niemczech kosztowało zaledwie 25 fenigów, więc nie było problemu z opłatami.

Od wczesnych lat Hans angażował się w różne ruchy polityczne. Obracał się wśród ludzi okupujących opuszczone budynki, czasami wśród anarchistów. Jego rodzice byli socjalistami. Sam zawsze dryfowałem w stronę lewicy tyle, że starał się być bardziej pragmatyczny. Niektórzy członkowie klubu byli weteranami 1968 roku, inni uważali się za wiecznych rewolucjonistów, ale większość hakerów to po prostu włamywacze bez ideologii.

Pierwszy konflikt z władzami nastąpił na samym początku działalności Hansa. W 1987 roku został aresztowany za włamanie do systemu. Oskarżono go o nielegalne korzystanie z Sieci i zarekwirowano komputer wraz z dokumentacją. W końcu dostał wszystko z powrotem i nigdy nie wspominano o tym wydarzeniu. Zapłacił jedynie 500 marek za nielegalne podłączenie telefonu z sekretarką.

Spędzając całe godziny przy komputerze wyspecjalizował się szczególnie w systemie operacyjnym VMS. Jak większość włamywaczy wymieniał z innymi zdobyte informacje. Tak natknął się na Singha. Współpraca nie utrwaliła się jednak.

Altos był główną europejską giełdą, na której włamywacze wymienili hasła i demonstrowali swe osiągnięcia. Postronny obserwator mógł natomiast obejrzeć w szczegółach, jak wygląda elektroniczne podziemie. Wiosną 1988 roku z pośrednictwem systemu Altos, Singh otrzymał ważną wiadomość od programisty z Politechniki Teesside. Ostrzegał go przed akcją amerykańskiego biura firmy Prime skierowaną przeciwko komputerowym włamywaczom. W liście przesłanym przez biuro prawne

uczelni władze zostały poinformowane o włamywaczach działających na terenie Teesside. Proszono o ustalenie i podanie ich nazwisk. W związku z wprowadzeniem do testowania nowego oprogramowania firma Prime chciała mieć pewność, że nie przeniknie ono w niepowołane ręce. Singh był zaskoczony tą informacją. Zbyt często buszował po sieci Prime w USA, aby nie zostało to zauważone. Jego aktywność ułatwiła też wyśledzenie drogi połączeń. Sprawdził wiadomość u nadawcy i dowiedział się, że jest proszony o kontakt z brytyjskim przedstawicielem firmy. Jak wspomina:

„Znalazłem numer filii w książce telefonicznej i zadzwoniłem do dyrektora. Malcolm Padina wyskoczył z krzykiem: To ty włamujesz się do moich komputerów?. Potem porozmawialiśmy o zabezpieczeniu systemu. Skrytykowałem stosowane przez nich metody. Odpowiedział, że jeśli chcę pomóc, to mogę złożyć pisemną ofertę".

Tak zaczęła się seria telefonicznych spotkań pomiędzy biznesmenem i komputerowym fanatykiem podejrzewanym o włamania do systemów na całym świecie. Parę tygodni później Singh wystąpił z propozycją podjęcia pracy w firmie Prime.

W tym samym czasie problemem bezpieczeństwa komputerowych zbiorów zainteresowały się służby specjalne Scotland Yardu. Operację schwytania Singha przygotowywano przez ponad 6 miesięcy, a jej korzenie sięgają Departamentu Skarbu USA. Od 1984 roku, czyli zaraz po wprowadzeniu przepisów federalnych o przestępstwach komputerowych, niektóre aspekty dotyczące włamań do systemów informatycznych znalazły się również w sferze zainteresowań sekcji specjalnej. Istnieje umowa zawarta pomiędzy Prokuratorem Generalnym USA i Departamentem Skarbu, dotycząca ich współdziałania z FBI w zakresie ścigania przestępstw tego typu. Nie zmienia to oczywiście faktu, że różne służby rywalizują ze sobą na tych samych polach. Aresztowanie Scotta Kleina w lutym 1988 roku pozwoliło agentom służb specjalnych na obserwację działalności Singha.

Wzięto go pod lupę. W tym momencie przypuszczano, że Singh współpracuje z niemieckim wywiadem, gdyż Singh włamał się do wojskowego systemu obronnego USA i wymieniał zdobyte informacje z kolegami z Klubu Komputerowego Chaosu. To podejrzenie spowodowało przyspieszenie działania służb specjalnych. Z rozmów z agentami Malcolm Padina wyniósł wrażenie, że Singh tkwi w samym środku międzynarodowej siatki szpiegowskiej związanej z niemieckimi włamywaczami.

Śledztwo w sprawie szpiegostwa elektronicznego na rzecz bloku wschodniego prowadziły niezależne agencje amerykańskie i zachodnioniemieckie. Singh miał szczęście, że policja brytyjska nie potraktowała tej sprawy równie poważnie. Na jego korzyść przemawiał też fakt, że nie akceptował i nigdy nie stosował żadnych programów w stylu konia trojańskiego.

Po próbie nawiązania współpracy, przedstawiciele Prime zaproponowali Singhowi podróż do USA. Propozycja była niezwykle atrakcyjna, dla bezrobotnego entuzjasty komputerów, który nie miał dotąd okazji odwiedzić Ameryki. Dochodziła do tego możliwość pracy w laboratoriach badawczych Prime w Massachusetts. Ale...

Kryła się w tym pułapka. W opinii FBI wyrządził on bowiem znacznie więcej szkód niż to faktycznie miało miejsce.

Detektyw Graham Seaby ze Scotland Yardu, który aresztował Singha, tak opisał przebieg przygotowań:

„Plan gry zakładał zwabienie Singha do USA, gdzie przejąłby go amerykański wymiar sprawiedliwości. Początek został zrobiony. Uzgodniono, kiedy Edward zwróci się o wizę dostanie ją bez żadnych problemów. Taka opcja rozważana była poważnie przez Amerykanów jeszcze we wrześniu. Fakt, że dowody oskarżenia były bardzo słabe, utrudniał nam działanie w ramach obowiązujących u nas przepisów. Na nasze szczęście Edward sam dał nam dowody, które pozwoliły zakwalifikować jego działalność jako normalne włamanie. Gdyby posługiwał się swym własnym, domowym terminalem, nie moglibyśmy go aresztować".

Plan opracowany przez amerykanów, polegający na zwabieniu Singha do USA, upadł ze względu na opór Departamentu Sprawiedliwości. Wyrażano obawy, że operacja tego typu ma znamiona uprowadzenia. Scott Klein miał również wątpliwości co do koncepcji podstępnego ściągnięcia Singha do USA. Po aresztowaniu nakłaniany był on do współpracy pod groźbą kary długoletniego wiezienia. Straszono go tak długo, aż wyraził zgodę. Oskarżono go jedynie za włamanie i zakłócanie międzymiastowej sieci komputerowej. Zastosowano wobec niego karę w postaci czasowego zakazu korzystania z Sieci.

Ale Singh nic o tym nie wiedział. Zniknięcie kompana z Sieci wytłumaczył sobie awarią sprzętu. Trzeci członek triady działał nadal. W tym momencie do akcji wkroczyła policja brytyjska. Z inicjatywą skierowaną do szefa sekcji włamań komputerowych inspektora Austina wyszli przedstawiciele Prime. Poinformowano Scotland Yard, ponieważ przypadek dotyczył przestępstwa popełnionego również poza terytorium Wielkiej Brytanii. Seaby, który właśnie wrócił z instytutu Cranfield, gdzie zajmował się komputerową analizą danych, został uznany za człowieka o odpowiednim doświadczeniu. W ramach przygotowań do akcji Seaby zebrał dodatkowe informacje o systemach i sieciach. Odbył kilka spotkań z amerykańskimi prawnikami firmy Prime oraz zapoznał się z dotychczasowymi ustaleniami amerykańskich służb specjalnych. Chociaż w liście do przedstawiciela Prime Singh podał swój adres w Leatherhead, nie miało to większego znaczenia dla policji, ponieważ rzadko tam bywał. Aresztowanie wchodziło w rachubę tylko w przypadku złapania go przy pracy. Wiadomo było, że utrzymuje kontakty z Politechniką Teesside, a ślady prowadziły do Uniwersytetu Surrey. Potwierdzono personalia Edwarda Austina Singha, ale nie sposób było ustalić aktualnego adresu. Nie był zarejestrowany w Surrey ani jako student, ani jako pracownik. Przypuszczalnie należało szukać go w miasteczku studenckim. Władze uczelni wyraziły zgodę na podłączenie dodatkowego terminalu rejestrującego zewnętrzne rozmowy telefoniczne.

Sprawa nie była wcale taka prosta. W Guildford funkcjonowało 900 terminali i ustalenie, z którego korzysta Singh nie było łatwe.

Wiadomo jednak było, że gromadzony przez włamywaczy materiał może być składowany na różnych kontach. Pozwolono zatem na legalne wejście hakera w centralny system firmy Prime w Massachusetts. Zaaranżowano to za pośrednictwem Billa Lennona, szefa działu ochrony danych.

Singh nawiązał kontakt z Lennonem za pośrednictwem Malcolma Padiny. Podstawą do podjęcia akcji był list Singha oferujący współpracę z ekspertami Prime. Skłonienie włamywacza do nawiązania łączności ze znanym policji miejscem pozwoliło na przetrzymywanie go na linii wystarczająco długo, aby zlokalizować terminal, z którego korzystał. W ten właśnie sposób misternie zaaranżowana akcja przyniosła sukces. Singh zjawił się w Surrey i nawiązał łączność. Ustalono, że komputer pracuje w głównym gmachu uniwersytetu.

Kiedy został ujęty była niedziela, 9 października 1988 roku. Ostatniej nocy Singh wybrał się na dyskotekę do klubu studenckiego. Wyszedł dopiero we wczesnych godzinach rannych. Po południu, z lekkim szumem w głowie, wolnym spacerkiem poszedł do centrum komputerowego i rozpoczął kolejną sesję.

„Szło mi całkiem nieźle" — wspomina. Łączył się po kolei z różnymi miejscami na świecie. O godzinie 7.10 wieczorem został aresztowany. Kiedy Seaby i Henson weszli do pokoju, Singh pracował w niemieckiej sieci Altos. Obok komputera leżała kartka z długą listą numerów. Ponieważ nie miał prawa do korzystania z urządzeń uniwersytetu, ani drukowania na kradzionym w takim przypadku papierze, został aresztowany pod formalnym zarzutem włamania. Nieco wcześniej Singh nawiązał kontakt z redakcją magazynu „Computing". Wiedza na temat systemów i zainteresowanie problemem zabezpieczenia danych, skłoniły go do opublikowania swych spostrzeżeń. Zdzwonił do redaktora działu tematycznego i zaproponował przygotowanie artykułu. Niestety nie zdążył zrealizować tego zamierzenia.

Wśród zarekwirowanych w domu rodziców Singha w Leatherhead materiałów (oprócz komputerowych wydruków) znalazł się jego notatnik zawierający listę kilkuset komputerów, do których udało mu się włamać, hasła, adresy i kody. Pomiędzy kartkami był też wycinek z „Financial Time" z ciekawą uwagą: „Jeśli ktoś na serio myśli o zdobyciu majątku za pomocą kradzieży, powinien wybrać ofiarę bardzo starannie. Trzeba znaleźć dużą firmę, najlepiej o zasięgu międzynarodowym i niezaangażowaną w interesy publiczne. Taka firma nie będzie dążyć do nagłośnienia sprawy, obawiając się negatywnego oddźwięku i utraty klientów. Ryzyko ujawnienia i aresztowania jest w takim przypadku bliskie zeru". Notatki Singha dowodziły metodycznego podejścia do pracy. Szczegóły dotyczące systemów, do których próbował się włamać ujęte zostały według ustalonego formatu zawierającego nazwę systemu, typ komputera, system operacyjny (pamięć, model procesora), dres i hasła. W wielu przypadkach dopisano dodatkowe komentarze. Przy opisie dotyczącym komputera zainstalowanego w szkole Medycznej w Londynie znalazła się uwaga:

„Marzec 88. Nowy system operacyjny. Większość kodów i haseł nieaktualna".

Wśród notatek był szkic artykułu dla magazynu Computing.

„Swobodny dostęp do systemu — pisał Singh — pozwala włamywaczowi na łatwe wniknięcie w zastrzeżone obszary poufnych danych. Rzadko udaje się przebrnąć przez zewnętrzny i wewnętrzny system, którego administrator prowadzi racjonalny schemat uzyskania pozwoleń na wejście". Wnioski Singha były całkowicie przeciwne do tych, które zgłaszały firmy instalujące sieci i sprzedające systemy. Ale nieposkromiony haker kontynuował:

„Mogłem dostać się do 90 komputerów w międzynarodowej sieci Prime Computer Company, a to oznacza całkowitą penetrację systemu. Byłem w stanie włamać się do każdego komputera Prime na świecie. Przy ciągłym rozprzestrzenianiu się publicznych sieci i wzroście ilości ludzi korzystających z komputerów, nie można lekceważyć problemu włamań wewnętrznych i zewnętrznych. Większość sieci nie posiada elementarnych zabezpieczeń. Uświadomienie sobie tego faktu jest podstawową i pilną sprawą, jakkolwiek nie jestem pewien, czy to wystarczy".

Zarówno Singh, jak i jego koledzy traktowali międzynarodową sieć informatyczna jako gigantyczną bibliotekę. Prawdziwą bibliotekę Babel rodem ze stronic opowieści Borghesa. Jak wspomina rozmarzony włamywacz:

„Wędrowałem po całym świecie. Granice nie miały dla mnie żadnego znaczenia. Niestety nie miałem możliwości zbierania wszystkich informacji, które mogłem zdobyć. W 1986 roku zainteresowałem się pewną teorią i dobrałem się do zbiorów laboratorium CERN w Lozannie. Miałem okazję obejrzeć dokumentację jednego z najkosztowniejszych na świcie projektów badawczych".

Później włamał się do centrum badań astronomicznych Jodrell Bank, a w zbiorach NASA dostał się do informacji na temat bezzałogowej wyprawy na Marsa określonej kryptonimem Scout Project. Udało mu się ponadto dotrzeć do zbiorów elektrowni atomowej Westinghouse oraz centrum obronnego TRW kierującego przemysłem zbrojeniowym USA. W Wielkiej Brytanii włamał się do Centrum Badań Broni Marynarki Wojennej. Wyznaje:

„Często wchodziłem do systemów uzyskując przywileje administratora. Dostałem się do zbiorów US Army, ale nie przeglądałem ich. Chciałem tylko sprawdzić skuteczność moich działań. Dostałem się tam wykorzystując upoważnienie ważne dla jednego z komputerów, którego użytkownik pracował na rzecz armii. Jestem pewien, że mógłbym transferować pieniądze z konta na konto. Na mojej liście były różne banki — Chase Manhattan, Salomon Brothers, Barclays i Security Pacyfic Bank of America. Poznałem system transferowania pieniędzy w tym ostatnim. Bardziej interesowały mnie jednak instalacje wojskowe ze względu na trudniejszy dostęp. Według mego szacunku, 75% sieci publicznych nie posiada odpowiedniego zabezpieczenia".

W notatkach dotyczących Security Pacyfic Bank of America zapisał:

„Poprzez PDN (sieć publiczna) — dostęp do wewnętrznego systemu operacyjnego. Możliwość transferu do 5 milionów dolarów. Około 20 kont osiągalnych; transfer poprzez sieć Telnet. Do dalszego zbadania — SWIFT".

W innym miejscu natomiast zanotował.

„Wejście do SWIFT poprzez Telnet. Wysokość transferu do 50 milionów przy odpowiednim obustronnym kodzie. Do dalszego przebadania".

Singh nigdy nie dokonał transferu pieniędzy, chociaż miał taką możliwość. W czasie śledztwa wyszło na jaw, że konsultował informacje dotyczące elektronicznych przekazów pieniężnych z pracownikami City Bank w Londynie. Pracownik ten został przesłuchany, ale utrzymywał, że ich rozważania nie wyszły nigdy poza sferę spekulacji. Włamania do instalacji militarnych są szczególnie fascynujące. Singh dostał się do sieci Milnet. Opisał to dość dokładnie w swoich notatkach:

„Po połączeniu z numerem 703 pojawia się napis: Witaj w DDN. Tylko do użytku służbowego. Podaj kod. Z przeprowadzonych prób wynika, że akceptuje dwa znaki przed sygnałem dźwiękowym".

Singh wykorzystał informacje na temat Milnetu rozpowszechniane w amerykańskim biuletynie P-80. Połączenie wiedzy z dociekliwością pozwoliły na przełamanie zabezpieczeń komputerów amerykańskiego systemu obronnego. Milnet został odłączony od ogólnej sieci Arpanet w 1983 roku, właśnie ze względu na wzrastającą liczbę włamań. Mimo to Singh nie miał większych problemów z dostaniem się do systemu.

„Jeśli ktoś chciał wykraść informacje wojskowe, to już dawno to zrobił — stwierdził Singh. — Ale penetrowaliśmy też inne instalacje. Raz zaczęliśmy szukać informacji na temat przemysłu motoryzacyjnego. Interesowały nas nowoczesne samochody. Włamaliśmy się bez problemu do systemów w Wielkiej Brytanii i Belgii. Niektóre z nich wykorzystywaliśmy do przechowywania zdobytych informacji. Wiele systemów, nie posiadało żadnych zabezpieczeń. Dzwoniłem nawet na uniwersytet w Oxfordzie i ostrzegałem ich o możliwości penetracji, ale nikt nie traktował tego poważnie. Ostrzegałem też Uniwersytet Surrey. Wysłałem do nich wiadomość za pośrednictwem elektronicznej poczty".

„Traded on Shox", zanotował Singh w rubryce „hasło" przy zapiskach dotyczących systemu Vax. „Shox" to nazwa biuletynu, z którego często korzystał, zbierając informacje na temat systemu operacyjnego VMS stosowanego w komputerach Vax. Jedna z kart zawierała spis kodów i haseł instalowanych rutynowo przez firmę, a które powinny zostać zmienione przez użytkowników. Często przez długi czas hasła pozostawały aktualne w efekcie nieodpowiedzialności korzystających z komputerów osób.

Inna metoda polegała na opracowaniu procedury transferu zbiorów z jednego systemu do innego, który był lepiej rozpracowany. W ciągu jednej tylko nocy udało mu się dostać do ponad dwudziestu komputerów Vax pracujących w sieci Janet. Tak złamał zabezpieczenia komputerów Jordell Bank, Królewskiego Obserwatorium Greenwich i laboratorium Rutherford Appleton. Biuletyn „Shox" funkcjonował w systemie Altger niemieckiej sieci Altos, z siedzibą główną w Monachium.

Redagowany prze dwóch hakerów przetrwał do 1987 roku. Później na jego miejscu pojawiły się inne giełdy wymiany informacji.

6 lipca wśród oferowanych programów można było znaleźć takie tytuły: „lista NUA (adresy użytkowników) Janet: autor — Scooler; „Włamania do VMS dla zaawansowanych"; Itapac (włoska sieć danych) — kompletna lista NUA. Upoważnienia!". Pomiędzy pseudonimami włamywaczami pracującymi tego dnia można było odczytać takie jak: Pengo, Electron, Kilroy, Firefox, Dario, Negabyte, Blackhck, BuckRogers, JohnDoe, Kazuma, Vertigo, Slugbreath, Haker Smurf, Tekno, Oberon, Maveryk, Lory orz Digi. „Shox" stanowił międzynarodową giełdę. Singh wydrukował listę adresów Janet. Obejmowała ponad 60 stron aktualnych adresów komputerów, podłączonych do sieci w każdym z wydziałów wszystkich uniwersytetów i politechnik w Wielkiej Brytanii.

Każda instytucja akademicka występowała pod hasłem UK.AC w odróżnieniu od obiektów militarnych, odnotowywanych pod UK.MOD. Niektóre instytucje, jak rządowe ośrodki badawcze typu NERC-Oban, NERC-Polaris, czy laboratoria NERC w Szwajcarii, zostały wyróżnione osobnym zapisem. Gdzie indziej Singh wypisał brytyjskie instalacje militarne, które udało mu się znaleźć w Sieci, a wśród nich UK.MOD.APRE, czyli Ośrodek Badawczy Admiralicji w Portsdown. Wykorzystywano tam komputery Vax. Był też adres Obrony Wybrzeża USA na Florydzie i dane dotyczące komputerów Europejskiego Laboratorium Fizyki Jądrowej w Cern. Inne zapiski zawierały informacje na temat Królewskiego Ośrodka Badawczego Wojsk Łączności i UK.MOD.PELAY — obsługi poczty wojskowej. Dodano do tego sugerowane metody dostępu do wymienionych zbiorów za pomocą wspólnych haseł stosowanych w komputerach Vax i procedur transferu danych. Singh wypisał również numery kont, jakie założył w systemie uniwersytetu otwartego Milton Keynes. Dostał się tam wykorzystując standardowe hasła, a potem otworzył nowe konta i zakodował je na nowo. Niżej znalazł się wniosek:

„*Odizolowanie systemu od Sieci nie rozwiązuje problemu bezpieczeństwa danych*".

Niektóre z otwartych przez niego kont zostały później usunięte przez innych użytkowników. Skłoniło to Singha do poinformowania administratora systemu o fali włamań. W październiku 1989 roku parlamentarzystka Emma Nicholson stwierdziła, że około 20% rozmów na rachunku telefonicznym uniwersytetu stanowiły połączenia hakerów. Wśród notatek nie zbrakło uwag na temat darmowych połączeń telefonicznych po całym świecie, uzyskiwanych za pośrednictwem kilku numerów w londyńskich bankach. Inna notka dotyczył przemysłowej jednostki kontroli Strathclyde:

„Maj 1987 — przez kilka tygodni korzystałem z komputera Vax 11/750. Potem poinformowałem ich o włamaniu. Myśleli, że jestem szpiegiem przemysłowym! Próbowali psychologicznych chwytów w stylu — jesteś samotną osobą, prawda?".

Zanotował też fragment wiersza o hakerach:

„Spróbuj złamać pierwszy kod
Potem hasło wstaw,
Strzel na próbę i od nowa,
Włam się, włam się, włam
Spróbuj imienia jego żony,
To coś więcej niż tylko gra,
Ale na nowo i wciąż tak samo,
Włam się, włam się, włam”.

Notatnik Singha skonfiskowany przez policję tuż po jego aresztowaniu, został mu zwrócony na początku 1989 roku. Komputerowe wydruki sporządzone z Uniwersytetu Surrey, które zostały znalezione w stosie papierów w domu jego matki. Potraktowano jako mienie kradzione i zniszczono.

Jednym z czynników, które przyczyniły się do sukcesów Singha i Kleina, były opracowane przez nich programy, pozwalające na przechwytywanie rozmów telefonicznych. Stanowiły one udoskonaloną wersję programów symulujących rzeczywistą pracę systemu i oszukujących użytkowników. Według Kleina programy te upowszechniły się w USA, wręcz zlewając publiczne sieci. Jego zdaniem:

„Wszyscy włamywacze korzystają z nich. W ten sposób można dostać się do każdego sytemu. Jedynym dogodnym momentem na przechwycenie jest chwila przerwy, to znaczy czas zanim komputer odpowie na sygnał. Jeśli uderzysz dokładnie w tym momencie, informacja zawarta w buforze zostanie przesłana do innego abonamenta. Masz wtedy hasło i całą procedurę połączenia. Nie ma odpornego komputera. Jeśli znasz system operacyjny, możesz przejść zabezpieczenia, przez ponowne jego załadowanie. Czasami udawało się dostać do systemu, znaleźć metodę kodowania i odkodować wszystkie używane hasła”.

Singh określił ich programy przechwytujące mianem „imitacji gospodarza”. Wspomina:

„Napisaliśmy program, który wykorzystywał nieszczelność systemów telekomunikacyjnych i pozwalał nam łączyć się z węzłami w sieci publicznej. Dzwoniliśmy więc na ten adres. Powtarzaliśmy to w kółko aż do uzyskania połączenia z innym użytkownikiem. Po uzyskaniu kontaktu symulowałem zgłoszenie systemu. Program udawał system, a oni myśleli, że uzyskali połączenie. Mój program prosił autoryzowanego użytkownika o podanie potrzebnych haseł i adresów. W ciągu godziny — od pierwszej do drugiej w nocy — potrafiłem wychwycić do czterdziestu haseł. Program działał równie dobrze w sieci akademickiej, jak i w sieciach wojskowych. Nie było wyjątku. Musiałem, jedynie uważać, aby nie robić tego zbyt często, gdyż mogłoby to wzbudzić czyjeś podejrzenia. Właściciele sieci wiedzieli, od dłuższego czasu o nieszczelnościach. Nie zrobili nic, aby temu zaradzić. Większość szefów sekcji ochrony to ludzie w średnim wieku, a ich doświadczenie ogranicza się zwykle do zmykania drzwi”.

Detektyw Seaby przyznał, że jako włamywacz Singh był technicznie doskonały, uparty i utalentowany. Był niewątpliwie człowiekiem uzależnionym od komputera, ale na pewno nie kryminalistą. Źródłem sukcesów Edwarda była jego zdolność

zgadywania haseł stosowanych w systemach. Wiele firm komputerowych wyrażało chęć zatrudnienia go w celu sprawdzania skuteczności stosownych zabezpieczeń. W US takie rozwiązanie jest już niejednokrotnie stosowane, ale zatrudnienie kogoś o takiej sławie, mogłoby być źle odebrane przez opinię publiczną. Jest natomiast przynajmniej jedna rzecz, w której Singh odniósł sukces — udało mu się zwrócić uwagę na problem włamań komputerowych i zmusić różne organizacje i firmy do zaprzestania strusiej polityki.

Nie wiadomo dokładnie, jakie informacje znalazły się w rękach Singha i jego kolegów. Większość zastrzeżonych systemów nie posiada wyraźnej specyfikacji określającej, co zawierają, a Singh podobnie jak inni włamywacze był zainteresowany, nie tyle zawartością zbiorów, ile sposobem dostania się do nich. W czasie swej działalności na Uniwersytecie Surrey wydrukował materiały jednej z długich sesji penetrowania amerykańskiego systemu obronnego. Zawierały one różne szczegóły dotyczące programu badawczego pod nazwą Tercom. Drukowane wiadomości nie wyglądały ciekawie, ale pojemność pamięci, jaką dysponował, zajęta przez inne zbiory, nie pozwalała na ściągnięcie całego materiału. Znużony Singh przerwał pracę i wyrzucił wszystko do kosza. Sześć miesięcy później zdziwił się bardzo, czytając artykuł naukowy na temat programu Tercom. Okazało się, że dotyczy on komputerowej kontroli prowadzenia pocisków Cruise wyposażonych w głowice jądrowe. Klein również nie był pewien jak głęboko wraz z Singhem wniknęli w zastrzeżone obszary systemów obronnych. Zapewniał:

„Jestem przekonany, że Edward miał dostęp do poufnych zbiorów danych, ale nie mam pojęcia, jakiej klasy były to materiały. Agenci służb specjalnych powiedzieli mi, że Edward penetrował system danych geograficznych, które zawierały informacje na temat złóż ropy naftowej. Obaj natrafiliśmy na pojęcie «trophy» pojawiające się na ekranie. Miało ono ostrzegać o poufności zawartych w zbiorach danych i odpowiedzialności karnej za nieautoryzowane przekraczanie tej bariery".

Większość amerykańskich komputerów wojskowych nie jest z oczywistych powodów podłączona do ogólnej sieci telefonicznej. Wiadomość „trophy" pojawi się zatem na ekranie monitorów komputerów rządowych po nawiązaniu pierwszego kontaktu i ma ostrzegać, że dalsza penetracja systemu jest zabroniona. Podane są również federalne akty prawne określające odpowiedzialność za nielegalne próby przejścia poza ten punkt. Singh przyznał, że niejednokrotnie natykał się na ostrzeżenie i przekraczał je, natomiast Klein utrzymywał, że nigdy nie próbował dostać się poza tę barierę. W odróżnieniu od amerykańskich komputery brytyjskiego ministerstwa obrony nie generują podobnych ostrzeżeń. Osobną sprawą, niezwiązaną z domysłami były fakty ustalone podczas śledztwa. Jeden ze znalezionych podczas aresztowania dokumentów o mało nie wpędził Singha w poważne tarapaty. Był to szkic, na którym naniesiono szczegóły rozmieszczenia łodzi podwodnych na Bałtyku i położenia radzieckich rakiet SS 21 w europie Wschodniej. Wzbudził on zrozumiałe zainteresowanie agentów służb specjalnych, ale wkrótce okazało się, że zawiera on informacje, które Singh wynotował z programu informacyjnego na temat kontroli zbrojeń. Faktem jest natomiast, że Singh spenetrował system Agencji Obrony Nuklearnej USA i próbował uruchomić program symulujący wojnę atomową z elementami SDI (technika wojen gwiezdnych). Zresztą sam o tym opowiadał tak:

„Dostałem od kogoś adres systemu i spróbowałem. Doprowadziło mnie to do innej, dużej sieci i listy opcji wyświetlonej na ekranie. Wybrałem komputer o nazwie „Bigtop", starałem się odgadnąć hasło i okazało się, że brzmi ono: Bigtop. Komputer pracował w systemie DEC 10. Porozglądałem się trochę. Było tam mnóstwo zbiorów. Próbowałem uruchomić niektóre z programów. Jeden ze zbiorów zawierał mnóstwo programów symulujących. Niestety, przy próbach uruchomienia nie chciał startować. Musiałem popełnić jakiś błąd. Pojawiło się polecenie: «wybierz teatr». Wpisywałem nazwy państw, ale rezultat był wciąż ten sam — polecenie pojawiało się od nowa. Nie udało mi się uruchomić tego programu, musiałbym poświęcić mu więcej czasu".

Wśród wytypowanych do rozpracowania systemów zanotowanych w rubryce: „przyszłe projekty", znalazły się m.in.: Inland Revenue, Police National Computer i system Departamentu Zdrowia i Opieki Społecznej. W czasie przesłuchań Singh często wyrażał swoje wątpliwości dotyczące możliwości przenikania danych z systemów rządowych do policyjnych. Obawiał się, że informacje zawarte w kartotekach różnych instytucji mogą być zbyt łatwo penetrowane przez policję. Wiele innych osób podzielało te obawy.

Ciekawe jest również jak Singh oceniał swoje możliwości penetracji różnych systemów. Wspomina więc:

„Wchodziłem do nich, jak chciałem. W większości przypadków byłem w stanie uzyskać status najwyższego uprzywilejowania. Mogłem dostać się do każdego zbioru. Kiedy miałem problemy, zawsze do dyspozycji pozostawały biuletyny i zawarte w nich rady. Mogłem też za ich pośrednictwem poprosić kogoś o pomoc. Przeglądając biuletyny amerykańskie wędrowałem od jednego do drugiego, korzystając z zawartych w nich spisów numerów kart kredytowych. Wiadomości, które tam przeglądałem były nieraz zaskakujące. Trafiłem na opisy konstrukcji bomby domowej produkcji i sposoby manipulowania połączeniami telefonicznymi. Nie ma reguł w tej grze. Ludzie nie rozumieją tego zjawiska".

Jedno z jego ulubionych zajęć poległo, na przechwytywaniu wiadomości przesyłanych przez różne firmy za pośrednictwem poczty elektronicznej. W ten właśnie sposób na początku 1988 roku dowiedział się o dyskusji na temat hakerów prowadzonej w firmie Prime. Podejrzewał, że może to doprowadzić do zwrócenia uwagi na jego działalność. Ale kiedy firma rzeczywiście zaczęła szukać jego śladów, był już człowiekiem, który przeszedł długą drogę kształtowania swego psychologicznego obrazu. Nie poszukiwał w penetrowaniu systemów drobnej sensacji. Jego działalność miała znamiona systematycznej, planowanej pracy badawczej. Niewątpliwie wywarło to wpływ na ocenę jego postępowania w momencie aresztowania.

Parę miesięcy po tej akcji Scotland Yardu Malcolm Padina przedstawił swoje spostrzeżenia na temat działalności Singha:

„Wszyscy mówią o ogólnej dostępności systemów komputerowych jako o drodze w przyszłość, ale nie wiele osób zdaje sobie sprawę z problemów, jakie niosą one z sobą. Pojawia się mnóstwo pytań i wątpliwości. Na świecie zainstalowano mnóstwo

komputerów Prime. Bezpieczeństwo systemu zależy w dużym stopniu od sposobu korzystania z niego przez użytkowników, a Primos nie jest gorszy od innych porównywalnych, powszechnie stosowanych systemów operacyjnych. Po prostu — jeśli zna się zasady funkcjonowania systemu jest o wiele łatwiej włamać się do układu. Singh twierdzi, że w porównaniu z innymi Primos sprawia więcej kłopotów w pierwszym podejściu, ale po wejściu pozwala na bardzo swobodne poruszanie się wewnątrz. Wszystkie firmy walczą, aby ich system był bezpieczny. Primos jest bezpieczny, pod warunkiem, że użytkownik zastosuje się do zaleceń. Wiele osób nie korzysta jednak z dostarczonych im wraz z systemem metod zabezpieczania danych".

Prime jest coraz bardziej znaczącym dostawcą sprzętu na rynku wojskowym, a przepisy Departamentu Obrony są coraz bardziej surowe (według „Orange Book" Departamentu Obrony Primos jest zakwalifikowany do klasy bezpieczeństwa C2).

„Sekcja bezpieczeństwa naszej firmy — ciągnie dalej Padina — wychwyciła sygnały, które wyglądały na działalność Singha w systemie Primos w sieci Arpanet. Kiedy prowadziłem z nim rozmowy telefoniczne nie wierzyłem, że jest szpiegiem. Nie sądzę, aby robił coś świadomie szkodliwego. Był zbyt zdezorientowany i prezentował nadmiernie intelektualne stanowisko. Jego wiedza koncentrowała się na sprawach technicznych. A podróże po elektronicznych sieciach były wyrazem jego egoistycznego nastawienia. Powstrzymywaliśmy go, ale czasy, w których włamywacze docierali jedynie do otwartych systemów należy uznać za przeszłość. Musimy dotrzeć do naszych klientów i wytłumaczyć im ten problem oraz potrzebę przeciwdziałania. Mieliśmy już wcześniej do czynienia z hakerami. Po włączeniu w ogólną sieć telekomunikacyjną system natychmiast jest obiektem ataku. Zwracamy szczególną uwagę na nieudane połączenia i próby podejmowane w normalnie nie wykorzystywanych porach. Jak dotąd nie mieliśmy problemów z wirusami. Nasza sekcja ochrony systematycznie przegląda biuletyny i zawarte w nich informacje. Moim zdaniem stosowanie «sprytnych kart elektronicznych» z kodowaniem typu PIN (personalny numer identyfikacyjny) w połączeniu z procedurami szyfrowania jest najlepszym rozwiązaniem na przyszłość. To, że Singh wybrał właśnie system Prime za obiekt swych badań było dziełem przypadku. Włamania są problemem, który nie omija żadnej z komputerowych firm".

Kilka tygodni po aresztowaniu Singha detektyw Seaby zaaranżował spotkanie agentów służb specjalnych i reprezentantów władz USA z włamywaczem, którego poczynania śledzili przez ostatnie 9 miesięcy. Konfrontacja odbyła się w sali konferencyjnej Uniwersytetu Surrey. Singh wciąż żył pod presją śledztwa prowadzonego przez policję i obawiał się ekstradycji do USA. Poinformowano go, że nadal trwają prace nad wniesieniem ewentualnego oskarżenia na podstawie ustawy o tajemnicy państwowej, związane z penetracją komputerów ministerstwa obrony. Z mieszaniną pokory i pewności na twarzy wyznał:

„Myślę, że stosowali taktykę zastraszania, robiąc wiele szumu o nic. Nie jestem kryształowo czysty, starałem się jednak pokazać, jak nieszczelne są te wszystkie systemy. Jestem tylko płotką. Ale są tacy, którzy wiedzą znacznie więcej ode mnie.

Nie miałem zamiaru walczyć z nimi. Zresztą byli bardzo przyjacielscy. Zapytali nawet, co myślę o Amerykanach. W spotkaniu uczestniczyło również kilku przedstawicieli uniwersytetu. Amerykanie powtarzali «spokojnie, spokojnie», ale tam w końcu było dziewięć osób. Agenci znali wszystkie szczegóły z mego życia. Chcieli rozmawiać o komputerach wojskowych. Kiedy rozmowa zeszła na temat sieci Milnet, odmówiłem odpowiedzi. Uznali to za brak chęci do współpracy. Zapytali o program, który napisałem w celu wykorzystania nieszczelności w sieciach, więc naszkicowałem wszystko na tablicy i wyjaśniłem zasady działania.

Zebranie trwało siedem godzin".

Z punktu widzenia władz brytyjskich przypadek Singha nadawał się do umorzenia. Nie wniesiono oskarżenia o włamanie ani o obciążenie go kosztami na rzecz uniwersytetu, gdyż ten rozliczał się ryczałtem niezależnym od liczby użytkowników i czasu trwania sesji. Nie było żadnych dowodów zniszczeń systemów lub zbiorów i w końcu oskarżono go o drobną sprawę kradzieży uniwersyteckiego papieru, na którym drukował. śledztwo zostało przekazane w ręce brytyjskich służb specjalnych, a wtedy wyszło na jaw, że miał on dostęp do systemu ASWRE i innych komputerów ministerstwa obrony. Nie znaleziono jednak żadnych dowodów świadczących o wykorzystaniu jakichkolwiek materiałów z zawartych tam zbiorów. Rozgłos towarzyszący całej sprawie wywołał oddźwięk w postaci kilku pytań zadanych przez parlamentarzystów, a dotyczących obrony tajnych informacji wojskowych zgromadzonych w pamięci brytyjskich komputerów. Prokurator Archie Hamilton obiecał zbadać sprawę dostępu do wojskowych systemów po stwierdzeniu przez jednego z deputowanych, że Singh miałby szansę na zniszczenie wewnętrznego systemu NATO i spowodowanie poważnego zagrożenia dla świata. Przypadek Singha spowodował ponadto zdyskredytowanie Ustawy o Ochronie Tajemnicy. Poczucie bezsilności sędziów było oczywiste i wszyscy zdawali sobie sprawę, że nikt nie może być osądzony na podstawie tak nieaktualnego aktu prawnego, ale w marcu 1990 roku nowe przepisy były nadal opracowywane. W tej sytuacji sprawa Singha została umorzona. Nikt nie miał zamiaru uczynić z niego męczennika. Aresztowanie Singha i śledztwo w jego sprawie nie przeszło jednak bez echa. Spora część brytyjskich hakerów, którzy znali go poprzez komputerowe biuletyny, zaprzestała działalności na wieść o aresztowaniu

Uniewinnienie Singha zawiodło jednak oczekiwanie amerykańskich władz. Jego wspólnicy w USA poddani zostali długiemu postępowaniu wyjaśniającemu. Na dom „MH", trzeciego członka „Triady", policja przeprowadziła najazd jesienią 1988 roku, zaraz po aresztowaniu Singha. Ostatecznie ani wobec niego, ani wobec Kleina, który zgodził się na współpracę z władzami, nie wyciągnięto żadnych konsekwencji. Nie znaleziono dowodów, które wskazywałyby na szkodliwość ich czynów. „MH" był w tym czasie studentem. Klein miał nadzieję podjąć pracę w branży informatycznej.

W rok po aresztowaniu Singha, w centrum komputerowym Uniwersytetu Surrey wciąż pamiętano o jego przypadku.

Hans Hübner

Krótko mówiąc — jest to włamywacz z Berlina Zachodniego, należący do grupy mającej na swym koncie liczne włamania do amerykańskich komputerów. Ale dokonania te nie były tylko zabawą. Grupa, która utrzymywała swą działalność w tajemnicy przed innymi członkami Klubu Komputerowego Chaosu, nawiązała kontakt z Rosjanami z Berlina Zachodniego.

Siedząc w swym mieszkaniu w Berlinie Zachodnim w marcu 1989, dwudziestotrzyletni Hübner opowiadał szczerze o swych powiązaniach. Nie odegrał w tym incydencie szpiegowskim dużej roli, ale przyznał, że utrzymywał kontakty z ludźmi z bloku wschodniego. Został za to aresztowany, oskarżony o szpiegostwo i zatrzymany w więzieniu do momentu, w którym zgodził się współpracę.

Pierwsze kontakty w Berlinie Wschodnim Hübner nawiązał w 1986 roku. Wspomina:

„Byłem tylko włamywaczem i jedyne, co mnie interesowało, to dostęp do bardziej wyrafinowanego sprzętu. Zamierzaliśmy zdobyć możliwie najlepsze wyposażenie. Pomyślałem, że oni wyłożą pieniądze. Nie zastanawiałem się wtedy nad konsekwencjami. W naszej grupie byli ludzie z Hanoweru i Berlina Zachodniego. Miałem wtedy 17 lat i nie przypuszczałem, że człowiek którego spotkaliśmy w Berlinie Wschodnim był agentem KGB. Miał na imię Serge albo Seriej. Chciał, abyśmy zdobyli określone oprogramowanie i był gotów za nie zapłacić. Nie różniło się to niczym od tego, co dotąd robiłem. Jeśli potrzebowałem jakiegoś programu, to po prostu go kopiowałem. Teraz chciałem mieć lepszy sprzęt, a ten człowiek mógł mi pomóc w realizacji tych zamierzeń. Nie były mi nawet potrzebne pieniądze. Potrzebowałem sprawniejszego komputera, nieograniczonego rachunku na połączenia telefoniczne i miejsca, w którym mógłby spokojnie pracować.

Spotkałem się z tym człowiekiem tylko raz. Nie miał zielonego pojęcia o szczegółach technicznych. Powiedział, że owszem zapłaci za informacje o charakterze wojskowym, ale głównie interesował go system operacyjny Digital VMS — wspomina Hübner. Próbowałem to zrobić, ale zadanie było nie do wykonania. Po prostu komputer, którym dysponowałem był za wolny, aby operować programami o pojemności megabajtów. Nie mogłem przecież pójść do Digitala, żeby kupić oryginalny egzemplarz oprogramowania. Nie jestem szaleńcem! Dostarczyłem więc Rosjanom trochę informacji, ale nie były to ani hasła, ani żadne tajne materiały”.

Drugim członkiem grupy był student z Hanoweru — Karl Koch. Jak twierdzi Hübner:

„Zaproponował on, aby przekazać Rosjanom hasła do systemów amerykańskich. Byłem temu przeciwny, ale Koch uwielbiał konspirację. Kreował się na jednego z tych, co mogą zbawić świat”.

Hans Hübner nie był jedynym, który nawiązał kontakty po wschodniej stronie. Wcześniej takie kontakty utrzymywali inni. Nie było również prawdą, że sam wszystko zorganizował. wielu ludzi było „po tamtej stronie” znacznie wcześniej.

Specjalnością Hübnera był system Unix, który udało mu się opanować, kiedy pracował jako konsultant komputerowy, ale jego ulubionym obiektem włamań pozostał system operacyjny Digital VMS. Wykorzystywał nieszczelności we wcześniejszych jego wersjach. Większość z nich została usunięta po licznych włamaniach do NASA. Próbował również penetrować systemy krajów Europy Wschodniej, ale bez większych sukcesów. Przyznaje jednak, że:

„W Związku Radzieckim zdołaliśmy jedynie zdobyć numery połączeń telefonicznych, ale w Jugosławii dotarliśmy do niektórych komputerów. Natomiast w USA opanowałem wojskowy komputer Optimis i elektroniczną pocztę obsługującą amerykańskich oficerów. Była tam też baza danych obejmująca różne jawne informacje. Moi koledzy penetrowali Thomsona-Philipsa, który również pracuje na rzecz wojska. Nie pamiętam, czy dostałem się do Lawrence Berkley Laboratory. Kiedyś trafiliśmy na komputer policji w Ottawie. Nie wiem, czy był to już pracujący, czy dopiero uruchamiany system, ale znaleźliśmy tam mnóstwo danych personalnych różnych ludzi. Nie udało nam się uruchomić głównego programu i zanim znaleźliśmy rozwiązanie zostaliśmy wyrzuceni, a komputer odłączono od sieci ogólnej".

Współpracę ze swą grupą Hübner przerwał na początku 1988 roku, ale handel ze wschodnimi sąsiadami ustał znacznie wcześniej. W czerwcu poprzez pośrednika nawiązał kontakt z Verfassungschutzm, odpowiednikiem brytyjskiego kontrwywiadu M15.

Policja rozpoczęła dochodzenie i 2 marca 1989 roku zatrzymano ponad dwudziestu hakerów. Nieco później — w 1989 roku — trzech Niemców zostało oskarżonych o szpiegostwo na rzecz Rosjan. Hübner pozostał na uboczu. Prowadzący dochodzenie byli usatysfakcjonowani, że zgodził się na współpracę i nie przekazał żadnych poufnych informacji na Wschód. Wśród oskarżonych znaleźli się Markus Hess, Peter Carl i programista Dirk Brzezinski. W styczniu 1990 roku postawiono ich przed sądem w Dolnej Saksonii. Na świadka został wezwany dr Clifford Stoll. W podróży do Niemiec towarzyszył mu agent FBI.

Clifford Stoll

Latem 1986 roku astronom dr Clifford Stoll rozpoczął tworzenie systemu informatycznego w LBL (*Lawrence Berkley Laboratories*) w Kalifornii z zamiarem stworzenia modelu zjawisk astronomicznych. Rozpoczął od przeglądu sprzętu należącego

do uniwersytetu. Przy tym zainteresował się także rachunkami płaconymi przez uczelnię za usługi komputerowe. W jednym z nich zauważył niedokładność w wysokości 75 centów.

Rachunek, który zbadał, należał do osoby, która nie pracowała na uniwersytecie. Obserwacje prowadzone przez kilka następnych miesięcy doprowadziły do wniosku, że ktoś wykorzystuje komputery LBL do połączeń z siecią Milnet, obsługującą producentów uzbrojenia, ośrodki akademickie i bazy wojskowe. Wysokiej klasy włamywacz, który korzystał z całej masy haseł i kodów, penetrował również większość komputerów laboratorium. W rzeczywistości włamywacz pomylił laboratorium Lawrence Berkley z Lawrence Livermore, które na zlecenie Pentagonu zajmowało się badaniami nad bronią nuklearną.

Zdążając śladami tajemniczego włamywacza, Stoll dotarł do informacji o planach obrony strategicznej, broni nuklearnej i chemicznej, obronie powietrznej, ekspedycjach kosmicznych i planach na wypadek kryzysu prezydenckiego. Włamywacz, który był tak uparty w swoich poszukiwaniach, jak Stoll w jego tropieniu, dotarł do laboratorium nuklearnego w Los Alamos, a ściślej — do komputera armii amerykańskiej Optimis i wielu innych wojskowych instalacji USA. Raz zdarzył się przypadek interwencji ze strony Narodowego Centrum Bezpieczeństwa Komputerowego, które ostrzegało LBL o próbach wejścia w ich system. Z komputera Dowództwa Obrony Wybrzeża na Florydzie włamywacz skopiował zbiór chroniony zaszyfrowanym hasłem i po jakimś czasie, mając go do dyspozycji, powrócił, odczytując resztę zbiorów. Na jego liście znalazł się również baza Fort Buckner w Japonii, skład wojskowy w Alabamie i Dowództwo Sił Powietrznych w El Segundo w Kalifornii. Opowiadał o tym następująco:

„Obserwowałem, jak przegląda ich zbiory. Potem zaczął drukować informacje o promie kosmicznym. Przedstawiciele Sił Powietrznych stwierdzili jednak, że nie są one tajne. Kiedy zastanawiam się nad tym, dochodzę do wniosku, że działalność włamywacza można by porównać do spaceru wzdłuż ulicy i sprawdzania drzwi każdego domu. Jeśli są zamknięte, to szuka się tylnych drzwi, a potem sprawdza okna. Kiedy wszystkie wejścia okażą się zamknięte, należy zająć się następnym domem".

Poszukując nieszczelności we systemie obserwowany włamywacz uzyskał przywilej administratora systemu LBL. Stoll przekonał władze uczelni, żeby zamiast zmieniać hasła i odcinać włamywaczowi dostęp do systemu, lepiej będzie przez jakiś czas przyglądać się jego poczynaniom, by później zawiadomić policję i FBI.

Trudno było skłonić policję do działania, gdy Stoll poinformował o stracie (75 centów), którą przyniosły działania hakera.

Mimo to Stoll nadal obserwował działalność włamywacza. Ale to jego żona doradziła mu, by założył specjalne łącze telefoniczne w celu wyśledzenia drogi połączeń. I Stoll stworzył minisieć, wypełnił zbiory informacjami na temat wojen gwiezdnych, a później już tylko czekał. Miał nadzieję, że włamywacz poświęci sporo czasu na przejrzenie danych i w ten sposób uda się go zlokalizować.

Plan sprawdził się. W ciągu dwóch godzin, w trakcie których włamywacz przeszukiwał podsunięte mu zbiory, inżynierowie łączności odtworzyli drogę połączenia prowadzącą poprzez sieć producenta uzbrojenia w Wirginii i uniwersytetu w Bremie do Hanoweru. Za pomocą władz niemieckich ustalono personalia włamywacza, ale nie aresztowano go. Policja chciała przyłapać go na gorącym uczynku.

Zbiory stworzone na przynętę zawierały jeszcze jeden haczyk. Podano tam bowiem adres w Berkley, pod którym rzekomo można było otrzymać dodatkowe informacje na temat wojen gwiezdnych. Trzy miesiące później przyszedł list powołujący się na tę wiadomość. Przekazano go FBI i sprawa ożyła. Ostatecznie w czerwcu 1987 roku aresztowano w Niemczech Markusa Hessa. Włamania do systemu LBL zakończyły się.

Stoll postanowił spisać swoje komputerowe doświadczenia i rozpoczął pracę nad książką *The Cuckoo's Egg*, która niedawno ukazała się w Polsce.

Agent Steal (Peterson, Justin)

Znany jako Samuel Grossman lub Eric Heinz, Peterson zasłynął z włamania do instytucji przydzielającej kredyty konsumenckie. Po złapaniu wydał swoich znajomych (między innymi słynnego Kevina Poulsena). Później jako tajny agent pracował dla FBI. Dzięki temu udało mu się wyjść na wolność... Ale szybko porzucił pracę tajnego agenta, by znów stanąć po ciemnej stronie. Obecnie mieszka w luksusowym apartamencie w Los Angeles, gdzie ma komfortowo urządzone biuro. Pracuje na Win2k zainstalowanym na komputerze z podwójnym procesorem 700 mhz P-3s, 2x20 GB HDD, Ata 100s, 256 MB RAM i podwójnej karcie video — Matrox. Oba monitory są połączone do maszyny i dają w sumie całkowity desktop 2048x768. Jest włączony do sieci poprzez modem SDSL (800 kbs). Następny komputer ma zainstalowany system BSDI 4.0. Nigdy nie rozstaje się z laptopem, na którym zainstalowany jest Winows 98. Nic dziwnego, że tak doskonały sprzęt pobudza jego wirtualne fantazje... Ostatnim wyczynem była jednak nieudana próba dokonania przez Internet fałszywej transakcji opiewającej na setki tysięcy dolarów.

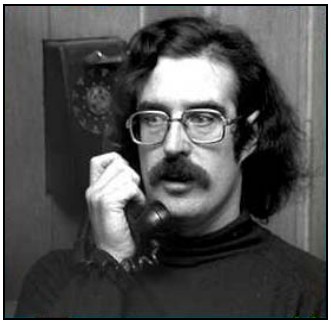
Cap'n Crunch (John Draper)

Ten niezły haker stał się sławny dzięki... umiejętności gwizdania na opakowaniu pieczywa Cap'n Crunch. Potrafił wydawać dźwięk o częstotliwości 2600 herców pozwalający na uzyskanie darmowego połączenia!

Na początku lat siedemdziesiątych Draper pomógł Steve'owi Jobs i Steve'owi Wozniakowi — późniejszym twórcom komputera Apple — w zaprojektowaniu niebieskiej skrzynki.

Pomimo swej przeszłości Draper jest obecnie cenionym konsultantem do spraw bezpieczeństwa w Internecie.

Andriej Rublov i jego przyjaciele



Grupa hakerów z republik kaukaskich — prawdopodobnie Czeczeńców — w 1994 roku w czasie jednego „skoku" dokonała w rosyjskich bankach rozmaitych fałszerstw, które umożliwiły następnego dnia wypłacenie 300 000 000 dolarów. Niezależne źródła w Moskwie uważają, że włamań takich było kilka i doprowadziły one na początku 1995 roku do poważnego kryzysu w rosyjskim systemie bankowym. Ile więc ukradli naprawdę czeczeńscy hakerzy — nie wiadomo. Wiadomo natomiast, że pieniądze te zasiliły partyzantów. Jedynym śladem, jaki pozostał po całej eskapadzie była krótka notka, która pojawiła się w bankowych bilansach: „Andriej Rublov i jego druzja".

Deri S

Z izraelskiego miasteczka Karmel pochodzi 16-letni uczeń, który w 1991 roku włamał się to systemu komputerowego amerykańskiego Ministerstwa Obrony, Międzynarodowego Towarzystwa Kredytowego VISA i izraelskiej sieci telekomunikacyjnej należącej do firmy Bezeq. Świetny pokaz nie zakończył się jednak szczęśliwie. Młodociany haker wpadł przez pazerność swoich przyjaciół z USA, którzy otrzymali od niego kody kart kredytowych Visa. Dokonali oni kosztownych zakupów na cudze karty kredytowe, co zakończyło się śledztwem policyjnym i zatrzymaniem całej grupy. W trakcie przesłuchań szybko ujawnili pochodzenie kodów. Prawdopodobnie z zasobów Deriego pochodziły numery kart Visa fałszowanych przez grupę Andrzeja Gąsiorowskiego — byłego współwłaściciela Art-B.

Antoine (Anthony Chris) Zbolarski

Pewien 21-letni Francuz polskiego pochodzenia sprzedawał pirackie konsole Nintendo wraz ze stosownym oprogramowaniem. Nieco później odbywał już karę w wiezieniu Beauvais. Ale władze pozwoliły mu na korzystanie z komputera i modemu. Z nudów — jak później twierdził — naruszył zabezpieczenia zasobów top secret firm General Motors i Uniroyal. Włamał się także do systemu oprogramowania sterującego rakiet balistycznych Pentagonu. W trakcie tych komputerowych włamań podszywał się pod rezydenta SDECE (czyli francuskiego wywiadu, gdzie równiez złamał kody).

Susan Thunder z Kalifornii

Luksusowa call-girl, inwestująca wszystkie oszczędności w komputery... To nie jest urojenie, ale prawdziwa kobieta, której pasją były systemy Pentagonu. Jeśli nie mogła złamać szyfru, okradała z kluczy do niego oficerów łączności poderwanych w barach. Taki miała sposób na łączenie przyjemnego z pożytecznym. Ale nie na długo... Jako pierwsza wystąpiła w 1983 roku przed senacką komisją bezpieczeństwa z zeznaniami dotyczącymi niebezpieczeństwa łamania wojskowych systemów komputerowych. Jednak absurdów nigdy dosyć — obecnie jest wzorową żoną i matką, a w wolnych chwilach pracuje jako konsultant Pentagonu do spraw zabezpieczeń systemów komputerowych...

Tsutomu Shimomura

Były haker, ekspert do spraw bezpieczeństwa i, jak twierdzą niektórzy, sprzedawczyk, który wytropił Kevina i wydał go w ręce FBI. Obecnie żyje z książek (i scenariusza filmowego) opowiadających historię Kevina Mitnicka.

Eric Raymond

Programista, uczestnik i „duchowy" przywódca ruchu open source. Największą popularność przyniosło mu opublikowanie w Internecie w 1997 roku opracowania „The Cathedral and the Bazaar", w którym zdefiniował i opisał dwa sposoby rozwoju oprogramowania: „katedra" i „bazar" (czyli model tradycyjny i model rozwojowy — open source). W 1998 przedstawił tzw. dokumenty Halloween, czyli zbiór felietonów omawiających fenomen powodzenia Linuksa oraz open source. Dokumenty Halloween stały się w rezultacie swoistym manifestem tego ruchu.

Paranoja wynikająca z braku wiedzy

Sława Mitnicka, Morrisa czy Poulsena wynikała w dużym stopniu z paranoi, jaką przeżywały Stany Zjednoczone w latach 80. i która po części przeniosła się w obecne dziesięciolecie (co widać na przykładzie szumu, jaki media zrobiły wokół włamań dokonanych przez Analyzera i Makaveliego). Hakerzy przedstawiani więc byli jako groźni przestępcy, ale motywy i metody ich działań pozostawały nieznane.

A hakerstwo nie jest dążeniem zarezerwowanym dla jednego obszaru sieci, państwa czy jednej grupy społecznej. Chęć zdobywania wiedzy, nabywania nowych umiejętności charakteryzuje młodych ludzi z każdego zakątka kuli ziemskiej.

Hakerski underground na Wschodzie

UGI — przeszłość, teraźniejszość i... przyszłość

Wiele lat temu wielu młodych, naiwnych ludzi przesiadywało w rosyjskich Pałacach Pionierów, uczestnicząc w tzw. kółkach komputerowych, gdzie pod okiem instruktorów uczyli się podstaw programowania. Od tego właśnie z wolna zaczął się kształtować rosyjski komputerowy underground oraz idea powstania UGI.

Jak to się zdarzyło? Był 1 grudnia 1987 roku. Wtedy właśnie < PC<C>H>, późniejszy Joyrider i jego szkolni koledzy Batman i Andy alias Power Ace, którzy mieli dość patrzenia się na obce winiety grup hakerskich (na C64 Atari ST) nagle uświadomili sobie, że na JBM-ach można zrobić coś podobnego. Właśnie wtedy w rosyjskim światku komputerowym, zaczęły się pojawiać pierwsze info-pliki i prymitywne winiety w pseudografice ANSI prezentujące grupy, takie jak: THG (*The Humble Group*) i INC (*Internationale Crackers*) późniejsza (*International Network of Cracks*). Już wtedy miały one swoje BBS-y, rosyjscy hakerzy jeszcze nie zdawali sobie nawet sprawy z możliwości modemu.

Rosjanie stawiali wówczas pierwsze kroki w transmisji modemowej. Kiedy EC-1840 uważany był za duże osiągnięcie radzieckiego przemysłu, a godzina pracy na nim kosztowała 1 rubla i 60 kopiejek na dość znanej starszym graczom Smolence, świeżo powstała grupa hakerów posiadała w swoim arsenale komputerowym: AMSTRAD 1512 XT 8 MHz /2x360 KB / CGA, Beltorn Datasform (XT 10 MHz /20 MB HDD) 1x360 KB /CGA i Datamini 125 (286/12 MHz/40 MB HDD/2x1, 2kb/EGA). Był to czas kiedy Joyrider spędzał wiele dni za granicą i zdobył przyjaciół w Londynie i Nowym Yorku. Przyjaźń ta zaowocowała późniejszą współpracą. Po powrocie do kraju Joyrider i jego rosyjscy koledzy regularnie otrzymywali niewielkie przesyłki z dyskietkami (innej drogi wówczas nie było), które przywozili do Moskwy ich znajomi. Były to czasy, w których rekordy popularności na Zachodzie święciła gra Kings Quest IV (mieszczące się na 9 dyskietkach 360 kB) i wielu ówczesnych hakerów nie przypuszczało nawet, że może się ona pojawić w Moskwie. A pewnego pięknego dnia pudełko z tą właśnie grą Joyrider otrzymał z Londynu. Szybko zrobił kopie drogocennych oryginałów i przyniósł je na Smolenkę. Jednak nie udało się uruchomić KQ IV na Nejronie z 256 kB pamięci. Joyrider został publicznie wyśmiany i parę godzin później obmyślał już plan zemsty. W domu szybko siadł do swojego Beltrona i zaczął tworzyć plik tekstowy, którym wyszczególnił wszystkie problemy związane z grą. Nikt z UGH (*Unitet Group*) wtedy jeszcze nie wiedział, że grę można scrackować...

Ale to były dopiero początki grupy. Plik szybko przeczytali inni i także dołączyli swoje spostrzeżenia i numery telefonu oraz adresy elektroniczne. Joyrider nie zastanawiał się długo. Postanowił wybrać się jak najszybciej do znanej mu grupy

hakerskiej na Szabłowce, gdzie na komputerze EC-1840 olśnił obecnych przy tym hakerów, uruchamiając plik *sierra.exe* z pierwszej dyskietki. Z pewnymi wszakże kłopotami, ale jednak pomyślnie udało się członkom grupy na Szabłowce zebrać dziewięć dyskietek (w tym czasie nosili oni przy sobie jedną, ewentualnie dwie dyskietki, co było szczytem możliwości finansowych) i za pomocą magicznego programu Pctools Deluxe i jego opcji „discopy", w ciągu godziny Kings Quest V został przez nich skopiowany. Po tym fakcie działalność GI trochę przycichła. Joyrider w dalszym ciągu otrzymywał gry z zagranicy i rozdawał je innym członkom grupy.

Telefon

Pewnego razu po powrocie z uczelni Joyrider zobaczył w progu swego domu zaniepokojonych rodziców, którzy poinformowali go, że dzwonił ktoś w sprawie gry komputerowej. W trakcie rozmowy okazało się, że ów nieznajomy posiadał wyrazisty akcent i pozostawił numer telefonu, pod którym będzie dostępny w jakiejś restauracji. Szybko okazało się, iż był to człowiek z Nowosybirska, który przeczytał plik *info* i chciał przegrać gry. Spotkanie odbyło się na podwórku i gość z Nowosybirska usłyszał od Joyridera, że musi pójść do kolegi, aby przegrać wszystkie gry (obowiązywała pełna konspiracja).W rezultacie wymiana nie doszła do skutku, ponieważ ów tajemniczy pan zaproponował w ramach rewanżu stare gry, które w Moskwie były już od dawna.

W tym czasie Joyrider i jego koledzy wykonali już sporo ansi obrazków, które włożyli do wszystkich archiwów, jakie były w ich posiadaniu. Wkrótce rozdzwoniły się telefony. Bardzo szybko wyłonił się krąg znajomych, posiadających swoje kanały, którymi otrzymywali gry i inne oprogramowanie.

Joyrider został zmuszony do nabycia Strymera (20 MB taśmy) i nieco później zaczął zbierać wszystkie możliwe gry i programy, by następnie przegrywać je na kasety (taśmy).Te właśnie taśmy i Strymer pomoły UGI rozpocząć pierwsze kroki prowadzące do sławy w sieci elektronicznej. Członkowie grupy szybko stali się właścicielami największej kolekcji gier w Moskwie. Czasami przyjeżdżający ludzie mówili, że podobną kolekcję posiadał ktoś w Tallinie, ale że trudno ją porównać z kolekcją Joyridera. Trzeba tu zaznaczyć, że był to okres, kiedy jeszcze bez trudu można było prześledzić wszystko, co wchodziło na rynek i każda gra spotykała się z zachwytem i analizowana była minimum kilkanaście dni. Obecnie wymazuje się na warezowych BBS- ach tygodniowe archiwa, w efekcie czego czasem nie ma nawet szansy na ich przejrzenie. Krótko mówiąc — droga do sławy UGI rozpoczęła się. Joyrider na wzór zachodnich hakerów, tworzył info-pliki i nagrywał wszystko na coraz większej ilości strymerowych taśm.

Modem

Wszystko trwało parę lat. W tym czasie niektórzy członkowie UGI zdążyli „wyjść" z grupy i stworzyć na jej wzór coś swojego (ani jedna z tych grup nie przetrwała więcej niż rok i obecnie nikt nie pamięta takich nazw jak: The Bears, McL, Blade-

runners). Ale pewnego razu jeden ze znajomych Joyridera oznajmił mu, że zaopatrzył się w dziwne urządzenie, które nazywa się „modem". Powiedział także, że w Moskwie jest już nawet jeden BBS (*Dialogue BBS*). Joyrider pospiesznie nabył nowe urządzenie i zaczął wydzwaniać na działający już od ponad miesiąca BBS. Zarejestrował się w nim i zgłębiał polecenia systemu, w czym pomagał mu operator systemu BBS. Znał on każdego użytkownika swojego systemu i miał wystarczająco dużo czasu, by kontaktować się z nimi. Jak to zwykle bywa po dwóch tygodniach od pierwszego wyemitowania programu MTEZ (wszyscy pamiętają to cudo z programową emulacją MNP) powstały trzy oddzielne BBS-y grupy UGI (UG#1 BBS, a następnie UG#2 BBS i UG#3 BBS). Kilka miesięcy później UG#1 BBS zaczął nazywać się Players DREAM, UG#2 BBS — Silent Station, a UG#3 BBS zawiesił działalność. Od tego momentu rozpoczęło się upowszechnienie UG#l wśród ludzi. Na Players Dream nie można było w ogóle się dodzwonić. Megabajty danych przez modem 9600 b/s spływały cały dzień i noc. W dzień oficjalnie BBS-y nie pracowały, ale mimo to bardzo często dzwonili do BBS-ów ludzie (nierzadko z innych miast) i prosili, aby im pozwolić coś ściągnąć, gdyż uporczywie, choć bezskutecznie starali się wcześniej przez kilka nocy nawiązać połączenie. Niemal błagali o listę plików. Trzeba im było pomóc. Rodzice Joyridera i innych hakerów byli w szoku po pojawieniu się modemu. Ich życie przekształciło się w koszmar — z telefonu nie można już było korzystać normalnie, a nocą bez przerwy rozlegały się dokuczliwe piski dochodzące z modemu. To było strasznie denerwujące. Joyrider był jednak maniakalnie zafascynowany modemami i UGI.

UGI (*UNITED GROUP INTERNATIONAL*)

Nie wielu z pewnością wie, że UGI to wcześniejsze UG, które dołączyło do swej nazwy przymiotnik „international". Był to ukłon w stronę ówczesnej mody, gdyż wszystkie sławne grupy posiadały wtedy skróty trzyliterowe (np. KGB). Kiedy Joyrider zadzwonił do Tallina na jeden z postępowych BBS-ów (wtedy jeszcze nie było podziału na elitę i lamerów), zobaczył winietę tallińskiego BBS-u. Wcześniej już próbował się dodzwonić do Stanów Zjednoczonych, ale ciągle miał sygnał zajętej linii albo informację, żeby zadzwonił później. Jego próby nie zakończyły się sukcesem. Natomiast do Finlandii udało mu się dodzwonić od razu. Spotkanie było oszałamiające — fiński sysop nie wierzył, że do niego dzwonią z Moskwy. Otrzymał od niego spis zasobów i jak narkoman na głodzie zaczął ściągać wszystko. Po miesiącu przyszły rachunki. Nie trzeba chyba dodawać, że były bardzo wysokie. Może dlatego właśnie Joyrider zaczął zastanawiać się, co zrobić, by były niższe. Rozwiązaniem okazało się nawiązywanie połączeń pod cudzym numerem. Joyrider i jego koledzy robili to nocą, ukryci w piwnicy, siedząc na plastikowych skrzynkach po butelkach, przy słabym świetle lampy. Modem sprytnie migał diodami, a oni jak zaczarowani wodzili palcami po matrycy monitora, z rzadka dając ujście radości, gdy oglądali długo oczekiwane nowinki, lub załamując się i ze strachem spoglądając do góry, gdzie wyraźnie były słyszane kroki mieszkańców parteru.

Coraz częściej nawiązywali kontakty z Finlandią, Szwecją, USA. I tak zostali grupą międzynarodową. Po pewnym czasie zaczęły do nich napływać gry i programy, kierowane z Tallina czy Rygi (tam najwcześniej pojawili się hakerzy.

Wiele tysięcy ludzi dowiedziało się o UGI. W dalszym ciągu kontynuowali rozdawanie gier i programów. Dla ludzi robili specjalne listy posiadanych archiwów i zamieszczali je w plikach *info*. Rozmiary archiwum, które było w ich posiadaniu, zaczęły przypominać powiększającą się kulę śniegową. Joyrider coraz częściej czuł, że sytuacja zaczyna wymykać się spod kontroli.

Mieli jednak bogaty wybór numerów telefonicznych zdobytych wcześnie. Po miesiącu dzięki namowom Joyridera opuścili zajmowane pomieszczenie, akurat wtedy, gdy policja zaczęła węszyć. W tym czasie nabijali rachunki na kilka milionów, ponieważ modem nie wyłączał się nawet na minutę. Wierni członkowie UGI zmieniali się nawzajem na posterunku z zadziwiającą regularnością raz na dobę „wynosząc na wolność" kilka paczek dyskietek nabitych drogocennym warezem. W Moskwie było wówczas około 20-30 działających aktywnie BBS-ów. Zabawa trwała dość długo, ale stawała się coraz bardziej niebezpieczna i kosztowna. Joyrider i jego koledzy z grupy skończyli studia i rozpierzchli się po kantorach lub urzędach telekomunikacji, gdzie po cichu kontynuowali wydzwanianie do odległych miejsc. Wówczas wiele BBS-ów wchodziło w zarząd członków grupy UGI.

Aktualnie w grupie w UGI działa Joyrider, Power Ace, Man Hunter, Vidator, Kaltenbruner. Z pozostałymi natomiast nie ma kontaktu, ale na pewno pamiętają, że należeli do najbardziej legendarnej i znanej rosyjskiej grupy, która nieustannie zajmowała czołowe miejsca na listach top BBS-ów w Europie.

Do tych, którzy najbardziej odcisnęli swoje piętno w historii UGI należą:

- *Joyrider* (powstanie, kariera, grafika, zarabianie pieniędzy);
- *Power Ace* (grafika, kierownicza funkcja w jednej z wielkich agend graficznych);
- *Man Hunter* (coding, cracking, phreacking);
- *Sted Rat* (coding, overlook);
- *Vidator* (represje ze strony policji, aktualnie — żona, rodzina..., dzieci i Amiga);
- *Demoniak* (DELTA CITY BBS, coding, cracking);
- *Bat Man* (założyciel);
- *Creasy Bear* (organizowanie działalności).

O wszystkich tych ludziach opowiadano wiele śmiesznych historii. W swoim czasie tworzyli oni z pełnym poświęceniem rosyjski komputerowy underground. Niektórzy tworzą go do dzisiaj aktywnie.

CCC — Chaos Computer Club

Elita hakerska zza Odry

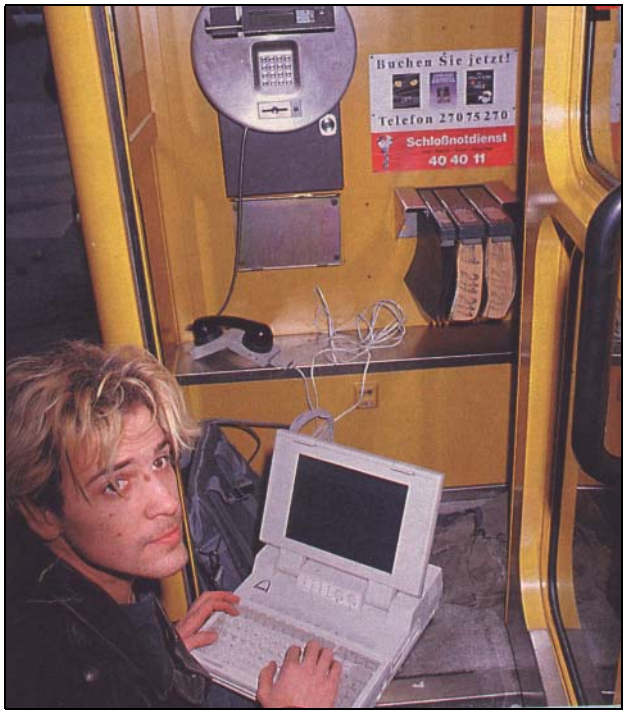
W obecnych czasach stało się jasne, że komputery zwyciężyły świat. Banki danych magazynują naukowe, gospodarcze, wojskowe lub osobiste informacje, które można wymieniać poprzez Sieć. Bardzo często przyczynia się to do zwycięstwa nad innymi czy przejęcia kontroli. Należy złamać kod, aby przeczytać dane i wykorzystać je do własnych celów. Ale przecież każdy system ma luki w zabezpieczeniach. Hamburski Klub Komputerowego Chaosu (CCC) pokazuje od 10 lat, gdzie takie dziury są.

Powstał on jako porozumienie trzech przyjaciół: Hansa Hubnera, Karla Kocha i Marcusa Hessa. Od 1987 roku włamywali się oni do systemów amerykańskiego Ministerstwa Obrony i sprzedawali uzyskane dane agentowi KGB o pseudonimie Serge. W 1990 roku po zjednoczeniu Niemiec wszystkich aresztowano. Koch, uwolniony na polecenie prokuratora jako „wabik" na agentów, został zamordowany przez KGB, Hubner i Hess jako szpiedzy odsiadują kary więzienia. Prawdopodobnie w zamian za współpracę z policją zostali jednak w październiku 1998 roku zwolnieni.

Pomieszczenia klubowe CCC znajdują się w... jednej z piwnic północnego Hamburga.

Odwiedziłam ją w pewien deszczowy wieczór. W małej bocznej uliczce przed starymi budynkami czynszowymi rosną wysokie drzewa. Spokojna dzielnica dla całkiem normalnych obywateli. Dom numer 85 ma niski parter. Można wejść po kilku schodkach. Przez szybę nie widać nic. Krótki dzwonek i drzwi się otwierają. W małym pomieszczeniu stoją dookoła stare kanapy. Na półkach leżą stare skoroszyty, akta. Na korkowej tablicy zawieszone są karteczki, listy, numery telefonów.

Przez wąski przedpokój wchodzi się do położonego z tyłu pokoju. Dwa komputery i wielki napis: Witamy w Komputerowym Klubie Chaosu! Ciekawe, czy są jeszcze w tym domu hakerzy, o których czyta się tak wiele. Banki, uniwersytety, tajne służby, również Pentagon i NASA zaczynają się przecież trząść, jeśli tylko słyszą te przeklętą przez nich nazwę — haker.



Członkowie tej elitarnej grupy hakerów dość niechętnie odpowiadają na zadawane pytania. Zwykle wypowiadają jedynie ogólne stwierdzenia.

„Chcemy ryzyka i szansy na poznanie rozmaitych technik informacji — wyjaśnia Ralf (lat 23) — i to jest celem naszego klubu. Czasy hakerstwa mamy już za sobą. Mit, którym obrósł nasz klub, powstał przez spektakularne akcje. W 1984 roku jeden z hakerów CCC manipulował siecią i komputerem bankowym. Trzy lata później hakerzy z CCC władali siecią komputerową NASA i klub przejął kontrolę nad dużą ilością systemów. Choć prywatnie nikt tego nie wykorzystywał, zawsze mieliśmy problemy z policją. Ale są także ludzie, którzy nas wspierają — np. hamburska organizacja do spraw ochrony danych. Bez niej nie mielibyśmy żadnych środków. Powoli także firmy zmieniają swoje myślenie. Jest lepiej kiedy młodzi fachowcy są potrzebni i wykorzystywani przez firmy, bo nie mają wtedy ochoty na inne nielegalne działania. Dzisiaj wiszą na naszej tablicy pytania kierowane z całych Niemiec. Są to także oferty pracy. Dlaczego zatem członkowie klubu CCC są częściej poszukiwani niż eksperci z Unii Europejskiej? My trudnimy się tym o wiele dłużej i bezpieczniej niż oni”.

Nie wszystkie informacje są zabezpieczone. Klub liczy sobie około dwudziestu stałych członków, którzy spotykają się co tydzień. Dyskutują na temat nowych zabezpieczeń czy urządzeń, mówią o programach i wymieniają doświadczenia. CCC ma też swoje oddziały w innych miastach. Dwustu pięćdziesięciu członków należy do stowarzyszenia, a dziewięćset zainteresowanych informuje się regularnie wykorzystując do tego celu swoją pracę. Czytają klubowe czasopismo. Klub CCC organizuje własne seminaria, kongresy, bierze udział w targach i prowadzi archiwum prasowe.

Na pytanie o to, czy są jakieś granice działalności klubu, Ralf odpowiada:

„Nie zabezpieczamy danych, które dla obywateli powinny być dostępne, na przykład te dotyczące zanieczyszczenia wody i zawartości ozonu. Dzięki niewielkim środkom wspierającym można nawet oszukać pocztę i dzięki miejscowej taryfie telefonować po całym świecie. Teraz eksperci szukają możliwości ochrony zabezpieczeń".

Do rozmowy włączył się również Andy (lat 21), student informatyki i technik informacyjnych, który wszedł do klubu w roku 1986. Jak wyznał:

„Widzę i oceniam pracę z komputerem jako pełnię komunikacji. Przede wszystkim — jako zakrojoną na cały świat wymianę myśli".

Do klubu należy także Ron (lat 21), student elektrotechniki, który wszedł do klubu CCC przez hamburski mailbox. Swoje hobby uważa on za wyższą formę stosunków międzyludzkich. Tego zdania jest Robert (lat 24), student informatyki, praktycznie na okrągło pracujący na komputerze. Wszedł do klubu w czasie kongresu. Jak twierdzi:

„Nie można ciągle pracować w samotności. Zespół taki jak CCC jest lepszy".

Przyjaciółka Roberta – Jessica (lat 24) — interesuje się bardzo jego hobby, choć zawodowo nie ma z tym nic wspólnego.

Natomiast Alex (lat 18), uczeń, uważa, że:

„Na szczycie może być każdy, ale żeby dostac się na Mount Everest trzeba być hakerem".

Alex pisze programy. Jego przyjaciółka — Aneke (lat 16) — nie podziela tych zainteresowań. Wypróbowała komputer najwyżej raz.

Pod hamburskim telefonem 49 03 757 stale dyżuruje któryś z klubowiczów. Można bez problemu nawiązać kontakt.

Najbardziej interesujące włamania były i będą zawsze dziełem elitarnych hakerów, kierujących się ciekawością, a nie chęcią wzbogacenia. Grupa związana ze słynnym Klubem Komputerowego Chaosu znalazła na przykład błąd w wersjach 4.4 i 4.5 systemu operacyjnego VMS, który pozwolił im włamać się do 135 sieci na całym

świecie. Na ich liście znalazło się Centrum Analityczne Fizyki Kosmosu (SPAN), którego sieć obejmuje wiele krajów. Jednym z jego odgałęzień jest system amerykańskiej agencji kosmicznej NASA. Włamywacze świadomi powagi odkrycia, zwrócili się do klubu o pomoc oraz poinformowali Hansa Glissa, wydawcę wiodącego niemieckiego magazynu komputerowego „Dateenschutz-Berater". Wiadomości rozpowszechniane tymczasem poprzez biuletyny wywołały reakcje różnych środowisk. Administrator systemu Europejskiego Laboratorium Biologii Molekularnej w Heidelbergu rozesłał poprzez Sieć ostrzeżenie wymieniając nazwiska dwóch włamywaczy związanych z Klubem Komputerowego Chaosu. Wzywał w nim kolegów zarządzających innymi systemami do ostrożności i podjęcia akcji, która powstrzymałaby w przyszłości włamywaczy od tego rodzaju działalności.

Historia została ostatecznie wyjaśniona przez Hansa Glissa. Klub próbował wprawdzie nadać całej sprawie zabarwienie polityczne nagłaśniając ją w czasie konferencji prasowej zwołanej w Hamburgu i utrzymując, że jest w posiadaniu 200 stron wydruków komputerowych związanych z badaniami nad nowoczesnym uzbrojeniem. Rzecznik klubu Wau Holland potwierdził istnienie materiałów z badań nad nowymi broniami i analiz wypadków rakietowych. NASA w odpowiedzi poinformowała opinię publiczną, że włamywacze nie dotarli do żadnych poufnych informacji, a te, o których mowa, zostały już zakwalifikowane jako jawne.

Ujawnienie opisanych faktów stało się źródłem kłopotów nie tylko dla NASA, ale również dla firmy Digital, autora systemu VMS. Klub Komputerowego Chaosu utrzymywał, że ujawnienie potencjalnych niebezpieczeństw było koniecznością i pomogło niektórym środowiskom w uświadomieniu sobie powagi problemu. Firma Digital, zaniepokojona aferą, w trosce o swych klientów, rozesłała do wszystkich użytkowników darmową instrukcję pozwalającą na uzupełnienie błędów w oprogramowaniu. Późniejsze wersje systemu VMS zostały poprawione.

Amerykański underground

Z chwilą powstania pierwszego komputera, a później z rozwojem sieci komputerowych, powstały również mniej lub bardziej wiarygodne opowieści o hakerach włamujących się do systemów informatycznych. Prawdą jest jednak, że przestępstwa komputerowe pojawiły się wraz z wykorzystaniem pierwszych maszyn cyfrowych w bankach. Prawdziwy rozkwit nastąpił natomiast w latach 70., co związane było z masowym wykorzystywaniem Sieci do porozumiewania się i przesyłania danych. Elektroniczni włamywacze nie zawsze łamią prawo dla zysku.. Czasem, jak to miało miejsce w przypadku Kevina Mitnicka, najsłynniejszego hakera w Stanach Zjednoczonych, chodzi o udowodnienie sobie i innym własnych umiejętności. Potem dopiero zaczyna się przestępcza działalność. W USA w czasie zbrojnego napadu łupem pada przeciętnie 650 dolarów. Tymczasem elektroniczne włamania kosztują średnio instytucje finansowe 600 000 dolarów. Nic dziwnego, że w Stanach Zjednoczonych powstały najszybciej specjalne organizacje mające zwalczać skutki niszczących dane wirusów. Jedną z nich jest CERT (*Computer Emergency Response System*) założony przez Departament Obrony we współpracy z Carnegie-Mellon University. W FBI powstała specjalna grupa (*National Computer Crimes Squad*) zajmująca się tropieniem hakerów.

Jednym z ciekawszych wydarzeń ostatnich lat było złamanie przez trzech chorwackich nastolatków z Zadaru kodów zabezpieczających serwer Pentagonu. Chłopcy skopiowali również dokumenty o wysokim stopniu utajnienia, zawarte w wojskowych bazach danych (m.in. dotyczące broni nuklearnej i satelitów wojskowych). Narzędziem przestępstwa był Internet oraz program wyszukujący i deszyfrujący. Pozostawiony ślad pozwolił jednak specjalistom z Pentagonu wyśledzić sprawców włamania, które spowodowało straty sięgające kilkuset tysięcy dolarów. Departament Obrony skontaktował się z Interpolem, ten natomiast zwrócił się do lokalnej policji, która skonfiskowała sprzęt komputerowy. Hakerstwo nie jest jednak w Chorwacji działalnością nielegalną, a nauczyciele chłopców podkreślili brak złej woli i wysoki poziom umiejętności.

Jak widać, rozmaite, czasem wyjątkowo zaskakujące są przypadki, które spotykają hakerów.

Weterani

Ludzie zafascynowani rodzącą się technologią komputerową, którzy tworzyli po wojnie zręby dzisiejszej informatyki to przede wszystkim Seymour Cray, Stan Kelly-Bootle i David E. Są oni ostatnimi bodajże weteranami tamtych czasów. Trudno ich nawet nazwać hakerami. Byli to bowiem informatycy zafascynowani nową, rodzącą się technologią, a „hakowanie" w dzisiejszym rozumieniu tego słowa zrodziło się w USA dopiero na początku lat sześćdziesiątych, czyli na długo przed powstaniem elektronicznej poczty (1972 rok) czy pojawieniem się terminu „Internet" (1974 rok). W czasie, gdy funkcjonować zaczynały pierwsze komputery typu mainframe (PDP-1) praca programisty nie była tak łatwa i przyjemna jak dzisiaj. Komputery te były bardzo wolne i często informatycy, aby skrócić czas przeprowadzania różnych operacji, tworzyli specjalne „programy-skróty". W swoim żargonie nazywali je „haks". Jednym z nich (najsłynniejszym po dziś dzień) był hak stworzony w 1969 roku przez Dennisa Ritchie'ego i Kena Thompsona o nazwie... Unix.


Dennis Ritchie, Ken Thompson

Pierwsi hakerzy lat siedemdziesiątych

Z roku na rok rozwój technologii informatycznych stawał się coraz bardziej dynamiczny. Wraz z nim rosło zafascynowanie możliwościami i chęć ich dogłębnego poznania w nadziei dotarcia do nowych, nieznanych możliwości. Tak zaczął rodzić się w Stanach Zjednoczonych ruch określany dzisiaj mianem „hakowania" czy „hakerstwa" (*hacking*), który wraz z rozwojem Sieci zaczął skupiać programistów i informatyków z całego świata. Szczególnie dotkliwie odczuwali oni brak miejsca, w którym mogliby wymieniać opinie, informacje i doświadczenia. Wkrótce więc powstał specjalny wirtualny klub, który w 1978 roku utworzyło dwóch mieszkańców Chicago — Randy Sousa i Ward Christiansen. Tak powstały jeden z pierwszych w USA BBS działał dość nieregularnie. Warto jednak wspomnieć, że w tym samym czasie niezwykle dynamicznie rozwijała się również telekomunikacja, a wraz z nią — phreaking. Wtedy właśnie zaczęli działać pierwsi wielcy phreakerzy

— John Draper alias Capta'n Crunch oraz Yippie Abbie Hoffman. W 1974 roku Vinton Cerf i Robert Kahn w swoim artykule o TCP po raz pierwszy użyli terminu „Internet", zaś rok później w ramach kontraktu Air Force w Albuquerque, powstał pierwszy mikrokomputer o nazwie Altair.

Złoty Wiek

Olbrzymi wpływ na rozwój hakerstwa miały lata osiemdziesiąte, a przede wszystkim — trzy wydarzenia tamtych czasów (światowa ekspansja Internetu, wprowadzenie w 1981 roku przez IBM pierwszych komputerów osobistych PC oraz nakręcony w 1983 roku film „Gry wojenne"). Sam film sprawił, że termin „haking" stał się znany szerokiej opinii publicznej i stał się synonimem zagrożenia ze strony komputerowych fascynatów. Stereotyp złego hakera funkcjonuje w świadomości większości ludzi, a podtrzymywany jest skutecznie przez media. Internet sprawił natomiast, że haking stał się ruchem o zasięgu ogólnoświatowym. Popularność BBS-ów znacznie wzrosła. Hakerzy zaczęli łączyć się w nieformalne grupy. Co ciekawe — ich członków łączyła wówczas nie tylko komputerowa pasja i chęć zgłębiania tajników systemów, lecz również muzyka (np. zespół The Clash), styl życia, światopogląd.

Lata dziewięćdziesiąte

Końcem „ery programistów" i początkiem dominacji nowej generacji hakerów, a zarazem początkiem wojny z nimi, było prawdopodobnie założenie w 1984 roku przez hakera określającego się jako Lex Luthor grupy o nazwie Legion of Doom. Skupiała ona najlepszych z najlepszych hakerów i phreakerów. Po kilku latach powstała jednak konkurencyjna grupa Masters of Deception. Utworzyli ją dwaj byli członkowie elitarnej LOM — Phiber Optik oraz Erik Bloodaxe. Od 1990 roku obie grupy rywalizowały ze sobą. Wyglądało to jak bezkrwawe porachunki mafii. Monitorowanie rozmów telefonicznych i blokowanie linii, łamanie zabezpieczeń i wchodzenie w system przeciwnika, czyszczenie dysków twardych, podrzucanie wirusów.

Te swoiste „działania wojenne" powodowały duże straty i nie ograniczały się tylko do komputerów „wroga". Wszystkie chwyty były dozwolone. Hakowano komputery lub systemy instytucji, firm i osób prywatnych podając się za przeciwnika. I to był błąd, bowiem do akcji wkroczyła FBI. Jej działania doprowadziły do złapania niektórych hakerów (m. in. Phibera Optika i jego przyjaciół). Potem zaczęły się długotrwałe sprawy sądowe i wyroki. Panuje nawet pogląd, że wraz z zakończeniem wojny pomiędzy LOM i MOD lub nawet wcześniej, bo od 1986 roku, gdy skutki „działań wojennych" zaczęli odczuwać niewinni ludzie, zakończyła się „era programistów", hakerów-ideowców, a rozpoczął się nowy cykl — czas włamywaczy komputerowych.

Wprawdzie elitarni hakerzy istnieją nadal i strzegą granic elektronicznej cyberprzestrzeni, ale trzeba też przyznać, że obecnie rejon ten został zdominowany przez pseudohakerów. Ciemna strona hakerstwa zaczęła się ujawniać wraz z komercjalizacją Internetu. Znacznie wtedy wzrósł wpływ rządu amerykańskiego na rozwój Sieci i równolegle dostępem do technologii informatycznych zaczęto wprowadzać szereg regulacji prawnych. W 1986 roku Kongres ustanowił Federal Computer Fraud and Abuse Act. To właśnie na jego mocy skazano Phibera Optika i jego przyjaciół. Żarty się skończyły. Konsekwencje prawne nie stanowiły jednak bariery dla hakerów.

Na scenie pojawił się Robert Tappan Morris, który w 1988 roku niemal dosłownie zdemolował sześć tysięcy komputerów połączonych z Internetem. A zrobił to — jak pisałem wcześniej — poprzez zainfekowanie ich wirusem. Niezły to wszakże wynik, niemniej jednak Robert miał pecha i stał się pierwszą ofiarą Federal Computer Fraud and Abuse Act. Sąd wydał łagodny wyrok — 10 000 dolarów grzywny oraz 400 godzin prac społecznych.

Ale po nim byli następni. Kevin Mitnick alias Condor włamał się m.in. do sieci komputerowej Digital Equipment Company, skąd wykradał numery kart kredytowych. Wyrok — 18 miesięcy. Później był jego imiennik, asystent programisty, Kevin Poulsen oficjalnie włamujący się do systemów Pentagonu w celu ich testowania. Zasłynął blokadą centrali telefonicznych Pacific Bell oraz licznymi włamaniami do systemów FBI i US Army. Skazany na 51 miesięcy i 56 000 dolarów grzywny.

Ale hakerska lista skazańców jest znacznie dłuższa. Pojawiło się bowiem nowe niebezpieczne zjawisko — zorganizowana przestępczość on-line. Oprócz wciąż działającej LOM zaczęły tworzyć się nowe podziemne grupy i organizacje pseudohakerskie. Rząd amerykański podejmuje wciąż nowe próby ich rozbicia wydając wojnę całemu środowisku hakerów. W 1990 roku FBI przeprowadziła słynną operację Sundevil, która nie przyniosła jednak spodziewanych rezultatów. Stoi za tym brak doświadczenia w walce z podziemiem sieciowym. W rozwiązaniu tego problemu zapewne pomóc mają hakerzy zatrudniani jako konsultanci do spraw... hakerów. I nieco później przygotowana operacja Crackdown Redux nie zakończyła się rozczarowaniem. Za kratki trafiło wówczas czterech członków Masters of Deception (w tym sam Phiber Optik). Z roku na rok aresztowań jest coraz więcej, ale i szeregi hakerów powiększają się o wciąż nowe postaci. Czy w tej wojnie będą zwycięzcy? Czy może niedługo już Sieć przypominać będzie ulice Chicago w latach trzydziestych?

Trudno prorokować, ale wszystko wskazuje na to, że w niedługim czasie w naszym kraju może być podobnie.

Polska scena hakerska

Polski underground to wciąż rozrastające się grono użytkowników komputerów, którzy toczą dyskusje na specjalnych kanałach IRC lub łączą się w internetowych grupach dyskusyjnych. Jest to grono niedostępne, hermetyczne. Trudno zdobyć jego zaufanie. Wielu z polskich hakerów, którzy naprawdę coś umieją zamiast pomagać innym, woli zadzierać nos do góry i nie zdradzać tajników swej wiedzy. Należy jednak podkreślić, że w ostatnim czasie polska scena hakerska znacznie się rozrosła. Pojawiły się bowiem silne grupy.

Całe polskie hakerstwo opiera się głównie o jeden kanał IRC— #hakpl. Na nim bowiem wszyscy polscy hakerzy poznają się i większość z nich, choć nie wszyscy, od tego kanału zaczynają swoją edukację.

Początkujący adept sztuki hakerskiej, zwykle szybko stwierdza, że w tym świecie najtrudniej jest zaistnieć. Jeden z polskich hakerów, który napisał tekst o rejestrach Windows 95 do najpopularniejszego hakerskiego zina POWER FAQ i w ten sposób poznał i zyskał uznanie w oczach Powera i Lcamtufa, znalazł się w gronie najprawdziwszej elity. To właśnie im zadawał pierwsze pytania, które były dla nich często śmieszne. Ale był uparty...

Warto podkreślić, że na tym etapie ważna jest duża cierpliwość. Trzeba bowiem zdobyć niezbędną wiedzę na dany temat, by rozpocząć poszukiwań na własną rękę. Często podstawowe umiejętności wystarczą do włamywania się do źle zabezpieczonego serwera. Można również nauczyć się wyszukiwać luki w systemie, odpalić exploita (czyli program dający roota) i nie trzeba wgłębiać się w dalsze szczegóły. Ale tak postępują początkujący hakerzy ewentualnie crackerzy. Prawdziwy haker na pewno zacznie dociekać tego, jak ten exploit działa.

Dla wielu hakerów prawdziwa edukacja zaczyna się z chwilą, gdy założy grupę hakerską. Kolejnym wyzwaniem jest znalezienie odpowiedniego pseudonimu. I można już zacząć się włamywać...

W Polsce działały dwie grupy — DHS oraz Division 666 założona przez Viedzmina. Jak łatwo się domyślić, biorąc pod uwagę przykłady innych krajów — przez dłuższy czas były one w stanie „świętej wojny", która skończyła się wraz z rozsypką grupy Division 666.

DHS funkcjonuje nadal, co przynosi bardzo duże korzyści jej członkom. Bowiem w takiej grupie wszyscy uczą się od wszystkich. Wielu hakerów zgodnie przyznaje, że wiele się uczą czytając ciekawe merytorycznie ziny (czyli elektroniczne magazyny hakerskie). Można w nich znaleźć mnóstwo ciekawych informacji. Ale i tak najwięcej można nauczyć się od innych. Ważne jest także, aby pozyskać zaufanie mądrego mentora, który przyjmie nad początkującym swoistą opiekę. W rezultacie adept sztuki hakerskiej szybko będzie mógł przeobrazić swoje szczeniackie wybryki w poważne włamania.

Hakerzy często pomagają administratorom serwerów, do których się włamują. Ważne jest, aby wybierać interesujące serwery i utrzymać je jak najdłużej, by można było przetestować na nich nowe backdory.

Ta wiedza pomaga później w znalezieniu odpowiedniej pracy. Bo większość hakerów zostaje administratorami różnych systemów.

Do najbardziej znanych polskich hakerów należą: Power, lcamtuf, Ultor, Rastlin, Kil3r, manY, Wojtekka, Luke-Skyw, Spacman. A największe dokonania grupy DHS to:

- Włamanie na stronę Secret Service (magazynu komputerowego, największego czasopisma o grach komputerowych w Polsce);
- Włamanie na stronę Windows.98.to.jest.to.

Natomiast Division 666 prawdopodobnie włamał się na serwer Radia Maryja, gdzie dokonał spustoszenia.

Gumisie a sprawa polska

Ze względu na nieco opóźniony rozwój sieci komputerowych w naszym kraju hakowanie stało się u nas głośne dopiero w połowie lat 90. Najsłynniejszym włamaniem była zamiana nazwy na witrynie Naukowo-Akademickiej Sieci Komputerowej (NASK) na jej niecenzuralny wariant. Dokonali tego żartownisie określający się jako Gumisie. Zamierzali w ten sposób zaprotestować przeciwko planowanym podwyżkom cen dostępu do Internetu (NASK w tym czasie był monopolistą w tej dziedzinie).

Nowe zabezpieczenia serwerów NASK-u nie zniechęciły hakerów, którzy w polskim środowisku nie byli specjalnie szanowani, gdyż posługiwali się gotowymi metodami i kodami dostępnymi w Internecie na zachodnich stronach hakerskich. Niedawno jednak Gumisie powróciły publikując swoje „zdjęcie" (tzn. kadr z filmu animowanego pod tym tytułem).

Natomiast w maju zeszłego roku doszło do włamania do serwera Biura Informacyjnego Rządu. Grupa Damage Inc. zmieniła prezentowaną na stronie WWW nazwę tej organizacji na „Biuro Dezinformacyjne Rządu" i skierowała odwiedzających na stronę WWW Playboya. Niedługo potem w programie „Tok Szok" pokazano, iż serwery rządowe nie są wystarczająco zabezpieczone (anonimowy haker „na żywo" włamał się do jednego z nich).

Argumentacja

Protest przeciwko łamaniu Praw Człowieka

Praca hakerów znajduje różnorodną motywację — od osiągnięcia materialnych korzyści aż po najbardziej wzniosłe przedsięwzięcia. Przykładem mogą być protesty skierowane przeciwko łamaniu Praw Człowieka, które stały się udziałem grupa chińskich hakerów. Ostrzegli oni władze, że zamierzają uszkodzić jednego z satelitów komunikacyjnych, jeżeli rząd nie zaprzestanie represjonowania i łamania Praw Człowieka, a ponieważ samo zapowiedzenie uszkodzenia nie przyniosło rezultatów, pogróżki stały się faktem. Satelita został unieruchomiony. Najprawdopodobniej ta sama grupa hakerów o nazwie Yellow Pages zaatakowała firmy zachodnie współpracujące z komunistycznymi Chinami. Na ich liście znalazły się Sun Microsystem, Lucent, Motorola, VW, Yahoo, Excite, a nawet jedna z polskich firm — Hortex. Działania tej grupy mają na celu zwrócenie opinii publicznej na nieprzestrzeganie Karty Praw Obywatelskich przez Pekin. Ofiarami represji niejednokrotnie byli rodzice hakerów, więc kolejne protesty podyktowane były poczuciem wielkiej niesprawiedliwości.

Protest przeciwko broni atomowej

Wielokrotnie hakerzy pokazywali całemu światu, że nie zależy im na rozgłosie, ale na zwróceniu uwagi społeczeństwa na kwestie dotyczące zagrożeń cywilizacyjnych. A tych nie brakuje. Państwa, takie jak Pakistan i Indie, które w maju 1998 roku przeprowadziły próby z bronią jądrową wywołały integrację środowiska hakerskiego, które solidarnie zaprotestowało przeciwko takiemu stanowi rzeczy. W ramach sprzeciwu kilku młodych hakerów zaatakowało serwer wewnętrzny Bhabha Atomick Research Center pod Bombajem. Skopiowali oni ponad 5 MB informacji i całą korespondencję e-mailową prowadzoną między naukowcami BARC, usunęli dane z dwóch serwerów ośrodka, a na jego stronie WWW umieścili wizerunek atomowego grzyba. Członkami tej grupy są nastoletni hakerzy prawdopodobnie z Nowej Zelandii, Wielkiej Brytanii, którzy należą do organizacji MilwOrm. O powodach ataku i jego przebiegu poinformowały największe e-ziny hakerskie oraz AntiOnline. Wiedzę potrzebną do przeprowadzenia protestu zaczerpnęli od Analyzera

(który zasłynął z udanego ataku na Pentagon) i wykorzystali stary program pocztowy Sendmail. Aby zdobyć dostęp do indyjskich serwerów z prawami administratora systemu potrzebowali aż 52 sekund. Kolejnym protestem tej grupy był atak na turecki serwer znajdujący się w Centrum Nuklearnym Catal Huyuk. Tym razem zhakowali całą korespondencję naukowców. Na początku roku 2000 grupa hakerów zhakowała około 300 stron WWW znanych firm mających swoje udziały w próbach nuklearnych i, tak jak za pierwszym razem, umieścili na stronach głównych tych firm wizerunek nuklearnego grzyba oraz manifest antynuklearny. W taki właśnie sposób chcieli zwrócić uwagę opinii publicznej na wciąż przeprowadzane nowe próby z bronią jądrową i napiętnować odpowiedzialnych. Na liście zaatakowanych firm zalazły się The Word Cup, Wimbledon, The Ritz Casino, a także oficjalna strona rodziny królewskiej.

Media

Także media, szczególnie w ostatnim czasie, stają się źródłem hakerskich ataków. Zdarza się dość często, że dziennikarze nie odróżniają crackera od hakera, co za tym idzie ugruntowują wizerunek złego hakera-przestępcy, który jest odpowiedzialny za całe zło. Dlatego właśnie hakerzy próbują bronić swego honoru i często decydują się na atakowanie stron WWW redakcji, stacji telewizyjnych i radiowych, które w jakiś sposób sobie na to zasłużyły. Niekiedy celem ataków stają się poszczególni dziennikarze i ich konta e-mailowe. Tak było wtedy, gdy prasa w złym świetle przedstawiała jednego z najsławniejszych z hakerów — Kevina Mitnicka. W odwecie grupa HFG (*Haking of Girlies*) zaatakowała główną stronę prestiżowej gazety „The New York Times", a pod adresem *www.nytimes.com* zamieszczone zostało zdjęcie rozebranej kobiety i kilka niecenzuralnych słów skierowanych pod adresem redakcji.

Ponadto hakerzy zamieścili w kodzie tekst o treści: „nasza obecność na stronie NYT jest najlepszym miejscem na zaprezentowanie opinii publicznej naszych haseł oraz na pokazaniem tego, jak źle zabezpieczone są strony internetowe wielkich korporacji i czasopism". Po kilku próbach zdjęcia tego tekstu, które stały się udziałem webmastera, redakcja zdecydowała się na zdjęcie całej strony głównej na kilka weekendowych dni. Była to trudna decyzja, ponieważ weekend to okresem największej oglądalności tej strony. Atak hakerski został zarchiwizowany przez AntiOnline i dostępny jest pod adresem: *www.antionline.com/archives/pages/www.nytmies/com*.

Włamania tego typu nie ominęły też współautora słynnej książki *Tekedown* — John'a Markoffa, który napisał również wiele artykułów na temat świata hakerskiego. Jego konto e-mail i strona WWW książki stały się tak popularnym celem jak serwery Pentagonu. Na stronie WWW też pojawił się napis, w którym hakerzy oskarżyli Markoffa o to, że przyczynił się do zamknięcia Mitnicka w więzieniu. Podobne zdarzenia przeżyła Carolyn Meinel, konsultantka do spraw bezpieczeństwa w Sieci, autorka książki *The Happy Haker*. Po jej publikacji popularność strony WWW poświęconej książce gwałtownie wzrosła. Grupa HFG nie poprzestała na tym, lecz włamała się do serwera internetowego Route 66 w Nowym Meksyku i tam wyrządziła wiele szkód.

Zlecenia

Od paru lat w USA istnieje firma Rent-A-Haker (*http://www.rent-a-haker.com*), której szefem jest John Klein. Firma ta specjalizuje się w wynajmowaniu hakerów. Zapotrzebowanie na ich usługi wyraża szereg instytucji rządowych, takich jak Biały Dom czy Pentagon oraz wielkie korporacje i firmy, którym szczególnie zależy na bezpieczeństwie swoich sieci. Bardzo często firmy i instytucje, pomimo iż mogą wybierać specjalistów z najznamienitszych uczelni w kraju, zatrudniają nastolatków lub byłych hakerów, których wiedza oparta jest na praktyce. Zespół złożony z byłych lub czynnych hakerów (podobno jego członkiem jest jeden z najsłynniejszych hakerów — agent Steal) pracuje dla FBI i skutecznie walczy z przestępczością on-line. Również Pentagon, Departament Sprawiedliwości i szereg innych instytucji korzysta z usług „wyjętych spod prawa". Ale nie tylko w USA usługi hakerów cieszą się taką dużą popularnością. Pracują oni na zlecenie także w Polsce (np. w Komendzie Głównej Policji). Podobno istnieje tam specjalna komórka do spraw przestępstw komputerowych w Polsce. Taki zespół specjalistów zatrudnia też znana firma IBM, która ponadto współpracuje z grupami, takimi jak Apache Group z Monachium.

Ideologiczne aspekty

Dla prawdziwego hakera złamanie systemu zabezpieczeń jest celem samym w sobie i stanowi pewien rodzaj wyzwania. Wystarcza mu świadomość, że jest lepszy od twórcy złamanego programu, systemu czy zabezpieczenia. A firmy produkujące owe systemy często reklamują je jako niezawodne i sprzedają po niebotycznych cenach. Jeżeli jednak nastoletni haker z powodzeniem próbuje łamać te zabezpieczenia, świadczy to tylko o jednym — że zawierają one błędy. Hakerzy pokazują, że takie błędy powinno się korygować, poprawiać, a co za tym idzie — ulepszać programy zabezpieczające. W takim rozumowaniu hakerzy nie mogą być postrzegani jako przestępcy, ale raczej jako siła napędowa do tworzenia i rozwoju wielu gałęzi inteligencji technicznej. Często wiedza hakerów wykorzystywana jest jako narzędzie nacisku w walce przeciwko korupcji, zatruwaniu środowiska, rozpowszechnianiu pornografii itd. Choć ta ostatnia z wymienionych znana jest tylko policji, ponieważ skutków działalności w tym zakresie nie nagłaśnia się, ale wiadomo, że istnieją hakerzy tropiący i niszczący wszelkie przejawy pornografii dziecięcej (np. grupa o nazwie Ethical Hakers Against Pedophilia, która uderzyła w znane i wysoko postawione osoby zajmujące się pedofilią). Biorąc pod uwagę takie aspekty działalności hakerów, mają oni chyba prawo protestować przeciw złemu wizerunkowi, jaki jeszcze dość często jest im przypisywany.

Przestępczość komputerowa

Przedstawione poniżej informacje zostały oparte na bardzo ciekawej pracy K.J. Jakubowskiego zawartej w „Materiale Konferencyjnym. Przestępczość w sieciach komputerowych".

Według Jakubowskiego *przestępczością komputerową* jest „zjawisko kryminologiczne, obejmujące wszelkie zachowania przestępcze związane z funkcjonowaniem systemu elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawa do programu komputerowego".

Zdaniem autora tej definicji bardzo ważne jest, aby zdać sobie sprawę z faktu, że włamanie do serwera nie jest tylko winą właściciela (lub innej osoby odpowiedzialnej — np. administratora systemu lub sieci komputerowej) i pozostaje w zgodzie z zasadą: „jeżeli do komputera można się dostać, niezależnie od stosowanych technik i sposobów, to wszystko, co na tym komputerze się znajduje jest nasze". Włamanie do serwera jest takim samym przestępstwem jak opróżnianie mieszkania przez złodzieja, który wykorzystał do tego celu otwarte okno balkonowe na którymś piętrze bloku mieszkalnego. Tak samo jak zgłasza się fakt włamania do mieszkania na policję, tak samo powinno się zgłaszać włamania do systemów komputerowych. Jakubowski zwraca jeszcze uwagę na fakt, że choć w Polsce istnieją formalne problemy związane ze ściganiem przestępczości komputerowej, można jednak skorzystać z pomocy specjalizowanych agencji, takich jak CERT NASK, czy IBS (Instytut Bezpieczeństwa Sieciowego). Gwarantują one pełną dyskrecję i prawo do tajemnicy. Aby dobrze zabezpieczyć system komputerowy, należy wziąć pod uwagę wiele czynników, takich jak: topologia sieci, użytkowane systemy operacyjne i sposoby autoryzacji użytkowników.

Gdy rozpoczynano pierwsze prace nad siecią powszechnego przekazu informacji, niewielu zaangażowanych w to ludzi przypuszczało, że stanie się ona „areną" dla przestępców. Różnią się oni nieco od typowego wizerunku złoczyńcy. Nie mają broni wprawdzie z pełnym magazynkiem, ale posiadają broń równie skuteczną w XXI wieku — komputer o potężnej mocy obliczeniowej, potrafiący korzystać z najwyższych priorytetów Sieci.

Przez wiele lat przez media rozpowszechniany wizerunek hakera-przestępcy, który włamuje się do serwerów sieciowych i niszczy ich zawartość, jest od początku do końca błędnym rozumieniem problemu. Potwierdza to także Jakubowski. Jego zdaniem hakerzy nigdy nie niszczą danych, gdyż tym zajmują się głównie pseudohakerzy. Do poprawnego rozróżnienia i zrozumienia różnic pomiędzy tymi dwoma grupami ludzi często stosuje się test zwany *mens rea*. Reguła ta w zestawieniu z relacją prawdziwy haker — pseudohaker, przedstawia się w następujący sposób. „Winny umysł" nie zaistnieje wówczas, gdy osoba spenetruje system komputerowy przy użyciu metod ogólnie stosowanych przez zwykłych obywateli. Jeżeli jednak zostanie naruszony system bezpieczeństwa za pomocą wyszukanych sposobów i narzędzi, to będzie można mówić o *mens rea* i o popełnionym wykroczeniu. Natomiast hakerom i pseudohakerom przyświeca całkiem inna motywacja. Ci pierwsi to programiści, realizujący założenie dążenia do doskonałości, a napisane przez nich programy analizują dany problem i wyszukują metodę jego wykorzystania w praktyce. W ten sposób powstają genialne aplikacje umożliwiające wyszukanie luk w systemie bezpieczeństwa sieciowego. Pseudohakerzy natomiast bazują na tym, co wcześniej wykonają inni. Używają cudzych programów. Są ograniczeni brakiem wyobraźni oraz umiejętności tworzenia.

Posiadają wypracowaną technikę, ale nie wnoszą nic nowego do świata cyberprzestrzeni. Mimo tego wszystkiego są bardzo silni w grupie. Wspólnie z hakerami i crackerami tworzą najsilniejszą społeczność sieciową.

Dla uzupełnienia warto zapoznać się z definicjami przestępczości komputerowej w zakresie różnych technologii, którymi posługuje się Interpol:

Naruszanie praw dostępu do zasobów, a w szczególności:

- hacking, czyli nieupoważnione wejście do systemu informatycznego (określane jako naruszenie tajemnicy korespondencyjnej zgodnie z art. 267§1 Kodeksu Karnego);
- przechwytywanie danych;
- kradzież czasu, czyli korzystanie z systemu poza uprawnionymi godzinami, niszczenie i naruszenie informacji;
- Modyfikację zasobów przy pomocy bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego;
- Oszustwa przy użyciu komputera, a w szczególności:
  - oszustwa bankomatowe;
  - fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesorowych);
  - oszustwa na maszynach do gier;
  - oszustwa dokonywane poprzez podanie fałszywych danych identyfikacyjnych;
  - oszustwa w systemach sprzedaży (np. w kasach fiskalnych);
  - oszustwa w systemach telekomunikacyjnych;
- Powielanie programów, w tym:
  - gier we wszelkich postaciach;
  - wszelkich innych programów komputerowych;
  - topografii układów scalonych;
  - Sabotaż dokonywany na sprzęciu i oprogramowaniu;
  - Przestępstwa dokonywane za pomocą BBS-ów;
  - Przechowywanie zabronionych prawem zbiorów;
  - Przestępstwa w Internecie.