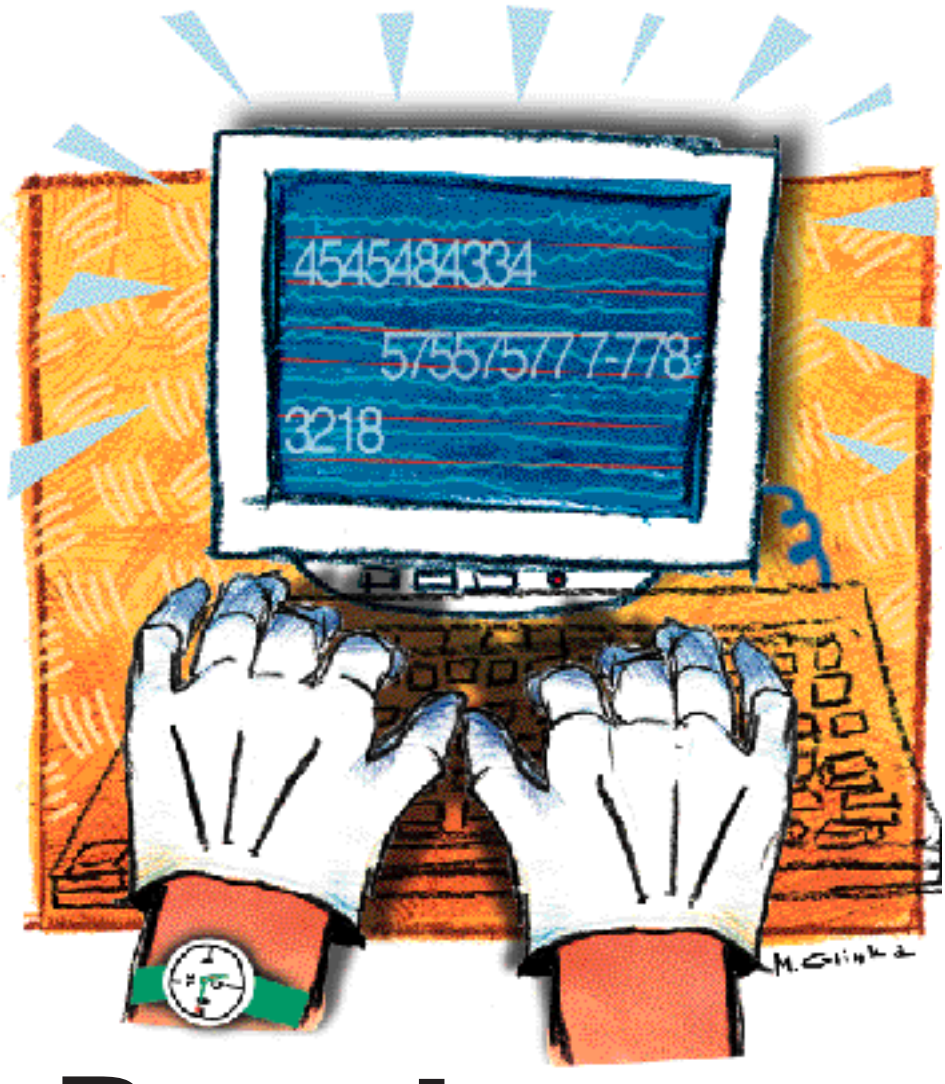

Przestępcy i filantropi

Grasują w Sieci, wnikając tylko sobie znanymi metodami do baz danych agencji rządowych, banków i osób prywatnych. Nie kieruje nimi chęć zysku: czują głód informacji i pragną doskonalić swoje umiejętności.

Tuż po północy 15 lutego 1995. Wśród ludzi obserwujących jeden z budynków na peryferiach Raleigh w stanie Północna Karolina (USA) narasta podniecenie. Pułapkę zastawili: grupa policjantów (w tym pięciu funkcjonariuszy Oddziału Specjalnego do Walki z Groźnymi Przestępstwami i zastępca szeryfa federalnego), agenci FBI, eksperci od telefonii komórkowej, dziennikarz „Timesa" i młody fizyk. Wszyscy znaleźli się w tym miejscu dzięki temu ostatniemu – Japończykowi, pracownikowi Centrum Superkomputerowego w San Diego.

W drzwiach mieszkania przy Tournament Road 4660 pojawia się sylwetka mężczyzny. Wszyscy czekają właśnie na niego. Po chwili do lokalu wpadają agenci FBI i dwaj członkowie Oddziału Specjalnego. Po sprawdzeniu tożsamości na rękach pucołowatego okularnika pojawiają się kajdanki.

Samuraj kontra Kondor

Tak skończyła się kariera Kevina Mitnicka (znanego również jako Kondor), jednego z najbardziej poszukiwanych włamywaczy komputerowych (hackera, a może crackera) na świecie. Człowiekiem, który najbardziej przysłużył się do jego aresztowania był Tsutomu Shimomura, specjalista od zabezpieczeń komputerowych i ...hacker. Hacker stojący po „właściwej" stronie prawa.
Pewne jest, że Japończyk był osobiście zainteresowany złapaniem Mitnicka. Nie mógł przeboleć własnej porażki: Kevin włamał się do jego komputera i ukradł informacje na temat zabezpieczeń oraz programy do tego służące.

Hacker czy cracker?

W latach 70. i 80. słowo „hacker" określało entuzjastów komputerowych zafascynowanych nowymi technologiami. To właśnie oni tworzyli w słynnej Dolinie Krzemowej pierwsze pecety i oprogramowanie do nich. Później pojawiły się sieci rozległe i kolejne wyzwania.

Ciekawość świata, komputer i sieci jako nowe media ułatwiające kontakty między ludźmi wykreowały nowy rodzaj buntownika. Kogoś, kto chciałby poznać zawartość dysków cudzych maszyn, a jednocześnie chronić swój przed ingerencją innych. Te cudze to z reguły komputery rządowe lub korporacyjne.

Hackerzy starają się wyraźnie odróżnić od crackerów. Uważają się za lepszych, wyraźnie dystansując od reszty. Ich działalność nie ma w sobie owej destrukcyjnej siły, która nieodłącznie towarzyszy crackerom, włamującym się do systemów komputerowych i niszczącym zawarte tam dane.

Przed laty wymieniano informacje korzystając z BBS-ów. Bardzo szybko zaczęły wokół nich powstawać nieformalne grupy – protoplaści dzisiejszych hackerów. Wydawali nawet swoje biuletyny: początkowo na własne potrzeby, później rozpowszechniane szerzej. Najbardziej znane elektroniczne magazyny wywodzące się z tamtych czasów to „2600" i „Phrack". Ukazują się one do dziś i są źródłem cennych informacji, również dla administratorów sieci i osób odpowiedzialnych za bezpieczeństwo systemów. Np. „Phrack" nr 50 z kwietnia 1997 zawiera informacje o sposobie złamania hasła w Windows NT 4.0.

Rozwój sieci komputerowych, a szczególnie Internetu, ułatwił życie członkom sieciowej awangardy. Wymiana informacji jest teraz prostsza i szybsza. Większa jest też liczba obiektów znajdujących się na celowniku hackerów.

Inżynieria społeczna

W jaki sposób hackerzy dostają się do komputerów? Poza umiejętnościami technicznymi, związanymi z informatyką, elektroniką czy też telekomunikacją, przydają się podstawy psychologii. Niektórzy z nich nazywają to inżynierią społeczną.

▶ 57

Zasady etyki hackerów

- Hacker nie posługuje się wirusami. Jedynym powodem eksperymentowania z nimi jest chęć poznania sposobu ich działania.
Hacker nie włamuje się dla osiągnięcia korzyści innych niż poszerzenie swej wiedzy.
- Hacker nie modyfikuje danych w systemach, które penetruje. Dopuszczalne są następujące wyjątki:
– zmiana zapisów systemowych, aby wejście do systemu pozostało niezauważone,
– korekty w plikach użytkownika w celu zapewnienia sobie dostępu w przyszłości,
– naprawy uszkodzonych plików.
- Hacker dzieli się swoją wiedzą. Pragnie, by ludzie poznawali luki w systemach zabezpieczeń i mogli je naprawiać (a nie wykorzystać!).
* Hacker pomaga tym, którzy pomagają sobie. Jeśli ktoś porządnie napracował się ucząc się czegoś, a mimo to nie radzi sobie, hacker wyciągnie do niego pomocną dłoń.
Chociaż hacker może łamać ustawowe prawo, nie złamie zasad etyki. Wejdzie nielegalnie do systemu komputerowego, ale będzie działał tylko na jego korzyść.
- Hacker płaci za oprogramowanie komercyjne i nie korzysta z pirackich kopii.
- Hacker wierzy, że informacja powinna być powszechnie dostępna, jednak respektuje prawo do poufności informacji prywatnych.

Kevin Mitnick zdobywał hasła wędrując po biurach i podając się za serwisanta. Po prostu prosił o hasła, które były mu rzekomo potrzebne do „wykonania pracy". Zdarzało mu się grzebać w śmietnikach firm telekomunikacyjnych i analizować znalezione tam wydruki (to jest dopiero źródło informacji!). Jednym z jego popisowych „numerów" było zatelefonowanie do administratora sieci dużej firmy, podanie się za jej prezesa i zażądanie hasła do systemu. Wydaje się to niewiarygodne, lecz takie właśnie metody były często niezwykle skuteczne.

Cyberpunk w cyberprzestrzeni

Hackerzy pojawiający się w Sieci (nazywają ją cyberprzestrzenią lub cybernetycznym pograniczem) występują zwykle pod fantazyjnymi pseudonimami, np. Knight Lightning, Cap'n Crunch. Są oni członkami grup o równie malowniczych nazwach: np. Legion Zagłady (nieistniejący już), Cyberpunk, The NATO Association.

Wydawałoby się to naturalne: obywatele łamiący prawo starają się nie ujawniać swojej tożsamości. Tak jednak nie jest: hackerzy w zasadzie nie ukrywają się. Co więcej, można ich spotkać na systematycznie organizowanych, oficjalnych spotkaniach. Uczestniczą w nich ludzie znajdujący się na co dzień po obu stronach barykady, czyli hackerzy, specjaliści od zabezpieczeń komputerowych, funkcjonariusze odpowiednich służb. W sierpniu podobny zlot odbędzie się niedaleko Almere w Holandii.

Buntownicy czy przestępcy

Od lat hackerzy i crackerzy traktowani są jak przestępcy oraz ścigani przez prawo w wielu krajach. Opisany na wstępie przypadek jest chyba najgłośniejszy w ostatnich latach. Kevin Mitnick był kilkakrotnie skazywany na karę więzienia. W uzasadnieniu jednego z wyroków uznano, że „uzbrojony w klawiaturę jest niebezpieczny dla społeczeństwa".

Magazyn „2600", oceniając wzrastającą liczbę akcji przeciwko hackerom w USA, napisał: „Z tego co odkryli hackerzy można się wiele nauczyć.(...) Włamania ujawniają luki w systemach i ich zabezpieczeniach. Działania hackerów dowodzą, że myśl człowieka jest wciąż najpotężniejszym narzędziem."

John Draper: jeden z pierwszych hackerów, któremu wytoczono proces publicznie ujawniający jego umiejętności

Do więzienia za gwizdanie

Prekursorami hackerów są phreakerzy. Ich działalność rozpoczęła się w latach 50., gdy wprowadzono w USA bezpośrednie międzynarodowe połączenia telefoniczne. Szybko okazało się, że stosując różne sztuczki można bezpłatnie dzwonić niemal po całym świecie. Ta umiejętność bardzo się później przydała hackerom i crackerom. Dostęp do sieci odbywa się bowiem głównie za pośrednictwem łączy telefonicznych.

Legendarną postacią komputerowego podziemia jest Captain Crunch. Naprawdę nazywa się John Draper, zaś jego przydomek pochodzi od nazwy gwizdka ukrytego w torebce chrupek „Cap'n Crunch". Draper odkrył, że wydaje on dźwięki o częstotliwości 2600 Hz, umożliwiające bezpłatne połączenie się z dowolnym abonentem. Następnie Draper pomógł Steve Wozniakowi i Steve Jobsowi (późniejszym twórcom komputera Apple) skontruować urządzenie zwane „niebieską skrzynką" (blue box). Służyło one do generowania dźwięków, oszukujących centrale telefoniczne i umożliwiających darmowe połączenia.

John Draper był jednym z pierwszych hackerów, skazanych za swą działalność na karę więzienia. Oficjalnym zarzutem, jaki mu postawiono było nadużywanie systemu telekomunikacyjnego (kilka darmowych połączeń przy pomocy „niebieskiej skrzynki"). W czasie pobytu w więzieniu Cap'n Crunch nie tracił czasu. Opracował edytor tekstu „Easy Writer" (dla komputera Apple), który, jak sam twierdzi, przyniósł mu całkiem niezłe pieniądze.

„Znalazłem się w idealnej sytuacji: mogłem się skupić i całkowicie poświęcić temu zadaniu" – zwierzył się nam podczas rozmowy w cyberprzestrzeni. Dziś, po niemal ćwierćwieczu od momentu uwięzienia, może już żartować na ten temat. Proces sądowy publicznie ujawniający jego umiejętności – uczynił go... sławnym.

W Europie... chaos

Zdecydowana większość nieformalnych grup hackerskich pochodzi z USA. Europejczycy starają się im dorównać: w 1981 roku powstał w Hamburgu Klub Chaosu Komputerowego (Chaos Computer Club), jedno z najsłynniejszych ugrupowań hackerów. Do ich „dokonań" zalicza się m.in. wykrycie luk w systemie operacyjnym VMS, a następnie włamanie do 135 sieci na całym świecie, w tym do NASA. Na początku bieżącego roku Klub po raz kolejny trafił na pierwsze strony gazet. Stało się to za sprawą Microsoftu, Internet Explorera i ActiveX. Członkowie CCC udowodnili bowiem, że korzystając z ActiveX można uzyskać nieautoryzowany dostęp do komputerów podłączonych do Internetu.

Kevin Mitnick alias Kondor: najsławniejszy hacker wszechczasów

W Polsce działalność hackerów nie jest specjalnie głośna. Poza przypadkiem gdy półtora roku temu włamano się do serwera NASK i zmieniono stronę główną. Młodzi-gniewni zafascynowani takimi filmami, jak: „Gry wojenne", „Snickers", „Hackerzy" też chcieliby spróbować swych sił. Administratorzy serwerów internetowych obserwują coraz więcej takich prób. Ostatnią odnotowano w maju br. Nieznany żartowniś zmienił stronę główną Centrum Informacyjnego Rządu i zamieścił na niej link do „Playboya". Znamy to z autopsji: mamy przecież własny serwer WWW.

Janusz Żmudziński