Arkana szpiegostwa komputerowego

Autor: Joel McNamara
Tłumaczenie: Bartłomiej Garbacz
ISBN: 83-7361-341-2
Tytuł oryginału: Secrets of Computer Espionage
Format: B5, stron: 392

Wartość informacji we współczesnym świecie rośnie. Dane przechowywane na twardych dyskach i przesyłane w sieciach komputerowych są łakomym kąskiem. Istnieją osoby posiadające odpowiednie zaplecze techniczne i wiedzę, które dołożą wszelkich starań, aby informacje takie przechwycić. Liczba udanych ataków przeprowadzanych przez hakerów rośnie i choć trudna jest do oszacowania, z pewnością sygnalizuje poważny problem. A przecież prawie każdy z nas ma w swoich komputerowych zasobach informacje, którymi nie chce dzielić się z innymi.

Książka jest adresowana do osób, dla których poufność danych jest rzeczą istotną. Chodzi zatem zarówno o indywidualnych użytkowników, jak i administratorów systemowych odpowiedzialnych za bezpieczeństwo przedsiębiorstw. Dzięki niej poznasz zarazem metody używane przez komputerowych szpiegów i sprawdzone metody zabezpieczania się przed ich działaniami.

Poznasz:

- Szpiegów komputerowych i ich motywy
- Ocenę stopnia zagrożenia Twoich danych
- Szpiegowanie a prawo
- Włamania fizyczne i wykorzystywanie socjotechniki
- Włamania do systemów Windows
- Gromadzenie dowodów włamań
- Metody szyfrowania informacji
- Sposoby łamania haseł i zabezpieczeń
- Inwigilację za pomocą monitorowania użycia klawiatury
- Szpiegowanie przy użyciu koni trojańskich
- Podsłuchiwanie w sieciach przewodowych i bezprzewodowych
- Podsłuchiwanie urządzeń elektronicznych
- Zaawansowane systemy szpiegostwa komputerowego: Echelon, Carnivore i inne

Joel McNamara jest konsultantem ds. bezpieczeństwa i ochrony prywatności o międzynarodowej renomie oraz twórcą Private Idaho, jednego z pierwszych narzędzi ochrony prywatności w internecie.

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

Spis treści

Rozdział 7.

Kopiowanie danych

„Zapisz to w notesie, moja upragniona, Harriet — szpiegu”.

— Indigo Girls, „Caramia”, *Shaming of the Sun*

Kiedy szpieg uzyska fizyczny dostęp do komputera, prawdopodobnie zechce skopiować znajdujące się w nim najważniejsze dane. Może się wydawać, że podobne działania są dość oczywiste i nie warto poświęcać im całego rozdziału, jednak w rzeczywistości należy wziąć pod uwagę wiele kwestii i możliwości związanych z kopiowaniem danych i szpiegostwem komputerowym.

Nośniki danych, takie jak dyskietki, płyty CD-R lub dyski ZIP, mają swoje zalety i wady, jeśli chodzi o ich wykorzystywanie przez szpiega. Ponadto warto poznać różnorodne urządzenia zewnętrzne podłączane do komputera, które są specjalnie zaprojektowane do kopiowania danych. Wiele z tych produktów charakteryzuje niska cena i dyskretny wygląd, tak że z powodzeniem mógłby je stosować James Bond.

W przeciwieństwie do większości rozdziałów niniejszej książki w tym brak jest podrozdziału „Środki zaradcze”. Wynika to z faktu, że jeśli odpowiednio zastosuje się środki omawiane w innych rozdziałach, takie jak zabezpieczenia fizyczne, szyfrowanie oraz silne hasła, nie pozwoli to szpiegowi ani na uzyskanie dostępu do komputera, ani na zapoznanie się z zawartymi w nim danymi.

Przejdźmy zatem do omówienia kwestii kopiowania danych widzianej z perspektywy szpiega.

Taktyka szpiegowska

Zanim zostaną omówione różne nośniki danych i nowoczesne gadżety, warto zwrócić uwagę na cztery wskazówki natury ogólnej związane z kopiowaniem danych, o których zawsze należy pamiętać, zanim podejdzie się do komputera ofiary.

- **Należy korzystać z dostępnych zasobów.** Używaj istniejących urządzeń do kopiowania danych.
- **Należy używać narzędzi kompresujących.** Zawsze miej pod ręką narzędzie kompresujące dane na wypadek, gdyby nie mieściły się one na nośniku danych.

- **Bierz pod uwagę inne dane.** Nie koncentruj się wyłącznie na dysku twardym jako jedynym źródle danych.
- **Poznaj dogłębnie proces kopiowania danych.** Przećwicz wcześniej metody ich kopiowania.

Wykorzystywanie dostępnych zasobów

Chiński strateg Sun Tzu zawsze radził wykorzystywanie zasobów wroga dla swoich korzyści i jeśli chodzi o kopiowanie danych, należy myśleć w podobny sposób. Komputer ofiary z pewnością będzie miał przynajmniej stację dyskietek. Jeżeli będziemy mieć szczęście, będzie miał nagrywarkę płyt CD lub napęd ZIP. W komputerze może być również zainstalowane oprogramowanie kopiujące.

Jeżeli nie jest konieczne wykonanie wiernej kopii dysku twardego, do skopiowania plików należy użyć dostępnych zasobów. Zawsze należy mieć przy sobie pudełko czystych dyskietek, płyty CD-R, CD-RW i być może dysk ZIP oraz Jaz, na wypadek, gdyby okazało się, że na miejscu nie ma możliwości „pożyczenia" nośnika.

Używanie narzędzi kompresujących

Oprócz czystych nośników danych należy mieć przy sobie podręczną szpiegowską dyskietkę narzędziową lub płytę CD-ROM, na której znajdzie się któreś z narzędzi kompresujących (takich jak Gzip, WinZip lub WinRAR) na wypadek, gdyby dane znajdujące się na dysku twardym były zbyt obszerne w stosunku do posiadanych czystych nośników. Należy jedynie pamiętać, że kompresowanie zwiększa ilość czasu potrzebnego do przeprowadzenia procesu kopiowania, a niekiedy każda sekunda może mieć znaczenie

Narzędzia kompresujące nie są identyczne pod względem szybkości działania oraz skuteczności zmniejszania objętości danych. Porównanie różnych narzędzi można znaleźć na stronie Martina Tsacheva pod adresem *martin.f2o.org/windows/archivers*.

Branie pod uwagę innych danych

Należy pamiętać, że dysk twardy nie jest jedynym miejscem, gdzie mogą znajdować się dane. Dyskietki, płyty CD lub taśmy leżące na biurku, w szufladzie lub w szafce mogą zawierać użyteczne informacje i powinno się je albo skopiować na miejscu, albo ukraść, jeżeli można przypuszczać, że ujdzie to uwadze ofiary. Jeżeli na podstawie etykiet wiadomo, że nośniki zawierają zarchiwizowaną kopię danych z dysku twardego, należy zbadać komputer i sprawdzić, jakiego oprogramowania archiwizującego użyto, tak aby później było wiadomo, jakiej aplikacji należy użyć w celu odtworzenia tych danych.

Dogłębne poznanie procesu kopiowania danych

Im dłużej trwa kopiowanie danych, tym większe jest prawdopodobieństwo zostania zdemaskowanym. To, że na filmie szpieg potrafi skopiować kilkaset gigabajtów danych na dyskietkę w kilka sekund, nie oznacza, że uda się to zwykłemu śmiertelnikowi. Trzeba dobrze poznać możliwości i ograniczenia związane z różnymi technikami kopiowania danych oraz różnymi nośnikami.

Ryzyko — słaba technika i wysokie ryzyko

14 grudnia 2002 roku dokonano włamania do biura firmy TriWest Healthcare Alliance Corp. w Phoenix w stanie Arizona. Nie było to typowe włamanie o podłożu rabunkowym. Złodziej najpierw uzyskał dostęp do biura kierownictwa działu obsługi majątku spółki, ukradł główną kartę otwierającą drzwi, a następnie dostał się do głównej siedziby TriWest. Nie zainstalowano tam żadnych kamer śledzących, które mogłyby zarejestrować włamanie, jednak dzienniki drzwi elektronicznych pozwoliły stwierdzić, że złodziej (lub złodzieje) dwukrotnie wchodził i wychodził z biura TriWest znajdującego się w kompleksie przemysłowym Northwest Phoenix.

Ktokolwiek dokonał włamania, wiedział co robi. Skradziono bowiem dyski twarde z serwerów używanych do przechowywania list ubezpieczeniowych oraz informacji o roszczeniach z tytułu ubezpieczeń. Znajdowały się tam dane osobowe ponad 550 000 beneficjentów sieci opieki TRICARE amerykańskiej armii z 16 stanów. Nikt nie określił, czy skradzione dane były zaszyfrowane czy nie.

FBI oraz Obronne Służby Śledcze ds. Kryminalnych próbują schwytać sprawców, firma TriWest zaoferowała nagrodę pieniężną w wysokości 100 000 dolarów za udzielenie informacji, które doprowadzą do ich ujęcia oraz przesłała listy do beneficjentów z ostrzeżeniem o możliwości kradzieży tożsamości. Z kolei Departament Obrony podjął działania zmierzające do sprawdzenia własnych procedur bezpieczeństwa w zakresie przechowywania danych przez cywilnych kontrahentów. Na razie nie ma żadnych podejrzanych, motywy są nieznane i nikt nie chce zbyt wiele mówić o wynikach śledztwa (implikacje związane z bezpieczeństwem obywateli oraz bezpieczeństwem narodowym są bowiem znaczące).

Nawet jeżeli okaże się, że kradzież nie była aktem szpiegostwa, pokazuje ona, jak bardzo nowoczesne formy danych są narażone na tradycyjne ataki fizyczne. Bardziej przemyślany atak mógłby wiązać się z zastąpieniem skradzionych dysków uszkodzonymi lub sformatowanymi dyskami tego samego typu. Administrator systemu mógłby przypisać to jakimś poważnym problemom z zasilaniem, które spowodowały uszkodzenia kilku dysków i po prostu zastąpić je nowymi oraz odtworzyć dane z kopii zapasowych. Przeprowadzone poprawnie włamanie takie mogłoby ujść uwadze zainteresowanych i nikt nawet nie podejrzewałby, że skradziono jakieś dane.

Jeśli chodzi o kopiowanie danych, istotną rzeczą jest wzięcie pod uwagę wskaźnika szybkości ich przesyłania (ang. *transfer rate*). Jest to teoretyczna maksymalna ilość danych, które można przesłać na nośnik w czasie jednej sekundy. Skrót MB/s oznacza megabajty na sekundę, Mb/s — megabity na sekundę, zaś kb/s — kilobity na sekundę (owe trzy skróty będą używany w dalszej części rozdziału do opisu różnych nośników danych). Niekiedy dysponuje się ograniczoną ilością czasu, jaki można spędzić przy komputerze, i używany nośnik danych decyduje o czasie skopiowania określonej porcji danych. Oczywiście na czas potrzebny do skopiowania danych mają wpływ również inne czynniki, na przykład prędkość szyny systemowej lub typ nośnika, na jakim znajdują się kopiowane dane, ale nad tymi kwestiami nie ma się zwykle żadnej kontroli.

Należy wcześniej przećwiczyć proces kopiowania danych za pomocą różnych narzędzi i nośników danych w celu poznania związanych z nimi wymagań czasowych oraz wysiłku potrzebnego do wykonania kopii.

Nośniki danych

Pamiętając o przedstawionych powyżej uwagach, poniżej omówimy najczęściej stosowane rodzaje przenośnych nośników danych, dzięki którym można kopiować dane (omówienie dużych, wyspecjalizowanych lub mało znanych nośników danych wykracza poza ramy niniejszego opracowania).

Dyskietki

Szpiedzy mogą bez problemów zapisać tajne dane na 3,5-calową dyskietkę schowaną w kieszeni koszuli i ukradkiem wydostać się z budynku. Nie zawsze jednak tak było.

W 1971 roku firma IBM wprowadził do sprzedaży „dysk pamięciowy" — był to pierwszy dysk elastyczny (nazwany tak z uwagi na fakt, że był właśnie elastyczny, a nie sztywny) o rozmiarze 8 cali, umożliwiający odczyt i przechowywanie tylko do 100 kB danych. Produkt stanowił rewolucyjne rozwiązanie, gdyż był mały i przenośny — nie trzeba było przewozić pliku kart dziurkowanych ani taśm magnetycznych w celu przenoszenia danych między komputerami. Kilka lat później firma IBM wprowadziła wersję dysku umożliwiającą odczyt i zapis do 250 kB danych. Podstawowe mechanizmy używane w tych pierwszych dyskach są wciąż obecne w produktach współczesnych.

Od tamtego czasu dyskietki stały się z jednej strony mniejsze, a z drugiej pojemniejsze. Dysk 5,25-calowy pojawił się w 1976 roku i mógł przechowywać do 100 kB danych. Jednak wkrótce naukowcy odkryli możliwość zapisu danych na obu stronach dysku oraz sposób zwiększenia gęstości zapisu i pojemność wzrosła do 1,2 MB.

W 1981 roku firma Sony wprowadziła dysk 3,5-calowy, który jako standard przemysłowy zastąpił dyski 5,25-calowe. Obecnie niewielka, obudowana, dwustronna dyskietka o podwójnej gęstości zapisu umożliwia przechowywanie do 1,44 MB danych, charakteryzuje się szybkością przesyłania danych na poziomie 500 kb/s i kosztuje około 20 centów.

Większość osób uważa, że dyskietki odchodzą w zapomnienie ze względu na swoje ograniczenia pojemnościowe. Jest to prawdą, jeśli chodzi kopiowanie dużych ilości danych lub dużych plików, jednak dyskietki wciąż są bardzo przydatne do kopiowania mniejszych porcji danych i w przypadku innych działań szpiegowskich. Skazani szpiedzy Robert Hanssen, Aldrich Ames oraz Ana Belon Montes używali dyskietek w trakcie swoich działań szpiegowskich na szkodę Stanów Zjednoczonych w celu otrzymywania instrukcji od swoich zwierzchników oraz w celu przekazywania skradzionych informacji.

Płyty CD-R i CD-RW

Dla wielu użytkowników komputerów dysk CD (ang. *compact disc*) zastąpił wszechobecne dyskietki jako podstawowy nośnik wymiany danych. Napędy CD umożliwiające zapis (potocznie zwane *wypalarkami*) szybko stały się standardowym elementem wyposażenia nowych komputerów, na co z pewnością miała wpływ popularność pobierania muzyki w sieciach typu P2P (ang. *peer-to-peer*). Poniżej wymieniono niektóre cechy tych nośników danych.

- Standardowa płyta CD umożliwia przechowywanie od 650 MB do 870 MB danych. Dyski CD-R umożliwiają tylko jednokrotny zapis danych, zaś na dyskach CD-RW dane można zapisywać i kasować wielokrotnie.
- Płyty CD-R i CD-RW są tanie i w zależności od liczby kupowanych sztuk pojedyncza płyta może kosztować mniej niż 50 centów.

Dochodzenie — przebiegłe dyskietki

Na podstawie dokumentów FBI można stwierdzić, że skazany szpieg Robert Hanssen często używał dyskietek w celu przekazywania i odbierania informacji od rosyjskich zwierzchników. W nakazie jego aresztowania xznajduje się interesujący fragment związany z dyskietkami.

„4 kwietnia 1988 roku KGB otrzymało kopertę od 'B' pod uzgodnionym adresem w Okręgu Wschodnim w stanie Wirginia. Na kopercie znajdował się adres zwrotny 'Jima Bakera' z 'Alexandrii' i została ona wysłana z Północnej Wirginii 31 marca 1988 roku. Na kopercie znajdowała się również uwaga od 'B' o treści: 'użyj trybu 40 ścieżek. Ten list nie jest sygnałem'.

Wyrażenie 'użyj trybu 40 ścieżek' odnosi się do technicznego procesu przeformatowania dyskietki w celu ukrycia danych poprzez wstawienie ich na jej odpowiednich ścieżkach. Jeżeli nie użyje się odpowiednich kodów do odszyfrowania takiej dyskietki, wydaje się ona pusta".

Opis wyrażenia „użyj trybu 40 ścieżek", jaki zawiera cytowane oświadczenie, jest dość niejasny i prawdopodobnie mylący ze względu na użycie słowa „odszyfrowanie". Wiele szczegółów dotyczących działalności szpiegowskiej Hanssena nie zostało opublikowanych, ale uwaga dotycząca trybu 40 ścieżek sugeruje kilka prawdopodobnych rozwiązań.

- Domyślnie 5,25-calowe, jednostronne dyskietki o pojemności 320 kB były formatowane w trybie 40 ścieżek. Istnieje możliwość sformatowania 5,25-calowej, dwustronnej dyskietki o pojemności 760 K lub 1,2 MB, która normalnie zawiera 80 ścieżek, jako 40-ścieżkową. Takie działanie może pozwolić na ukrycie danych znajdujących się na drugiej stronie dyskietki.
- Wirus sektora rozruchowego o nazwie Joshi w celu ukrycia swojego kodu tworzył 41. ścieżkę, która byłaby ścieżką 40. na 5,25-calowej dyskietce o pojemności 320 kB. Hanssen mógł ukrywać dane na dodatkowej ścieżce (choć wirus Joshi odkryto w 1990 roku — dwa lata po wysłaniu przez Hanssena tajnej wiadomości).
- Komputer Tandy TRS-80 wykorzystywał dyskietki o 35 ścieżkach, jednak użytkownicy odkryli, że można również było formatować je do niestandardowej liczby 40 ścieżek. W 1988 roku komputer Tandy był już przestarzały, jednak czasem może to stanowić zaletę w przypadku szpiegostwa, jeżeli przeciwnik zakłada, że używa się współczesnych metod komunikacji.

O ile nie zostaną opublikowane bliższe informacje na temat działalności Hanssena związanej z komputerami, wszystko co nam pozostaje, to spekulacje odnośnie znaczenia uwagi o 40 ścieżkach.

- Szybkość przesyłania danych, która zależy od rodzaju nagrywarki, jest zwykle wyrażana za pomocą szybkości zapisu. Im większa wartość, tym szybciej odbywa się zapis dysków (zapis xna dyskach CD-R odbywa się szybciej niż na dyskach CD-RW). Przykładowo starszy model nagrywarki o prędkości zapisu wynoszącej 8× (około 1200 kB/s) kopiowałby płytę CD około 10 minut, natomiast nowszy model o szybkości zapisu 24× (około 3600 kB/s) zrobiłby to samo w czasie niewiele dłuższym od 4 minut. Pod koniec 2002 roku zaczęły się pojawiać nagrywarki o szybkości zapisu 52× i zapewne jest to wartość bliska maksymalnej możliwej do osiągnięcia.

Większość nagrywarek jest sprzedawana wraz z programami, które traktują dyski CD-R tak samo jak dyskietki i umożliwiają kopiowanie lub zapisywanie plików bezpośrednio na nich (na przykład popularny program DirectCD). Jeżeli używa się nagrywarki w celu skopiowania danych na dysk CD-R na komputerze ofiary, należy określić, że płyta ma być odczytywalna na innych komputerach. Oprogramowanie oferujące zapis bezpośredni nie pozwala, aby dysk CD traktowany jak dyskietka był dostępny na innych komputerach jako dysk CD tylko do odczytu. W takim przypadku przed wyjęciem płyty z napędu należy określić, że dysk ma zostać zapisany tak, aby odczytywały go inne napędy (w formacie ISO 9660).

Narzędzia — USB i IEEE 1394

Złącza USB (ang. *Universal Serial Bus*) oraz IEEE 1394 stanowią spełnienie marzeń szpiegów. Używane w przypadku nowoczesnego systemu operacyjnego obsługującego mechanizm Plug and Play wymagają od użytkownika jedynie podłączenia urządzenia takiego jak dysk twardy lub nagrywarka CD do komputera i rozpoczęcia procesu kopiowania plików. Zanim kupi się jednak jedno z takich urządzeń zewnętrznych, warto poznać kilka szczegółów.

Złącze USB pojawiło się w 1997 roku jako nowy sposób podłączania urządzeń peryferyjnych, ale nie wzbudziło większego zainteresowania aż do momentu pojawienia się systemu Windows 98 w czerwcu 1998 roku. Oryginalny standard USB 1.0/1.1 oferuje względnie wolny transfer danych (12 Mb/s). Komputery posiadające nowy układ USB 2.0 zaczęły się pojawiać latem 2002 roku. Ta wersja standardu USB umożliwia znaczne zwiększenie szybkości przesyłania danych — do 480 Mb/s. Na rynku zaczęły się pokazywać szybsze urządzenia magazynowania danych, które wykorzystują możliwości standardu USB 2.0 i zachowują zgodność wstecz ze standardem USB 1.1. Jednakże większość komputerów, jakie istnieją obecnie, obsługuje jedynie standard USB 1.1.

Rywalem USB jest standard IEEE 1394 (znany pod nazwą FireWire, będącą nazwą handlową firmy Apple, oraz i.Link — zastrzeżoną nazwą handlową firmy Sony). IEEE 1394 istnieje od 1986 roku i został przyjęty jako standard przez *IEEE* (ang. *Institute of Electrical and Electronics Engineers*) w 1995 roku. Firma Apple spopularyzowała go jako wydajny sposób przesyłania danych wideo oraz audio między komputerami Macintosh a innymi urządzeniami. Złącze IEEE 1394 umożliwia transfer danych na poziomie 400 Mb/s. Standard IEEE 1394b, dla którego produkty zaczynają się pojawiać na rynku, zwiększa tę wartość do 800 Mb/s.

Chociaż firma Microsoft zapewnia obsługę standardu IEEE 1394 w systemach Windows, o wiele bardziej prawdopodobne jest spotkanie w komputerze złącza USB. Dobrym źródłem informacji o urządzeniach USB, w tym o dyskach twardych i nagrywarkach CD, jest witryna EverythingUSB znajdująca się pod adresem *www.everythingusb.com*.

Płyty DVD

Płyty DVD (ang. *digital video disc* lub *digital versatile disc*) to kolejna generacja optycznych nośników danych. Płytę DVD można postrzegać jako szybszą płytę CD, która może przechowywać do 4,7 GB danych. W miarę jak ceny maleją (ceny napędów zaczynają spadać poniżej wartości 1000 zł) i kształtują się standardy, płyty DVD powoli będą wypierać płyty CD jako standardowy nośnik danych.

- Obecnie toczy się rywalizacja między grupami wspierającymi standardy DVD-R/DVD-RW a DVD+R/DVD+RW o dominującą pozycję na rynku. Niektórzy producenci, na przykład Sony, wybierają drogę kompromisu i zapewniają obsługę obu standardów.
- Zapis danych na płycie DVD z szybkością 1× odpowiada transferowi danych o wartości około 11Mb/s, co oznacza około dziewięciokrotny wzrost w porównaniu z szybkością 1× w przypadku płyt CD. Obecnie produkowane napędy umożliwiają zapis płyt DVD-R z szybkością 4×, zaś płyt DVD-RW z szybkością 2× (nagrywarki DVD umożliwiają również zapisywanie płyt CD-R oraz CD-RW).
- W zależności od liczby kupowanych sztuk, ceny płyt DVD-R wynoszą od ok. 6 do 14 zł, zaś płyt DVD-RW od ok. 10 do 18 zł. Ceny z pewnością spadną, kiedy nośniki będą stosowane powszechnie.

Obecnie o wiele bardziej prawdopodobne jest spotkanie komputera wyposażonego w nagrywarkę CD niż DVD, jednak warto mieć przy sobie kilka czystych płyt DVD — na wszelki wypadek.

Dyski ZIP

Zanim ceny nagrywarek CD spadły i stały się one popularne, firma Iomega (*www.iomega.com*) wprowadziła na rynek napędy ZIP, które miały stanowić alternatywę wobec dyskietek jako standard przenośnego nośnika danych. Pierwsze dyski ZIP pojawiły się w 1994 roku i oferowały pojemność 100 MB. Miały wygląd dużych dyskietek. Późniejsze modele napędów ZIP oferowały pojemności do 750 MB, zaś napędy Jaz — do 2 GB.

Zewnętrzna wersja napędów ZIP wykorzystująca port równoległy pracowała przy bardzo małej szybkości przesyłania danych — od 300 do 800 kB/s, gdy wewnętrzne wersje, współpracujące z magistralą IDE, zapewniały transfer rzędu 1,4 – 1,6 MB/s. Chociaż napędy Jaz oraz późniejsze modele ZIP zapewniały większą szybkość, koszt nośników (od ok. 30 do 40 zł za dysk) oraz pojawienie się tanich modeli nagrywarek CD nie pozwoliły na zdobycie przez nie popularności. Wciąż można spotkać napędy ZIP podłączone do starszych komputerów lub w niektórych kręgach specjalistów (napędy te były popularne wśród grafików komputerowych i w środowiskach twórczych).

Urządzenia pamięciowe

Jeżeli nie ma konieczności kopiowania dużych ilości danych, najlepszym rozwiązaniem może być wykorzystanie jednego z urządzeń obsługujących pamięć flash. Takie urządzenie można bardzo łatwo ukryć, gdyż ma grubość pudełka zapałek, a nawet mniejszą, oraz nie wymaga zewnętrznego źródła zasilania, gdyż pamięć flash jest nieulotna.

Wystarczy kartę pamięci włożyć do odpowiedniego adaptera oraz do złącza PC Card znajdującego się w laptopie (niektóre laptopy posiadają nawet złącza, które umożliwiają bezpośrednie wkładanie określonych typów kart) lub podłączyć ją do czytnika kart połączonego z komputerem PC i rozpocząć kopiowanie plików.

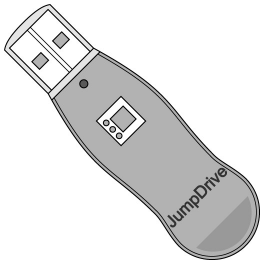
Producenci kamer cyfrowych, komputerów podręcznych i odtwarzaczy muzycznych nie opracowali wspólnego standardu pamięci flash i obecnie istnieje wiele ich typów, z których część wymieniono poniżej.

- **CompactFlash (CF).** Pierwsze urządzenie pamięciowe, wprowadzone na rynek przez firmę SanDisk w 1994 roku (i wciąż najpopularniejsze).
- **MemoryStick.** Urządzenie opracowane przez firmę Sony, wprowadzone do sprzedaży w 1998 roku.
- **Multimedia Memory Card (MMC).** Mała karta pamięciowa o rozmiarze znaczka pocztowego.
- **Secure Digital.** Karta pamięciowa z mechanizmem zabezpieczania przed zapisem zapobiegającym przypadkowemu usunięciu zawartości.
- **SmartMedia.** Urządzenia, które są mniejsze i lżejsze od kart CF.

Karty pamięci CompactFlash są dobrym rozwiązaniem dla szpiega, ponieważ mogą przechowywać o wiele więcej danych (w marcu 2003 roku firma SanDisk ogłosiła, że latem rozpocznie sprzedaż kart CF o pojemności 4 GB w cenie ok. 4000 zł za sztukę) niż inne urządzenia oraz są bardzo wytrzymałe. Nowe modele kart firmy SanDisk Ultra CF charakteryzuje prędkość przesyłania danych na poziomie 2,8 MB/s — to jest około dwa razy szybciej niż w przypadku standardowych kart CF. Ceny pamięci o pojemności 128 kB wynoszą ok. 200 – 250 zł (i wciąż spadają).

W przypadku znalezienia w czasie włamania karty pamięci, jeżeli zajdzie potrzeba skopiowania jej zawartości na dysk twardy, warto rozważyć wykorzystanie urządzenia czytającego i zapisującego karty FlashGo! Card firmy Imation (*www.imation.com*). To przenośne urządzenie wykorzystujące złącze USB obsługuje karty CompactFlash (Type I i II), SmartMedia, Multimedia Card, Secure Digital oraz Memory Stick i kosztuje ok. 220 zł. Najpierw należy włożyć kartę pamięci do niewielkiego, podręcznego czytnika, a następnie podłączyć czytnik do portu USB i rozpocząć kopiowanie plików.

Innym produktem opartym na wykorzystaniu pamięci flash, który z powodzeniem mógłby znaleźć się w filmie szpiegowskim, jest USB Flash Drive (patrz rysunek 7.1). Jest to niewielkie urządzenie pamięciowe, o rozmiarze nieco większym od kciuka, które podłącza się do portu USB. W systemach Windows ME, 2000 oraz XP wystarczy po prostu podłączyć je i rozpocząć kopiowanie plików (w przypadku starszych wersji systemu Windows należy najpierw zainstalować odpowiedni sterownik).



Rysunek 7.1. *Urządzenie JumpDrive 2.0 Pro firmy Lexar (www.lexarmedia.com), oferujące 256 MB pamięci przy transferze danych na poziomie 4,8 MB/s. Wystarczy podłączyć je do złącza USB i rozpocząć kopiowanie plików*

Urządzenia flash często mają jaskrawe kolory i niektóre z nich przypominają wyglądem długopisy, zaś inne pełnią rolę breloków. Ze względu na swój niewinny wygląd oraz fakt, że pojawiły się na rynku stosunkowo niedawno, mogą ujść uwadze osób, którym uda się złapać szpiega. Czytelnik posiadający odpowiednie umiejętności może nawet wyjąć urządzenie z oryginalnej obudowy i umieścić je w jeszcze mniej podejrzanym przedmiocie, na przykład w dużym markerze.

Oferowane pojemności wahają się obecnie od 8 MB do 512 MB, zaś ceny kształtują na poziomie od ok. 160 do 1000 zł. Szybkość przesyłania danych wynosi około 1 MB/s, zaś w przypadku niektórych nowszych modeli, pracujących w standardzie USB 2.0, nawet 4,5 MB/s.

Listę różnych typów pamięci flash można znaleźć pod adresem *www.everythingusb.com/hardware/Storage/USB_Flash_Drives.htm*.

Narzędzia — inwazja użytkowników odtwarzaczy iPod

W lutym 2002 roku w czasopiśmie *Wired News* ukazał się artykuł poświęcony wypadkowi, jaki wydarzył się w Dallas w stanie Teksas. Nastolatek, który słuchał muzyki, wykorzystując urządzenie Apple iPod (informacja dla starszych Czytelników — jest to swego rodzaju walkman, który odtwarza pliki MP3 zgrane z płyty CD lub pobrane z internetu), podłączył je do jednego z komputerów znajdujących się w sklepie. Pewien klient widział, jak nastolatek skopiował nową wersję pakietu Office dla systemu OS X na swoje urządzenie iPod (*www.apple.com/ipod/*). Dzięki złączu FireWire był w stanie skopiować produkt zajmujący 200 MB w czasie krótszym od minuty.

Choć z pewnością był to przypadek ewidentnego piractwa komputerowego powiązanego z kradzieżą sklepową, to wskazuje on jednak, że urządzenie iPod (występujące w wersjach o pojemnościach 5 GB, 10 GB oraz 20 GB i reklamowane jako umożliwiające przegranie całego dysku CD w ciągu 15 sekund) może być również użyte do przeprowadzania tajnych włamań do komputerów Macintosh lub PC wyposażonych w złącze FireWire.

Są dostępne podobne produkty współpracujące z komputerami PC, na przykład Nomad Jukebox Zen firmy Creative Labs (*www.nomadworld.com/products/Jukebox_Zen/*). Owe nowe odtwarzacze plików MP3, które podłącza się do portu USB, zapewniają ogromne możliwości szpiegowskie. Odtwarzacz Zen posiada nawet mikrofon umożliwiający podsłuch z nagrywaniem.

Odtwarzacze plików MP3 podłączane do portu USB i obsługujące proces kopiowania plików mogą stanowić idealne narzędzie szpiegowskie, maskujące rzeczywiste działania: „Kto? Ja? Tylko sprzątałem pokój, słuchając muzyki".

Dyski twarde

Pierwszy dysk twardy pojawił się w 1957 roku jako element komputera klasy mainframe firmy IBM (RAMAC 350). Zawierał on 50 24-calowych dysków, które mogły przechowywać 5 MB danych. Kosztował ok. 140 000 zł za roczne wypożyczenie. Obecnie, kiedy dyski mają ponad 100 GB pojemności, ceny przekroczyły wartość graniczną kilku złotych za gigabajt pamięci.

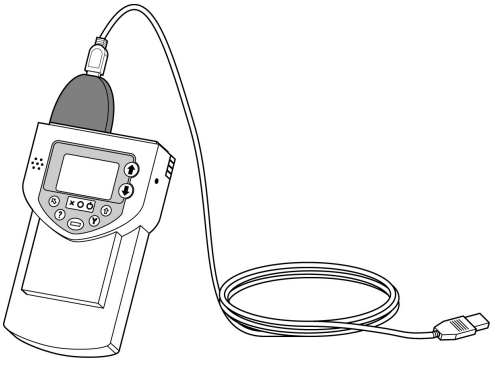
Kopiowanie dysków twardych jest bardzo często wykonywaną operacją w przypadku badań sądowych, czasem także w trakcie operacji szpiegowskich. Należy otworzyć obudowę komputera i podłączyć dysk jako podrzędny (slave) względem głównego dysku wewnętrznego. Następnie należy uruchomić komputer za pomocą dysku utworzonego przez program służący do kopiowania i utworzyć kopię całej zawartości dysku głównego na dysku podrzędnym. Nie trzeba się nawet martwić o problemy związane z logowaniem do systemu Windows. Po zakończeniu działań wystarczy wszystko złożyć z powrotem razem i zabrać dysk podrzędny do bezpiecznego miejsca w celu przeprowadzenia analiz.

Szybkość przesyłania danych w przypadku typowego wewnętrznego dysku twardego, szczególne w przypadku szybszych modeli o prędkości obrotowej talerzy wynoszącej 7200 obr/min z mechanizmem buforowania danych, może osiągnąć wartość 100 MB/s. Jednakże należy również wziąć pod uwagę czas wymagany do otwarcia obudowy, zainstalowania dysku, przeprowadzenia procesu kopiowania, wyjęcia dysku twardego oraz zatarcia śladów. Jeżeli w trakcie włamania nie dysponuje się zbyt dużą ilością czasu, być może lepszym rozwiązaniem będzie wykorzystanie napędu zewnętrznego, takiego jak dysk twardy USB lub Microdrive.

Narzędzia — sprzętowe metody kopiowania zawartości dysków

Jednym z ulubionych narzędzi FBI (i innych rządowych agencji wywiadowczych oraz organów ścigania) służącym do sporządzania kopii zawartości dysków twardych jest SF-5000 firmy Logicube (patrz rysunek 7.2). Wystarczy jedynie podłączyć źródłowy dysk twardy oraz czysty dysk docelowy do urządzenia, a to utworzy wierną kopię zawartości dysku. FBI używało tych urządzeń setki razy przez ostatnich kilka lat i ceni je za szybkość działania, przenośność oraz łatwość użycia. (Urządzenie sprawuje się bardzo dobrze w przypadku dysków IDE, jednak znacznie zwalnia w przypadku dysków SCSI). Cena urządzenia w podstawowej wersji wynosi ok. 4800 zł (pełny zestaw kosztuje ok. 9000 zł). Więcej informacji można znaleźć pod adresem *www.logicube.com*.

Rysunek 7.2. *Podręczne urządzenie SF-5000 firmy Logicube służące do kopiowania zawartości dysków twardych z kablem USB. Jest to jedno z ulubionych urządzeń FBI i innych agencji*



Inne podobne urządzenia popularne wśród funkcjonariuszy organów ścigania (choć oczywiście można ich używać także w trakcie „mniej" legalnych działań) to:

Portable Pro Drive firmy Corporate Systems. Chociaż urządzenie Logicube jest szybsze w przypadku kopiowania zawartości dysku IDE, produkt Corporate Systems obsługuje kopiowanie dysków IDE, SCSI, SCA oraz 2,5-calowych dysków używanych w laptopach. Nie jest to urządzenie w pełni przenośne i zajmuje sporych rozmiarów walizkę, ale wielu specjalistów uważa, że przy swojej cenie wynoszącej ok. 4000 zł jest to niesłychanie opłacalny zakup. Więcej informacji można znaleźć pod adresem *www.corpsys.com*.

Image Masster Solo-2 firmy Intelligent Computer Solutions. Image Masster Solo-2 to kolejne przenośne urządzenie służące do kopiowania, bardzo podobne do produktu firmy Logicube. Wiadomo, że urządzenie to dobrze sobie radzi w przypadku napotkania uszkodzonych sektorów na dysku, co może powodować problemy w przypadku niektórych innych narzędzi. Podstawowa wersja urządzenia kosztuje ok. 6000 zł. Więcej informacji można znaleźć pod adresem *www.ics-iq.com*.

Urządzenia te bardzo dobrze nadają się do wykonywania kopii na miejscu, jednak można również skorzystać z laptopa i programu, takiego jak linuksowe polecenie dd lub Norton Ghost w celu osiągnięcia tych samych rezultatów.

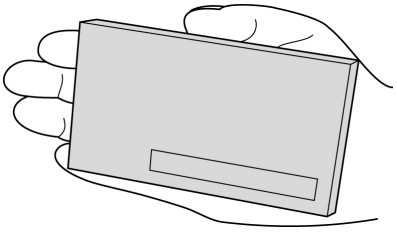
Oprogramowanie służące do wykonywania kopii dysków twardych omówiono w rozdziale 5.

Dyski twarde USB

Dyski twarde USB (oraz IEEE 1394), pracujące w standardzie Plug and Play, stanowią doskonałe narzędzia służące do kopiowania danych. Zamiast tymczasowo instalować wewnętrzny dysk twardy w komputerze ofiary, podłączamy po prostu dysk zewnętrzny

do portu USB i rozpoczynamy kopiowanie plików (szybkość przesyłania danych jest niższa niż w przypadku dysków wewnętrznych, gdyż ograniczeniem jest tu maksymalna szybkość transferu danych poprzez złącze USB). Dostępne są dwa rodzaje dysków.

- **Standardowe.** Choć urządzenia te można uznać za przenośne i wykorzystywać w trakcie działań szpiegowskich, z pewnością nie zmieszczą się one do kieszeni (szczególnie w przypadku posiadania dodatkowego zasilacza oraz kabla zasilającego). Dyski twarde przechowują od 20 do 200 GB danych i kosztują od ok. 400 do 1000 zł.
- **Kompaktowe.** Te niewielkie napędy z łatwością mieszczą się w kieszeni koszuli i mogą przechowywać od 5 do 60 GB danych (patrz rysunek 7.3). Kosztują od ok. 700 do 1600 zł. Zasilanie pobierają ze złącza USB, tak więc nie są potrzebne zewnętrzne źródła zasilania.



Rysunek 7.3. *Dysk Pockey DataStor (www.pocketec.net) bez problemu mieści się w kieszeni i waży tylko około 150 g. Stanowi doskonałe narzędzie szpiegowskie służące do kopiowania dużych ilości danych*

Microdrive

Jeśli celem ataku jest laptop lub komputer biurkowy z czytnikiem kart PC Card, warto rozważyć użycie urządzenia Microdrive. Microdrive to czytnik PC Card z wbudowanym jednocalowym dyskiem twardym, który może przechowywać do 340 MB, 500 MB, 1 GB lub 4 GB danych (w zależności od modelu). Napęd współpracuje z dowolnym portem zgodnym ze standardami CompactFlash CF+ Type II lub PC-Card i charakteryzuje się szybkością przesyłania danych na poziomie od 40 do 60 Mb/s. Napęd o pojemności 1 GB kosztuje ok. 1400 zł. Pod koniec 2002 roku firma Hitachi przejęła od firmy IBM działalność związaną z produkcją dysków twardych i obecnie produkuje i sprzedaje napędy Microdrive. Więcej informacji można znaleźć pod adresem *www.hgst.com/products/microdrive/index.html*.

System archiwizacji na taśmach

Systemy taśmowe są popularne w warunkach korporacyjnych jako metoda archiwizacji danych i choć istnieją modele przenośne, nie nadają się one zbytnio do celów szpiegowskich (chyba że w celu archiwizacji materiału dowodowego w warunkach laboratoryjnych). Tańsze systemy taśmowe są wolne w porównaniu z innymi nośnikami danych i wymagają częstego zmieniania taśm. Jeżeli w komputerze ofiary spotka się system taśmowy, należy użyć innego nośnika w celu skopiowania plików. Jeżeli jednak zdecydujemy się na użycie takiego systemu, koniecznie trzeba zanotować rodzaj sprzętu oraz oprogramowania, tak aby później uniknąć problemów z odtworzeniem danych.

Alternatywne metody kopiowania danych

Nie należy sądzić, że dyskietki, płyty CD, dyski twarde i karty pamięci to jedyne możliwości kopiowania danych. Dobry szpieg zawsze ma pod ręką odpowiednie narzędzie do wykonania zaplanowanego zadania i istnieje kilka alternatywnych rozwiązań związanych z kopiowaniem danych, których wykorzystanie szpieg może wziąć pod uwagę.

Przesyłanie danych siecią

Jeżeli komputer ofiary jest podłączony do sieci (na przykład internetu), można przesłać dane do innego komputera, również podłączonego do internetu, zamiast nagrywać je na nośniki danych. Należy jednak pamiętać o kilku sprawach.

- Szybkość przesyłania danych jest całkowicie uzależniona od szybkości połączenia sieciowego. Wolne połączenie może narazić na zdemaskowanie, jeśli będzie trzeba zbyt długo czekać na przesłanie.
- Połączenia sieciowe często podlegają rejestracji (czasem również monitorowaniu) i prawdopodobnie zostawi się wówczas ślady włamania. Należy przynajmniej zapewnić, że adres IP, pod który wysyła się dane, nie umożliwi wyśledzenia nas.

Jeżeli warunki umożliwiają przeprowadzenie kopiowania poprzez sieć, istnieją trzy możliwości wyboru.

- **FTP, Telnet oraz SSH.** Jeżeli posiada się dostęp do konta obsługującego usługę FTP, Telnet lub SSH, zawsze można połączyć się z tym kontem, a następnie skopiować pliki lokalne na odległy komputer. Należy mieć ze sobą odpowiednie aplikacje klienckie na dysku narzędziowym.
- **Poczta elektroniczna.** Jeżeli na komputerze ofiary ma się dostęp do klienta poczty elektronicznej, można po prostu przesłać załączniki na założone w tym celu konto pocztowe. Należy jednak zachować ostrożność, gdyż w przypadku większych ilości danych można przekroczyć ograniczenia rozmiaru skrzynki pocztowej.
- **NetCat.** NetCat to narzędzie uruchamiane z poziomu wiersza poleceń, które każdy szpieg powinien posiadać. Opracował je haker o pseudonimie Hobbit w 1995 roku. Umożliwia ono skanowanie portów, kopiowanie plików, zdalne wykonywanie poleceń i przeprowadzanie wszelkiego rodzaju przydatnych działań sieciowych. W celu skopiowania plików na inny komputer należy sprawdzić, czy NetCat działa na maszynie docelowej, uruchomić program na maszynie źródłowej, określić adres IP oraz numer portu celu i w końcu rozpocząć kopiowanie. Program jest dostępny w wersjach dla systemów Windows i Unix (*www.atstake.com/research/tools/network_utilities/*). Program CryptCat, będący zmodyfikowaną wersją NetCata, który szyfruje dane za pomocą algorytmu Twofish, jest dostępny pod adresem *www.farm9.org/Cryptcat/GetCryptcat.php*).

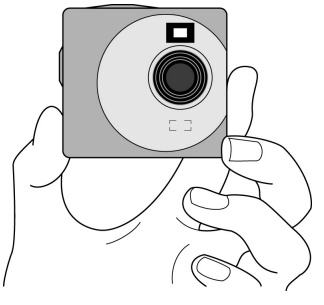
Aparaty cyfrowe

Każdy szpieg komputerowy powinien mieć do dyspozycji aparat cyfrowy. Aparaty stanowią podstawowe narzędzie służące do wykonywania zdjęć istotnych informacji, które

nie znajdują się w łatwej do skopiowania postaci cyfrowej. Są również nieodzowne czasie tajnych włamań w celu udokumentowania stanu otoczenia, tak aby po zakończeniu działań mieć pewność, że wszystko wygląda tak, jak przed włamaniem.

Kwintesencją aparatu szpiegowskiego jest miniaturowy model Minox (więcej informacji na jego temat można znaleźć pod adresem *www.minox-web.de*). Ten niewielki, ważący 56 gramów aparat, wykonujący zdjęcia na filmie 8 × 11 mm istnieje od lat 30. XX wieku i wciąż jest popularny wśród wielu agencji wywiadowczych na całym świecie.

Choć Minox stanowi klasykę, aparaty cyfrowe są zdecydowanie bardziej wszechstronne i w wielu przypadkach bardziej odpowiednie dla celów szpiegowskich. Można korzystać z aparatu o standardowych wymiarach, ale powstaje również coraz więcej aparatów, które kosztem jakości zdjęć oferują bardzo małe rozmiary. Aparaty takie jak SiPix StyleCam Snap (*www.sipixdigital.com*, patrz rysunek 7.4) oraz Creative Labs Cardcam (*www.americas.creative.com*) mieszczą się w dłoni, są bardzo łatwe do ukrycia i tanie (ich cena wynosi około, odpowiednio, 1600 oraz 2400 zł). Chociaż nie mają wyświetlaczy ciekłokrystalicznych, fleszów, opcji zbliżenia, a jakość otrzymywanych zdjęć nie jest najlepsza, z pewnością znajdą zastosowanie w przypadku wielu działań szpiegowskich.



Rysunek 7.4. *SiPix StyleCam Snap — niewielki aparat cyfrowy ważący mniej niż 60 g*

Podsumowanie

Istnieje wiele możliwości skopiowania danych z komputera ofiary, a niektóre z nich są szybsze i zapewniają większe bezpieczeństwo niż inne. Kopiując dane, w pierwszej kolejności należy wziąć pod uwagę czas, jakim dysponuje się na wykonanie zadania. Ograniczenia czasowe determinują wybór metody kopiowania, odpowiedni nośnik danych oraz ilość danych możliwą do skopiowania. Przed przeprowadzeniem procesu kopiowania, czy będzie to wykonanie obrazu dysku twardego w laboratorium, czy potajemne skopiowanie biznesplanu konkurencji, najpierw należy przećwiczyć działania związane z wybranym urządzeniem oraz nośnikiem danych. Takie ćwiczenia sprawiają, że poznaje się cały proces (i identyfikuje potencjalne problemy) oraz pozwalają na oszacowanie wymagań czasowych odnośnie kopiowania.

Z drugiej strony, bezpieczeństwo fizyczne stanowi klucz do skutecznej ochrony przed utratą danych. Oczywiście im trudniej jest szpiegowi uzyskać dostęp do komputera, tym istnieje większe prawdopodobieństwo, że dane uda się ochronić. Czas jest zawsze po stronie potencjalnej ofiary. Bezpośrednio wiąże się on z ilością danych, jakie można skopiować, tak więc, jeśli można ograniczyć czas, jaki szpieg spędzi przy komputerze,

ogranicza się jednocześnie ilość danych, które może potencjalnie skraść. Systemy alarmowe, kamery systemu nadzoru oraz strażnicy, którzy regularnie patrolują budynek, stanowią rozwiązania mogące ograniczyć możliwości działania szpiega. Traktowanie czasu jako środka obronnego sprawdza się dobrze w sytuacji, gdy należy skopiować duże ilości danych, jednak pojedynczy dokument często można skopiować w ciągu kilku sekund. W tym momencie dużą rolę zaczyna odgrywać szyfrowanie jako kolejna warstwa zabezpieczeń. Nawet jeśli szpieg zdoła skopiować dane, w przypadku użycia silnych metod szyfrowania (i stosowania prawidłowych zasad używania haseł) istnieje duże prawdopodobieństwo, że nie uda mu się odczytać interesujących go informacji.