Rozdział 4.
Cracking

Internet daje nam możliwość łatwego i szybkiego przepływu i dostępu do informacji na całym świecie, czyniąc zeń tzw. „światową pajęczynę". Bardzo szybko w związku z tym producenci wszelkiego typu oprogramowania oraz autorzy software'u w Polsce zdali sobie sprawę z możliwości taniego udostępniania swoich programów szerokiemu gremium. Powstawały i powstają wciąż nowe serwery gromadzące wszelkiego rodzaju oprogramowanie dla różnych systemów operacyjnych. Są to często ogromne archiwa. Można je sklasyfikować następująco:

- Programy oferowane za darmo — *freeware* lub *public domain*;
- Programy oferowane za niewielką opłatą — *shareware*;
- Programy oferowane w wersji demonstracyjnej — *trial*.

Freeware to najczęściej zbiór aplikacji niewielkich rozmiarów, których zakres możliwości ogranicza się do kilkunastu funkcji. Nie posiadają one drukowanych instrukcji obsługi, a często nawet pomocy podręcznej. Ich twórcami są najczęściej początkujący programiści.

Autorzy w większości przypadków nie biorą odpowiedzialności za ewentualne szkody powstałe w wyniku eksploatacji programów. W zamian za te ograniczenia użytkownik uzyskuje całkowicie darmowe oprogramowanie, z możliwością powielania i przenoszenia na inne komputery dowolną liczbę razy. Ten fakt spowodował, że programy typu freeware należą do najbardziej lubianych przez użytkowników, gdyż pomimo wielu niedogodności niektóre z nich okazują się bardzo przydatne.

S*hareware* to najczęściej dosyć zaawansowany program. Choć nie jest to jeszcze rozbudowany pakiet oprogramowania, ma często wbudowaną pomoc podręczną i podręcznik użytkownika (nawet w wersji drukowanej). Zdarza się, że są to rozbudowane wersje programów freeware wzbogacone o nowe możliwości.

Wielcy i znani producenci oprogramowania bardzo chętnie rozpowszechniają swoje produkty w postaci shareware. Jednak całe wsparcie techniczne ze strony autora lub producenta użytkownik zyskuje dopiero po uiszczeniu opłaty rejestracyjnej i zareje-

strowaniu swojej kopii programu. Zanim program typu shareware zostanie zarejestrowany, posiada wbudowane ograniczenia funkcjonalności.

Oprogramowanie w wersji *trial*, czyli w wersji demonstracyjnej to najczęściej aplikacje, które są okrojonymi zaawansowanymi produktami profesjonalnych firm softwareowych. Najczęściej można je wypróbowywać przez określony okres czasu (np. 30 dni), ale mogą one nie posiadać podręcznej pomocy, a część funkcji jest nieobsługiwana.

Należy tutaj zaznaczyć, że w dzisiejszych czasach dopiero zakup pełnej wersji programu, najczęściej na krążku CD wraz z instrukcją użytkownika, zapewnia wsparcie techniczne ze strony producenta.

Ponieważ programy shareware są zwykle wersjami z wbudowanymi elementami zabezpieczeń i różnorakich ograniczeń, cracker może modyfikując odpowiednio ich kod usunąć te zabezpieczenia i „przerobić" na wersję nieposiadającą żadnych ograniczeń.

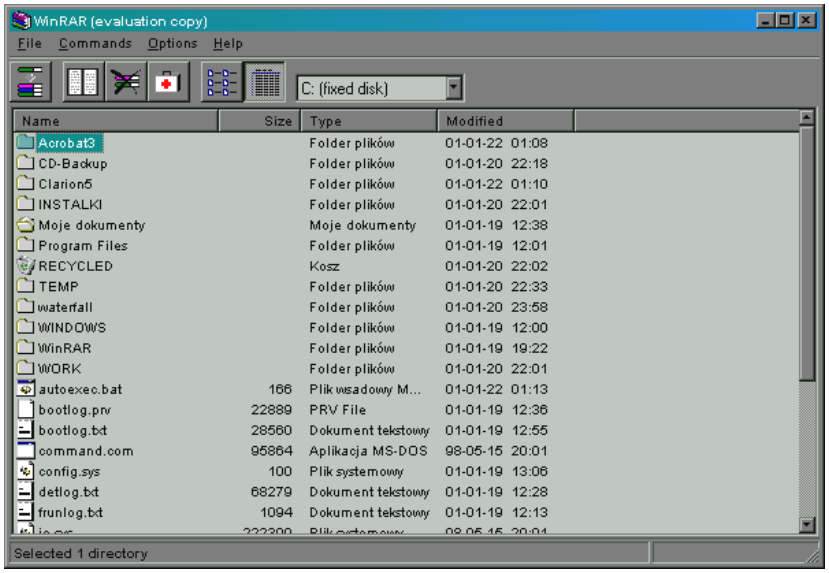
W znacznej mierze procesowi crackowania podlegają programy typu shareware. Ich definicję najprościej jest podać za magazynem komputerowym *PC World Computer* (Płyta CD 1/99/A, PC World Computer nr 1/99, IDG Poland S.A., 1999, *http://www.pcworld.com.pl.)*.

Shareware — to popularny sposób dystrybucji oprogramowania „działający" na zasadzie „wypróbuj, zanim kupisz". Obejmuje on programy (chronione zastrzeżonymi prawami autorskimi), które do chwili rejestracji użytkownik posiada tylko „na próbę". Czas testowania programu jest ograniczony zwykle do 10-60 dni. Czasami program ma „wyłączone" niektóre opcje. Legalizacja programu polega na wniesieniu na rzecz autora lub producenta stosownej — ale dość niskiej w porównaniu z cenami programów komercyjnych — opłaty rejestracyjnej. W opisie każdego programu shareware powinny się znajdować zasady jego rejestracji. Należy pamiętać, że opłata za udostępnienie oprogramowania obejmuje tylko koszt nośnika i koszty handlowe dystrybutorów, wydawców CD-ROM, itd. i nie zwalnia w żaden sposób z konieczności wniesienia opłaty rejestracyjnej dla każdego programu shareware.

Definicja ta uświadamia nam fakt, że programy shareware są dostarczane do końcowego odbiorcy bądź to zapisane na płytach CD dołączanych do czasopism komputerowych (użytkownik staje się posiadaczem kopii programu „przy okazji"), bądź przez Internet (użytkownik może otrzymać zawsze najnowszą wersję programu). Dalej odbiorca jest zachęcany do wypróbowania programu, aby mógł się przekonać, że jest on niezbędnie potrzebny przy korzystaniu z komputera. Jeżeli zatem użytkownik rzeczywiście uzna, że program mu się przyda i zdąży się przyzwyczaić do korzystania z niego, będzie chciał przedłużyć okres jego użytkowania.

Jednak normalnie program może się dać uruchomić tylko przez pierwszy miesiąc, a niektóre z jego funkcji mogą nie być aktywne. Wtedy pojawia się propozycja autora, który sugeruje, by dokonać rejestracji kopii i stać się posiadaczem legalnej i pełnej wersji programu. Ale z wielu przyczyn część użytkowników nie decyduje się

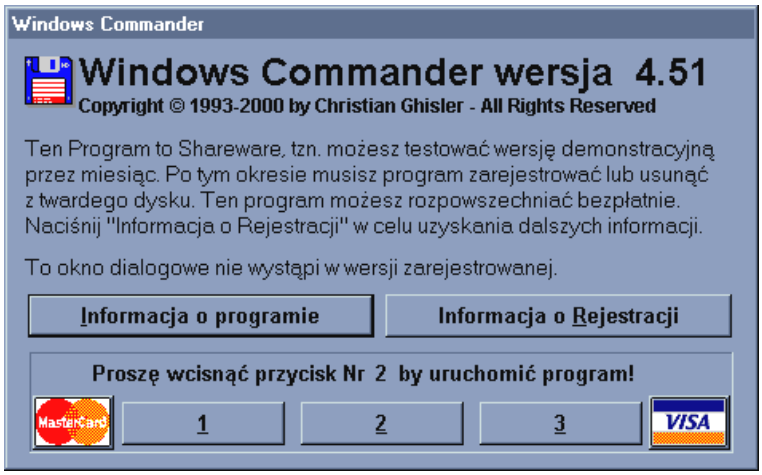
na wybór tego rozwiązania. Program shareware ma jeszcze jedną wielką zaletę — opłata rejestracyjna jest zwykle niska, co wpływa na podjęcie decyzji.



Dystrybucja shareware'a jest obecnie bardzo rozpowszechniona na całym świecie i każde szanujące się czasopismo komputerowe dołącza do swoich wydań krążki CD, z aktualnymi wersjami lub zupełnie nowymi programami shareware. Z drugiej strony autorzy programów starają się dotrzeć do jak największej liczby końcowych odbiorców, a najbardziej popularne programy, można znaleźć na kilku krążkach jednocześnie wydanych w tym samym okresie czasu. Wspomnieć tu można o takich programach, jak WinAmp służący do odgrywania bardzo popularnego formatu zapisu dźwięku Mpeg Layer 3 czy WinZip i WinRar służący do kompresji i archiwizowania danych, których coraz to nowe wersje ukazują się prawie co miesiąc. Jednak największym dystrybutorem tego typu oprogramowania jest Internet. Popularne serwisy gromadzą w swoich archiwach dane na temat kilku — a nawet kilkudziesięciu milionów programów — z których większość to właśnie programy typu shareware.

W czasach kiedy Internet nie był powszechnym środkiem wymiany informacji, a magazyny komputerowe były pozbawione drogich wówczas płyt CD, dystrybucja shareware'u była dość ograniczona, ale jednak istniała. Najprostszym sposobem zdobycia upragnionego programu było posiadanie znajomych, którzy albo mieszkali za granicą i mieli bliższy kontakt z producentem, albo też mieli znajomych, od których dostawali pocztą przesyłane na dyskietkach programy. Co prawda ta metoda dystrybucji była dość powolna, pomimo to popularne programy miał prawie każdy (tak było np. w Polsce czy byłym Związku Radzieckim). Innym sposobem choć raczej praktykowanym w Polsce w ograniczonym zakresie było zdobywanie programów z sieci BBS-ów. Oprócz samego komputera potrzebny był zatem modem i jakiś BBS, który pozwalał na ściąganie oprogramowania. Obecnie jednak BBS-y zostały w dużej mierze wyparte przez serwery FTP, a pocztą przesyłane są megabajty programów.

Dlaczego programy te drażnią crackerów? Otóż jedną z rzeczy najbardziej uprzykrzających życie użytkownika jest tzw. *nagscreen*, czyli okienko z komunikatem, które pokazuje się albo przed uruchomieniem — często zanim można je wyłączyć mija kilka sekund — albo pojawia się co jakiś czas w trakcie działania programu i przypomina użytkownikowi, że program, którego używa jest typu shareware i jego kopia nie została jeszcze zarejestrowana, w związku z czym autor prosi o dokonanie wpłaty na jego konto i zalegalizowanie programu. Po pewnym czasie cracker zaczyna się trochę denerwować taką nadopiekuńczością autora i zwykle wtedy podejmuje decyzję o tym, aby w jakiś sposób obejść ograniczenia i otrzymać produkt naprawdę przyjazny dla użytkownika.



Jak postępuje cracker w tym wypadku? Zwykle musi poznać kod źródłowy programu, który jest najbardziej strzeżoną tajemnicą autora i w żaden sposób nie można go od niego wyciągnąć (chociaż dysponuje skompilowaną postacią kodu — wykonywalnym plikiem zakodowanym w postaci maszynowej zrozumiałej dla procesora). Trzeba zatem dokonać dekompilacji kodu i w ten sposób otrzymać można program, który już pozwala się modyfikować. Jednak dekompilować kod maszynowy można tylko do języka najniższego poziomu — asemblera, a ten nie jest najbardziej przejrzystym i czytelnym językiem programowania. Co więcej — kod małego programu to kilkadziesiąt tysięcy linii kodu asemblera i nawet pobieżne jego przejrzenie nastręcza wiele trudności. Tym właśnie, czyli odpowiednim zmodyfikowaniem kodu i dostarczeniem gotowego produktu, zajmuje się cracker.

Cracking (łamanie, rozgryzanie problemu) to innymi słowy — podjęcie działań mających na celu usunięcie ograniczeń czasowych lub funkcjonalnych zabezpieczonego programu komputerowego poprzez modyfikację jego kodu lub dokonanie nieuprawnionej rejestracji umożliwiającej korzystanie z programu niezgodnie z przepisami prawa.

Jak wynika z przedstawionej definicji, procesowi crackowania podlegają wszystkie zabezpieczone programy komputerowe. Dotyczy to zarówno gier, które zwykle nie dają się uruchomić bez umieszczonej w napędzie płyty CD, jak i programów typu trial, które zwykle są zubożone o niektóre funkcje i dodatkowo posiadają ograniczenie

czasowe. Crackowanie nie musi oznaczać modyfikacji kodu, ale może prowadzić do poznania mechanizmu uzyskiwania numeru rejestracyjnego na podstawie wprowadzonej nazwy użytkownika. Zarówno sam proces crackowania, jak i następujące po nim korzystanie ze zmodyfikowanego lub nielegalnie zarejestrowanego programu jest łamaniem prawa.

Ponieważ nie wszyscy użytkownicy komputerów posiadają umiejętność programowania, to ktoś, kto włamuje się do programu komputerowego musi nie tylko być zaznajomiony z samym systemem operacyjnym, w którym program pracuje, ale również — chociaż niekoniecznie bardzo dobrze — z językiem asemblera. Tym kimś jest właśnie cracker. To on stara się wniknąć w program, zanalizować wszystkie zabezpieczenia jakie autor zastosował, a następnie zniwelować je pozostawiając program pozbawiony ograniczeń, którego można używać do woli. Crackerzy najczęściej uzasadniają to, co robią na dwa różne sposoby. Część z nich uważa, że jakiekolwiek oprogramowanie, które zostaje rozpowszechniane publicznie nie powinno zawierać ograniczeń, gdyż to bardziej zniechęca niż zachęca użytkownika do zakupu pełnej wersji. Ponadto jeśli użytkownik uzna, że program wart jest zakupu, to na pewno go kupi, gdy jednak używa go tylko raz na jakiś czas, to nie ma sensu wydawać pieniędzy, bo wartość inwestycji będzie niewspółmiernie wysoka w stosunku do osiągniętych korzyści. Z tych właśnie powodów należy umożliwić użytkownikom nieskrępowany dostęp do wszystkich funkcji danego programu oraz nie ograniczać czasu jego eksploatacji, a decyzję o tym, czy program kupić, czy też używać dalej jego nielegalnej kopii, należy pozostawić użytkownikowi i jego sumieniu. Inni crackerzy uważają to, co robią za sztukę. Podchodząc w ten sposób do całej sprawy, traktują złamanie jakiegoś programu jak wyzwanie rzucone im przez twórcę. Wyzwanie, z którego najczęściej wychodzą zwycięsko. Wynika to po części z faktu, iż programy są zabezpieczane zwykle bardzo podobnie i kiedy już opanuje się metody rozpracowywania poszczególnych zabezpieczeń złamanie kolejnego, podobnie zabezpieczonego programu nie jest dużym problemem i trwa czasem mniej niż dziesięć minut. Z drugiej strony cracker-artysta odczuwa przyjemność ze swojej pracy tylko wtedy, gdy znajduje nowe rodzaje zabezpieczeń po raz pierwszy zastosowane w danym programie, lub tak skomplikowane, że ich „rozgryzienie" zajmuje kilka dni. Widać tu zresztą pewną analogię do hakerów, którzy satysfakcję osiągają dopiero, gdy uda im się włamać na dobrze zabezpieczony serwer, a nie taki, który jest źle administrowany. Ze względów bezpieczeństwa crackerzy nie ujawniają swoich prawdziwych imion, ale używają pseudonimów. Najbardziej pracowici z nich łamią w ciągu roku kilka tysięcy programów (np. słynna grupa Phrozen Crew). Po złamaniu zabezpieczeń cracker pisze tzw. c*rack*, a więc program, który po uruchomieniu zamienia część łamanego programu tak, aby przekształcić go w pełną wersję. Crack jest najczęściej bardzo małym programem napisanym dla środowiska DOS, a jego objętość wynosi kilka kilobajtów. Swoje poglądy crackerzy wymieniają na łamach wielu usentowych list lub za pomocą usługi IRC. Najczęściej przedstawiane tam wysyłki dotyczą próśb o konkretny crack.

Cracki są zwykle umieszczane w Internecie, jednak często ich żywot jest krótkotrwały, gdyż administratorzy usuwają „zakazane" strony, mimo iż prawie zawsze osoby odpowiedzialne za daną witrynę umieszczają tzw. *disclaimer* (zaprzeczenie).

Ponieważ ich treść jest bardzo podobna, można przytoczyć tu disclaimer pochodzący z jednej z polskich stron poświęconej crackowaniu, który głosi, że:

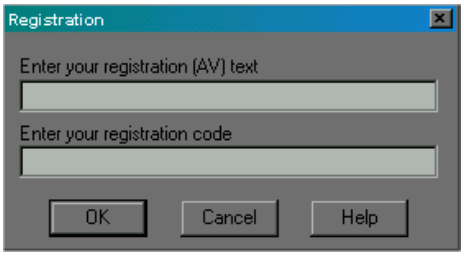
„Wszelkie materiały i informacje zawarte na tych stronach przeznaczone są jedynie do celów informacyjno-edukacyjnych. Autorzy zastrzegają sobie, że nie odpowiadają za użycie tych informacji do niecnych i niezgodnych z prawem celów. Autorzy nie odpowiadają za straty poniesione w wyniku wykorzystania tych materiałów. Prawo do pisania tego typu tekstów zapewnia wolność słowa i publikacji. Prosimy o rozsądne wykorzystanie informacji zawartych na tych stronach".

Poszukując cracka do konkretnego programu, można posłużyć się wyspecjalizowaną wyszukiwarką internetową. Obecnie największą z nich jest Astalavista (*http://astalavista.box.sk*), która kataloguje w swoich bazach ponad tysiąc stron zawierających cracki. Są wśród nich również polskie cracki.

Z jakimi rodzjami zabezpieczeń boryka się cracker? Do najczęściej łamanych zabezpieczeń należą aktualnie:

- Klucz rejestracyjny (*serial number*);
- Program rejestracyjny (*upgrade patch*);
- Plik kluczowy (*key file*);
- Sprawdzenie obecności płyty CD (*CD check*);
- Ograniczenia w programach trial;
- Klucze sprzętowe.

Zdecydowanie najpopularniejszym, ale i najłatwiejszym do złamania sposobem rejestracji programów, jest *klucz rejestracyjny*. Z reguły po wpłaceniu odpowiedniej opłaty rejestracyjnej użytkownik dostaje pocztą zwykłą lub przez Internet tzw. *serial number*, który zostaje wygenerowany na podstawie jego danych u producenta programu. Następnie po wprowadzeniu go w odpowiednie pole, program staje się w pełni działającym produktem bez jakichkolwiek ograniczeń.

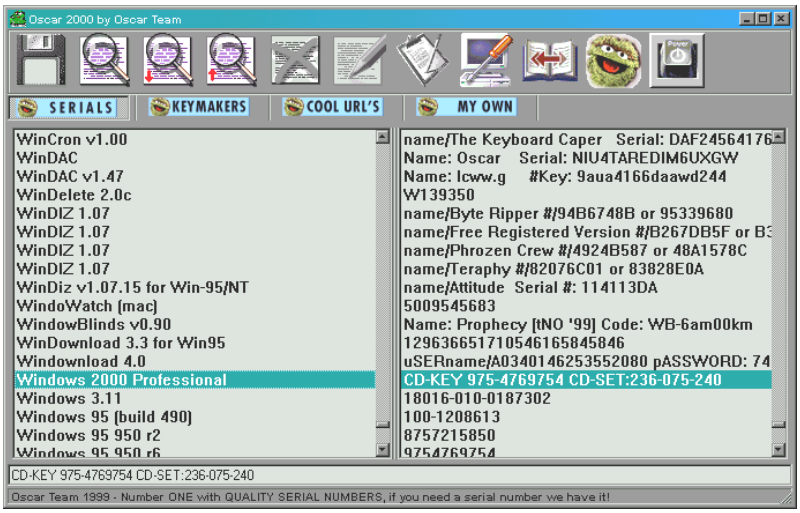


Aby dostarczyć użytkownikowi rozwiązanie problemu klucza, crackerzy stosują dwa sposoby. Pierwszy polega na wygenerowaniu klucza dla wybranej przez siebie nazwy użytkownika, który następnie jest udostępniany poprzez witryny internetowe albo poprzez programy zawierające bazy danych aktualnych kluczy rejestracyjnych popularnych programów. Najbardziej znanym tego typu programem jest Oscar grupy

Phrozen Crew. Zawiera on (oprócz kluczy) kilkadziesiąt plików kluczowych oraz adresy stron WWW producentów oprogramowania. Można również dodać własne klucze rejestracyjne poszerzając tym samym bazę Oscara. Drugi sposób polega na zamianie części kodu odpowiedzialnej za sprawdzenie czy kod wpisany przez użytkownika jest poprawny i został dostarczony przez producenta. Wówczas wystarczy, że użytkownik wpisze dowolny klucz, a zmieniony program uzna, iż jest on poprawny i zarejestruje program. W tym wypadku cracker pisze cracka, który po uruchomieniu zamienia część łamanego programu umożliwiając w ten sposób wprowadzenie dowolnego klucza.

Niektóre programy (jak np. WinDAC32) wymagają osobnego programu, dostarczanego przez producenta po wpłaceniu opłaty rejestracyjnej, który usuwa jego ograniczenia i w ten sposób zamienia go na pełną wersję bez ograniczeń. Do zadań crackera w tym przypadku należy znalezienie wszystkich miejsc, w których program jest ograniczany funkcjonalnie bądź czasowo, a następnie napisanie cracka, który zlikwiduje te ograniczenia. Spełnia więc on taką samą rolę jak dostarczony przez producenta tzw. *upgrade patch*. Zdarza się jednak i tak, że w Internecie zamiast cracków są umieszczane programy *upgrade patch* pochodzące wprost od producenta programu, które zostały dostarczone przez jednego z legalnych użytkowników programu albo wykradzione z serwera firmy. W tym wypadku plikiem kluczowym jest wygenerowany przez producenta plik, w którym zawarte są w postaci zaszyfrowanej informacje dotyczące użytkownika, który dokonał opłaty rejestracyjnej. Ponieważ jest to zwykle mały plik wielkości kilku kilobajtów, jest przesyłany pocztą elektroniczną lub — coraz rzadziej — na dyskietkach pocztą tradycyjną. Proponuje się w tym przypadku dwa rozwiązania. Pierwsze polega na tym, że cracker musi zmodyfikować kod programu tak, aby ignorował on nieobecność pliku kluczowego, a mimo to zachowywał się w taki sposób, jak gdyby on istniał i upoważniał do korzystania ze wszystkich funkcji programu przez czas nieokreślony. Drugim, bardziej eleganckim, chociaż trudniejszym rozwiązaniem jest wygenerowanie *key file (*najczęściej z danymi zawierającymi jako nazwę użytkownika pseudonim crackera). Wystarczy wówczas skopiować taki plik do katalogu łamanego programu i ten uzna, iż został poprawnie zarejestrowany.

Na rysunku przedstawiony został ekran powitalny słynnego programu grupy Phrozen Crew-Oscar.



Numery seryjne dla systemu operacyjnego Windows 2000 Professional w programie Oscar Y2k przedstawiają się tak, jak to widać na rysunku.

Zupełnie inną kategorią cracków, są te, które usuwają zabezpieczenia z gier i innych programów dostarczanych na płytach CD. Wymagają one często tego, by podczas ich działania krążek CD był uruchomiony. W tym wypadku cracker usuwa zabezpieczenia sprawdzające, czy nośnik, z którego odczytywane są poszczególne informacje, jest płytą CD. Oczywiście wszystkie dane muszą być wcześniej skopiowane na dysk twardy. Czasem wystarczy jednak zainstalować program emulujący stację CD-ROM w konkretnym katalogu dzięki czemu program zachowuje się dokładnie tak, jak gdyby był uruchamiany z prawdziwej płyty CD.

Ale zdarzyć się może (np. w przypadku gier), że dane programu zajmują całą płytę (650 MB), co sprawia, że taki program, z którego tylko usunięto sprawdzanie na obecność płyty i tak będzie zbyt duży, by go rozpowszechniać. Wtedy cracker musi usunąć nadmiar danych z płyty (np. filmy, animacje itp.) występujących pomiędzy poszczególnymi elementami gry. W ten sposób można zmniejszyć objętość programu do kilkudziesięciu lub kilkunastu megabajtów.

W przypadku programów innych niż gry wycina się zwykle wszystkie dodatki, takie jak zbiory rysunków, dodatkowe biblioteki, programy w wersjach próbnych, programy pomocnicze itp. Tutaj najbardziej widoczna staje się różnica pomiędzy złamanym programem, a jego pełną wersją — użytkownik otrzymuje esencję produktu, jednak nie ma możliwości skorzystania ze wszystkich dodatkowych elementów współtworzących klimat gry lub środowisko pracy programu. Jeżeli jednak ktoś dysponuje internetowym łączem stałym taka alternatywa może być wystarczająco kusząca.

Ograniczenia w programach typu trial są równie interesujące. Producenci zwykle nie wyposażają tych programów we wszystkie funkcje oferowane w pełnej wersji produktu, więc nie wystarczy pominąć zabezpieczeń, by rozszerzyć możliwości programu. Dodatkowo wersje demo programów działają tylko przez określony okres czasu (najczęściej 30 dni). Crackerzy w zależności od chęci i środków dostarczają użytkownikowi dwa rozwiązania — albo usuwają jedynie ograniczenie czasowe pozwalając cieszyć się złamanym produktem przez czas nieokreślony, albo dostarczają kompletny upgrade patch, który zawiera różniące się elementy plików w wersji trial oraz wersji pełnej i modyfikuje istotną część programu tak, aby zamienić go w wersję kompletną. O ile w pierwszym przypadku cracki nadal są małych rozmiarów, o tyle w drugim są to już aplikacje osiągające rozmiary kilkuset kilobajtów.

Łamanie programu

Do najbardziej rozpowszechnionych i najbardziej cenionych przez crackerów narzędzi służących do podglądania kodu łamanego programu należą: SoftIce firmy Numega Technologies Inc. (*http://www.numega.com*) oraz W32Dasm firmy URSoftware Co. Pierwszy z nich działa na zasadzie debuggera i umożliwia ustawienie tzw. punktów krytycznych lub pułapek (*breakpoints*). Są to określone wywołania funkcji, procedur lub odwołania do pamięci, przerwań itp., które są przechwytywane przez SoftIce sprawiają, że kontrola systemu jest przekazywana programowi. Wyświetla on bieżący kod wykonywany przez dany program, stan wszystkich rejestrów procesora, obszar pamięci (począwszy od zadanego adresu), pozwalając tym samym skutecznie śledzić działanie programu na wszystkich jego etapach. Jako że programy napisane dla systemu operacyjnego Windows komunikują się z użytkownikiem poprzez system operacyjny, to (znając nazwy standardowych funkcji) można ustawić „pułapkę" dla konkretnej funkcji i przejąć kontrolę nad sposobem jej wykonywania.

Można to zaobserwować dowolnym na przykładzie. Załóżmy, że do pobierania wprowadzonych przez użytkownika znaków w oknach dialogowych służą następujące standardowe funkcje: *GetWindowText, GetWindowTextA, GetWindowTextW, GetDlgItemText, GetDlgItemTextA, GetDlgItemTextW*. SoftIce przejmując kontrolę nad systemem przełącza ekran w tryb znakowy, więc nie widać na bieżąco debugowanego programu. Drugi program — W32Dasm — jest bowiem nie tylko debuggerem, ale i deasemblerem i umożliwia śledzenie rezultatów wykonywanego programu podobnie jak SoftIce. W odróżnieniu od niego pracuje jednak w trybie okienkowym, co znacznie ułatwia pracę.

Mimo że działania crackerów są imponujące, nie można zbyt łatwo ulegać fantazjom. Tylko w niewielkim stopniu crackowanie jest sztuką samą w sobie. Nie wielu crackerów może poszczycić się nieprzeciętną inteligencją. Ale właśnie ich wiedza i umiejętności mogą świadczyć o tym, że cracker nie zawsze ponosi odpowiedzialność za całą złą reputację hakerów. Podsumowując należy zatem stwierdzić, że cracker to osoba, która:

- Bardzo dobrze posługuje się komputerem;
- Zna asemblera;

- Potrafi zmieniać kod programu, znajdować odpowiednie hasła itp.;
- Zna się na kryptografii;
- Usuwa zabezpieczenia z programów;
- Zajmuje się analizowaniem zdesemblowanego kodu programu w celu znalezienia numeru seryjnego programu lub pozbycia się tzw. „nag screena";
- Nie orientuje się w zasadach organizujących pracę w Sieci, więc nie wykorzystuje luk w systemach komputerowych;
- Odnajduje błędy w programach, znajduje luki i dokładnie zna algorytm generujący seriala;
- Samodzielnie tworzy nowe sposoby zabezpieczeń programów;
- Łamiąc programy poznaje zasady działania systemu, zależności między jego elementami i uczy się lepiej pisać własne programy.

Prawo polskie a cracking

Cały świat byłby jednak zbyt piękny, gdyby używanie cracków do rejestracji programów było całkowicie legalne. Na nieszczęście crackerów (ale na szczęście dla autorów programów) obecnie obowiązujące przepisy prawa polskiego regulują stosunki miedzy twórcami i odbiorcami programów komputerowych. I tak ustawa z dnia 4 lutego 1994 roku („O prawie autorskim i prawach pokrewnych") w rozdziale siódmym zawiera część zatytułowaną — „Przepisy szczególne dotyczące programów komputerowych". Najbardziej istotne są dwa ustępy. Art. 74, pkt 4 mówi:

„Autorskie prawa majątkowe do programu komputerowego (...) obejmują prawo do: (...) tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym z zachowaniem praw osoby, która tych zmian dokonała".

W art. 75, pkt 1 czytamy:

„Jeżeli umowa nie stanowi inaczej, czynności wymienione w art. 74 ust. 4 pkt 1. i 2. nie wymagają zgody uprawnionego, jeżeli są niezbędne do korzystania z programu komputerowego zgodnie z jego przeznaczeniem, w tym do poprawiania błędów przez osobę, która legalnie weszła w jego posiadanie".

Najlepszym komentarzem do wymienionych aktów będzie fragment książki *Prawno-autorska i patentowa ochrona programów komputerowych*:

„Czynności polegające na tłumaczeniu, przystosowywaniu, zmianie układu lub jakichkolwiek innych zmianach w programie są objęte zakresem wyłączności podmiotu uprawnionego. Inaczej niż w stosunku do pozostałych utworów, samo podjęcie takich czynności — bez zgody uprawnionego stanowi naruszenie prawa, chyba że mieści się w granicach zezwolenia zawartego w art.75 pkt 1 ustawy".

Zatem deasemblacja lub debugowanie programu objętego prawem autorskim jest prawnie zabronione. Z drugiej strony jednak, ustawodawcy brali pod uwagę zalecenia specjalnej grupy ekspertów Rady Europy, która w latach 1985-89 zajmowała się prawnymi aspektami przestępstw komputerowych. Ich raport klasyfikuje przestępstwa z wykorzystaniem komputera na dwie kategorie: główną — zawierającą czyny wymagające, zdaniem Komitetu Ekspertów, kryminalizacji we wszystkich krajach członkowskich, oraz fakultatywną — zawierającą typy nadużyć komputerowych, o mniejszym na ogół stopniu szkodliwości i implikacjach międzynarodowych w zakresie ich ścigania i jurysdykcji. Listy te prezentują się następująco:

Lista minimalna:

1. Oszustwo związane z wykorzystaniem komputera;
2. Fałszerstwo komputerowe;
3. Zniszczenie danych lub programów komputerowych;
4. Sabotaż komputerowy;
5. „Wejście" do systemu komputerowego przez osobę nieuprawnioną;
6. „Podsłuch" komputerowy;
7. Bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych;
8. Bezprawne kopiowanie topografii półprzewodników.

Lista fakultatywna:

1. Modyfikacja danych lub programów komputerowych;
2. Szpiegostwo komputerowe;
3. Używanie komputera bez zezwolenia;
4. Używanie prawnie chronionego programu komputerowego bez upoważnienia.

Crackowanie zaliczyć można zatem do drugiej grupy, w której wyliczone zostały przestępstwa o mniejszym znaczeniu. Komitet Ekspertów tak je definiuje:

„Modyfikacja danych lub programów komputerowych — jest to czyn polega na nieuprawnionej ingerencji w treść danych poprzez dopisanie nowych danych lub zmianę istniejącego zapisu.

Używanie prawnie chronionego programu komputerowego bez upoważnienia — jest postępowaniem równie nagannym jak paserstwo. Nie tylko więc nielegalne kopiowanie programów komputerowych, ale i używanie takich programów powinno być traktowane jako naruszenie praw autorskich i podlegać ochronie prawnokarnej. Warunkiem karalności powinno być działanie w celu osiągnięcia korzyści majątkowej lub spowodowanie szkody osobie uprawnionej (autorowi)".

Można zatem stwierdzić, że zarówno sam proces crackowania danego programu komputerowego, jak i używanie takiego programu jest złamaniem prawa. Kodeks Karny z dnia 6 czerwca 1997 roku w art. 268 reguluje karalność tego typu czynów stosowanymi artykułami.

Art. 268.

„§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego”.

Warunki Temidy są zatem jasne — jeśli ktoś użyje cracka w celu zmienienia programu podlega karze pozbawienia wolności do lat trzech.

Według statystyk Business Software Alliance (*http://www.bsa.org*) udział pirackich programów komputerowych w stosunku do całego rynku oprogramowania danego państwa w Polsce wynosił 61%. Dla porównania współczynnik ten w Rosji kształtował się na poziomie 89%, zaś w USA — 27% . Zatem można stwierdzić, iż jesteśmy dopiero na początku drogi, na końcu której nie ma już piractwa, ale daleko od miejsca, w którym wszystkie programy są pirackie. Świadczy to o pewnym trendzie — najpierw następuje gwałtowny wybuch zainteresowania rynkiem komputerowym i wówczas prawie wszystkie nabywane programy pochodzą z nielegalnych źródeł, stopniowo rynek ulega nasyceniu, a nabywcy coraz częściej skłaniają się w kierunku legalnych źródeł oprogramowania.

Na początku jednak wyraźnie istnieje potrzeba pirackiego software’a, gdyż jest on jednym z warunków szybkiego rozwoju rynku. Należy więc życzyć polskiemu rynkowi oprogramowania, by jak najszybciej osiągnął stadium dojrzałości. Zanim to nastąpi nie powinno się hamować jego rozwoju. Niektóre wyszukiwarki internetowe umożliwiają podgląd statystyk dotyczących najczęściej zadawanych im pytań. Jak można się spodziewać, pytanie „crack” zawsze pojawia się w pierwszej dziesiątce zaraz obok haseł „sex”, „porno” czy „hak”. Dziwi więc fakt, iż opracowania, artykuły w fachowych czasopismach, jak i wiadomości w zwykłych dziennikach dotyczące przestępstw komputerowych skupiają się zwykle na hakingu, nie wspominając w ogóle o sprawie ogólnie znanej i interesującej szerokie grono użytkowników komputerów, jakim jest cracking.

Phreaking

Nowoczesna kultura w dużym stopniu zależna jest od telefonów. Należą one do naszej codzienności. Różne telefoniczne spółki, które ustalają zasady rynkowe, mają więc potęgę, siłę oraz wielki wpływ na nasze życie. W tym właśnie tkwi wielkie bogactwo i wartość ludzi, którzy potrafią manipulować systemami telefonicznymi. Phreaking jest rozmyślnym wykorzystywaniem telefonicznej technologii na szkodę spółek telefonicznych. W praktyce dość często jest stosowany przez hakerów, ponieważ w przeciwieństwie do innych sposobów i metod zabawa z telefonami niszczy złudzenie prywatności ludzkiej. Jakkolwiek jest to szeroko praktykowana i bardzo intrygująca dla kogoś, kto za pracę w Sieci musi pokrywać wysokie rachunki telefoniczne.

Phreakerzy to prekursorzy włamywaczy komputerowych. Ich historia zaczęła się wraz z początkiem lat pięćdziesiątych, kiedy w USA wprowadzono bezpośrednie połączenia międzynarodowe. Umiejętność darmowego łączenia się z dowolnym miejscem na świecie należała do dobrego stylu. Dla przykładu: londyńskie biuro Transworld Airlines zostało zmuszone do usprawnienia wolnej od opłat linii telefonicznej, gdyż w momencie, gdy nagrana na taśmie informacja z dowolnym komunikatem kończyła się i w słuchawce pojawiał się sygnał, phreaker włączał się wybierając zamiejscowy numer kodowy i dzwonił po całym świecie, zostawiając opłatę liniom telefonicznym. Dopiero specjalna blokada założona przez British Telecom ukróciła ten proceder.

Łamanie zabezpieczeń telefonicznych w Wielkiej Brytanii nie było tak masowym zjawiskiem jak w USA, gdzie w latach siedemdziesiątych samozwańcza Młodzieżowa Partia Międzynarodowych Połączeń (YIPL) postawiła sobie za cel zredukowanie dochodów AT&T Bell Corporation, która wówczas była potężną firmą. Aktywiści YIPL głosili, że jest to faszystowska i kapitalistyczna organizacja, której wpływy należy zablokować.

„YIPL jest niekomercyjnym stowarzyszeniem propagującym technologie służące ludzkości; chcemy pokazać wam, jak walczyć z komputerami, które opanowują nasze życie" — czytamy w magazynie organizacji, w którym „porady dla czytelników" obejmowały najskuteczniejsze sposoby użytkowania darmowych połączeń i schematy urządzeń ułatwiających je (zwane niebieskimi, czerwonymi lub czarnymi skrzynkami). Były to generatory dźwięków, które podłączone do linii telefonicznej wytwarzały sygnały o odpowiednich częstotliwościach. Niektóre z rad YIPL były mniej konwencjonalne i w jednym z wydań można było znaleźć na przykład informacje o podkładkach z brązu, które pasują do automatów telefonicznych.

W niektórych sklepach odmawiano nawet sprzedaży tego rodzaju podkładek. W tym samym roku YIPL rozpoczęła kampanię „Poparcie dla Cap'n Cruncha", legendarnego phreakera, który został aresztowany w 1971 roku za nielegalne używanie systemu telekomunikacyjnego. Proszono o pomoc czytelników.

Cap'n Crunch (John Draper) stał się sławny — o czym wspomniałem już wcześniej — dzięki umiejętności gwizdania na opakowaniu pieczywa Cap'n Crunch. Potrafił on wydawać dźwięk o częstotliwości 2600 herców pozwalający na uzyskanie darmowego połączenia.

Na początku lat siedemdziesiątych Draper pomógł Steve'owi Job i Steve'owi Wozniakowi, późniejszym twórcom komputera Apple, w zaprojektowaniu niebieskiej skrzynki. Był świetny, więc pomimo swej przeszłości jest obecnie cenionym konsultantem komputerowym i objeżdża świat opowiadając o przygodach z przeszłości.

Phreakerzy (tak siebie nazywają również polscy „piraci telefoniczni") używają rozmaitych metod. Na początku korzystali oni z *wybieraczy* (specjalnych urządzeń służących do wybierania numeru) zwanych *czerwonymi boxami*. Były to dostępne w sklepie, trzymane w dłoni wybieracze tonowe (*tone dialer*) cyfrowo generujące dźwięki. Phreakerzy przebudowywali je, zamieniając wbudowany kryształ na inny, dostępny w każdym sklepie elektronicznym. Wymiana trwała około pięciu minut.

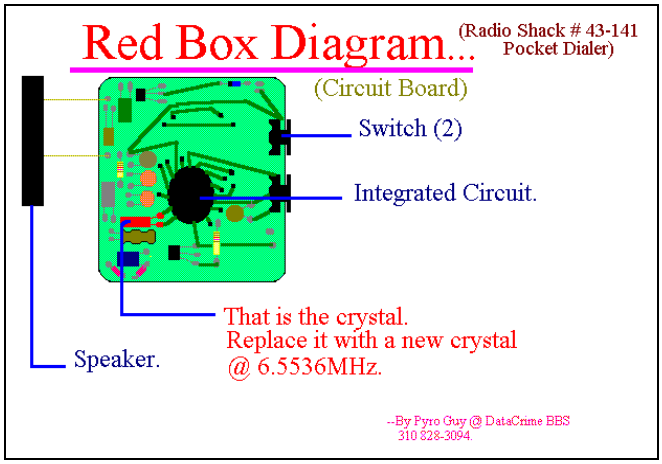
Po takiej przebudowie można już było symulować dźwięk ćwierćdolarówek wrzucanych do automatu. Pozostałe czynności były proste. Phreaker wykręcał numer. Kiedy automat prosił o zapłatę, ten symulował aparatem dźwięk wrzucanych monet i rozmowa nic nie kosztowała.

Dokładne instrukcje wykonania takich urządzeń dostępne są na setkach stron internetowych. Używanie ich stało się tak powszechne, że po pewnym czasie samo posiadanie przebudowanego wybieracza tonowego stało się podstawą do rewizji, zatrzymania i aresztowania. Z czasem konstruowano coraz bardziej zaawansowane urządzenia. Określenie „phreaking" zostało zastąpione terminem „boxing". Wkrótce dostępnych było ponad 40 rozmaitych boxów. Opis niektórych z nich znajduje się w poniższej tabeli.

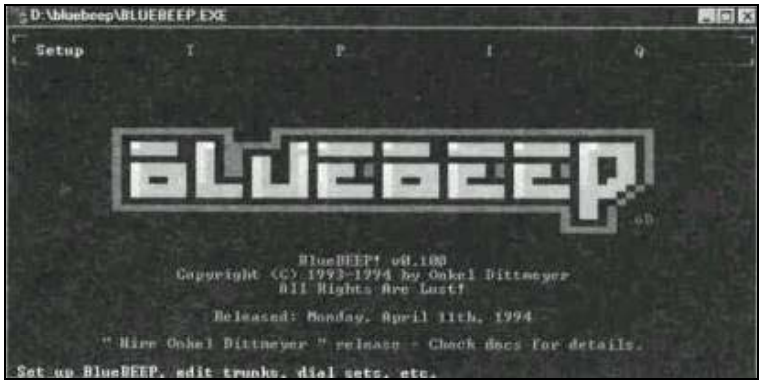
BOX	**Zastosowanie**
Blue Box	Przy tonie 2600Hz pozwala na prowadzenie rozmów międzymiastowych (Pudełko stało się bardzo popularne wśród studentów uczelni amerykańskich o profilu technicznym. Wtedy właśnie Steve Wozniak i Steve Jobs wykonywali i sprzedawali niebieskie pudełka w okresie swoich studiów. Szczęśliwie od tego momentu ci dwaj słynni już dzisiaj panowie, poszli naprzód w stronę bardziej szanowanych eksperymentów przemysłu komputerowego. Niebieskie pudełko pozwalało użytkownikowi za darmo telefonować w każde kuli ziemskiej z doolnego telefonu znajdującego się w USA. Używało ono systemu tonów do oszukiwania telefonicznych systemów. Wydawało z siebie odpowiednie tony DTMF, które były takie same jak tony, które są używane, kiedy wybieramy numer w normalnym telefonie. To właśnie ten ton faktycznie pozwalał użytkownikowi wykonać telefon wolny od opłat. Używanie „niebieskiego pudełka" było czynnością względnie prostą)
Dayglo Box	Pozwala na korzystanie z linii telefonicznej sąsiada
Aqua Box	Pozwala na „oszukiwanie" podsłuchów FBI poprzez dostarczenie do linii telefonicznej prądu o wysokim natężeniu
Mauve Box	Służy do podsłuchu linii telefonicznej
Chrome Box	Służy do kontroli sygnałów pojawiających się w liniach telefonicznych
Red Box	Podrabia sekwencje sygnałów pulsowych, która powiadamia centralę, że włożona została moneta do automatu

BOX	Zastosowanie
Back Box	Zmienia napięcie na liniach w starych centralach
Neon Box	Pozwala podłączyć telefon do zewnętrznych źródeł audio
Brown Box	Jest to ciekawe i łatwe do wykonania urządzenie. Potrzebne są jedynie dwie linie, by zrobić sobie „party line" na trzy telefony. Jedyny problem, na który można się natknąć dzwoniąc przez brązową skrzynkę, to kiepska jakość rozmowy
Green Box	Generuje tony Coin Collect oraz Coin Return

poniżej przedstawiony został schemat budowy „czerwonego pudełka".



W pewnym momencie phreakerom zaczęli pomagać także programiści, w wyniku czego powstało wiele potężnych narzędzi programowych, np. BlueBEEP, którego ekran powitalny przedstawiony został poniżej.



BlueBEEP przypomina wiele aplikacji komercyjnych i działa równie dobrze jak one. Pracuje w środowisku DOS lub w oknie DOS-owym w systemie operacyjnym Windows 95 lub NT.

Jest — jak na razie — najlepiej zaprogramowanym narzędziem phreakerów. Powstał w językach Pascal i Asembler, zawiera funkcje kontroli linii międzymiastowych, generowania sygnałów wybierania (red box i inne), skanowania central telefonicznych itd. Został jednak stworzony zbyt późno.

Aby przyjrzeć się, w jaki sposób phreaking doprowadził do włamań do Internetu, należy cofnąć się o kilka lat.

Phreakerzy robili wtedy, co mogli, by „rozgryźć" nowe systemy telekomunikacyjne. Niejednokrotnie przeszukiwali dziesiątki linii telefonicznych nasłuchując interesujących sygnałów bądź wyszukując ciekawych połączeń. Część z tych, które udało im się znaleźć, dopływała z modemów.

Nikt nie wie, kiedy phreaker po raz pierwszy zalogował się do Internetu. Prawdopodobnie było to bardziej przez przypadek niż dzięki umiejętnościom. Nie korzystano wtedy z bezpośredniego połączenia modemowego PPP, więc trudno by było określić, w jaki dokładnie sposób uzyskano dostęp. Prawdopodobnie ktoś podłączył się przez linię telefoniczną do komputera typu mainframe albo do którejś stacji roboczej. Maszyna ta połączona była z Internetem poprzez Ethernet, inny modem albo inny port. Spełniała jedynie rolę pomostu pomiędzy phreakerem a Internetem. Po jego przekroczeniu phreaker wkraczał do świata komputerów, z których większość była niedostatecznie zabezpieczona. Od tego czasu zaczęli włamywać się do wszelkich możliwych systemów.

Carding

Wraz ze stopniowym upowszechnieniem handlu on-line, płatności kartami kredytowymi i jednoczesnym brakiem uniwersalnej i skutecznej metody ochrony danych w trakcie ich przesyłania z przeglądarki do serwera rozwinęła się w Sieci sztuka oszukiwania związana z kartami kredytowymi i telefonicznymi.

Polega ona głównie na zdobywaniu prawdziwych danych, ściślej mówiąc numerów kart istniejących, bądź — tworzeniu fałszywych. Istnieją nawet specjalne programy umożliwiające generowanie fałszywych numerów kart, na podstawie różnych formuł charakterystycznych dla poszczególnych organizacji kart płatniczych (Visa, Mastercard, American Express). Najistotniejszą bowiem informacją w cardingu jest sam numer karty, nie zaś dane jej właściciela czy termin jej ważności. Dlatego numery te są na wagę złota. Dlatego tak głośny był przypadek Carlosa Felipe Salgado, który w maju ubiegłego roku włamał się do komputera jednego z providerów w San Diego kradnąc numery ponad 100 000 kart kredytowych z zamiarem ich sprzedaży on-line (bowiem istnieje mnóstwo stron, na których numery takie można kupić lub wręcz spisać sobie za darmo!). Zamiar ten uniemożliwiła mu FBI. Straty spowodowane przez carding w samych tylko Stanach Zjednoczonych oceniane są na około miliard dolarów rocznie. W Polsce carding ze zrozumiałych powodów nie był długo popularny, choć ostatnio coraz częściej można usłyszeć o aresztowaniach młodych ludzi za korzystanie z cudzych kont bankowych.

Zdobywanie karty

Jest kilka możliwości i sposobów na zdobycie karty lub odczytanie z niej danych potrzebnych do zawarcia transakcji. Niektóre z nich są całkowicie dla cardera bezpieczne, inne zaś narażają go na duże niebezpieczeństwo. Oto kilka z tych metod:

- *Na chama* — metoda podpatrzona u „dresiarzy", którzy w ten sposób zdobywają komórki. Polega na tym, że pseudocarder podchodzi do ofiary stojącej przy bankomacie, ciosem w głowę ogłusza go i zabiera kartę. Sposób bardzo prostacki i ryzykowny. Czasami carderzy zlecają jego wykonanie komuś innemu.
- *Trash diving* — metoda stosowana przez carderów z USA. Gdy mnóstwo ludzi płaci kartami, obsługa sklepów, restauracji i barów zazwyczaj pod koniec tygodnia lub miesiąca wyrzuca do śmieci kwitki z numerami kart. Wystarczy wtedy „ponurkować" w śmieciach i można coś znaleźć.
- *Generator* — powszechnie znane są generatory numerów kart, takie jak Credit Master lub Credit Wizard (do pobrania z *http://kwantam.home.ml.org*), które działają w oparciu o dostępne algorytmy służące do generowania numerów kart.
- *Supplier* — czyli dostawca. Jest to zaufany człowiek, który może sprzedać całą gamę ciekawych produktów (dowody osobiste, legitymacje szkolne, karty lub ich numery). Metoda trudna do wykorzystania, bo nie łatwo jest znaleźć odpowiedniego „dostawcę".
- *Na szpiega* — podsłuchiwanie i wykorzystywanie ujawnionych przez przypadek informacji.
- *Na telefon* — metoda, która wykorzystuje ludzką naiwność. By ją zastosować, wystarczy jedynie wiedzieć, w jakim banku klient ma rachunek i zadzwonić przedstawiając się za przedstawiciela tego banku. Rozmowa powinna przebiegać mniej więcej według poniższego schematu:

  CARDER: Dzień dobry, czy rozmawiam z panem Piotrem Janowskim?

  PJ: Tak, to ja.

  CARDER: Moje nazwisko Halina Dzięcioł, dzwonię z Banku Śląskiego.

  PJ: Tak? A co się stało?

  CARDER: Limit pana karty został zmniejszony do 100 zł.

  PJ: Ależ to niemożliwe! Mój limit wynosi 3000 zł.

  CARDER: Hmm, być może zaszła jakaś pomyłka w komputerze. Czy mogę prosić o podanie numeru karty oraz datę jej?

  PJ: Tak, oczywiście, ten numer to XXXX — XXXX — XXXX — XXXX, a exp.data to XX/XX.

  CARDER: Dziękuję, postaramy się sprawę szybko wyjaśnić. Do widzenia.

  PJ: Do widzenia.

  Po tej miłej i przyjemnej konwersacji carder ma wszystko, co jest mu potrzebne do dokonania atrakcyjnych zakupów.

Sprawdzenie działania karty

Najczęściej carder sprawdza, czy karta działa właściwie wchodząc na jakąś stronę WWW, gdzie można wykupić abonament na oglądanie zdjęć pornograficznych. Większość tych stron ma bezpośrednie połączenie on-line z Centrum Autoryzacji i od razu carder może dowiedzieć się, czy karta jest aktualna.

Czas

Skradzioną kartą (czy jej numerami) nie należy posługiwać się przez pół roku. Zależy to jednak od celu, do jakiego karta ma być przeznaczona. Jeśli carder będzie na przykład kupował w sklepach z „żelazkami" (i to poniżej limitu punktu), przy założeniu, że kartę znalazł (lub ukradł) między 1 a 25 dniem danego miesiąca, to pocieszy się nią tylko do 1 następnego miesiąca, bo wtedy właśnie sprzedawcy dostaną nową stop-listę z jej numerem (więc w najlepszym wypadku 6 dni). Jeżeli natomiast kartę znalazł (lub ukradł) po 25, to może jej używać do końca następnego miesiąca, bo dopiero wtedy ukaże się ona na nowej stop-liście (czyli ma przed sobą ponad miesiąc). Gdy jednak w sklepie jest terminal elektroniczny, to praktycznie Polcard umieszcza kartę w bazie skradzionych w ciągu 24 godzin. Carderowi pozostaje więc możliwość wykorzystania jej przez Internet.

Zakupy

Metoda zakupów prowadzonych z wykorzystaniem karty jest przeznaczona tylko dla prawdziwych carderów, którzy panują nad swoimi nerwami. Carder musi iść do sklepu, wybrać towar, a następnie podejść do kasy i zrealizować płatność. Najczęściej wybiera się on na zakupy do innego miasta, oddalonego od jego miejscowości. Dobrze jest również wybrać sklep, w którym przewija się mnóstwo klientów (np. hipermarket).

A później już z górki... Carder wybiera towar, podchodzi do kasy, sprzedawca pyta o rodzaj płatności, carder odpowiada, że zapłaci kartą... Sprzedawca bierze plastik i wszystko zależy od tego, jakie urządzenie posiada sklep: „żelazko" czy terminal POS.

„Żelazko"

Każdy sklep ma określony indywidualny tzw. limit punktu. Jest to maksymalna kwota, za jaką klient może zakupić towar bez potrzeby telefonicznej autoryzacji karty. Limit ten ustala Polcard i jest on tajemnicą sklepu. Jeśli carder przekroczył ten limit, to sprzedawca powinien zadzwonić do Centrum Autoryzacji. Jedna gdy udało się carderowi zmieścić w limicie, to sprzedawca wyciąga „stop listę" wydawaną przez Polcard pierwszego każdego miesiąca (są tam numery wszystkich skradzionych kart oprócz American Express) i sprawdza kartę. Jeżeli jest trefna, to do obowiązków sprzedawcy należy zatrzymanie jej i powiadomienie Polcardu. Powinien on także zatrzymać cardera. Ale nie może zrobić tego od razu, gdyż lepiej jest trochę pooszukiwać, by przedłużać rozmowę. Jeśli carder zauważy, co się dzieje, z reguły stara się uciec.

Gdy jednak karta nie figuruje na „stop-liście", sprzedawca kładzie ją na tzw. „żelazko" i przejeżdża po niej (odbija się wtedy na rachunku), a następnie prosi o podpis potwierdzający płatność. I tu pojawia się kolejny problem. Oryginalny podpis jest z tyłu karty. Jeśli carder nie nauczy się go podrabiać, może zastosować pewien wybieg. Wystarczy wziąć wacik do czyszczenia uszu, spirytus 95 % i delikatnie zetrzeć oryginalny podpis. Potem należy całość przemyć wodą, wysuszyć i cienkopisem nanieść dowolny podpis (oczywiście najlepiej zgodny z nazwiskiem, bo takich podpisów wymagają w banku podczas wyrabiania karty). W tym układzie złożenie autografu w sklepie nie jest niczym trudnym. Później sprzedawca powinien porównać podpis z tym, który jest na odwrocie karty i — jeśli wszystko będzie do siebie pasowało — wydać rachunek potwierdzający zakup i konkretny już towar.

Terminal POS

W tym przypadku sprzedawca bierze kartę cardera i przejeżdża po niej elektronicznym terminalem autoryzującym płatność. Od razu wtedy widać, czy karta ma autoryzację czy nie (np. zgłoszona została kradzież lub po prostu przekroczony został limit kredytowy). W przypadku braku autoryzacji z powodu zgłoszenia kradzieży powinien zgłosić to i zatrzymać cardera. Jeśli transakcja nie będzie autoryzowana przez wyczerpanie limitu kredytowego, sprzedawca powinien poprosić o inną kartę lub zapłatę gotówką. Carder może wtedy zrezygnować z zakupów nie wzbudzając podejrzeń. Gdy jednak karta uzyska autoryzację centrum, sprzedawca powinien wydać wydrukowany paragon i towar.

Czasami stosuje też pewien trick uwiarygodniający. Otóż po dokonaniu zakupu można zawrócić i jeszcze raz podejść do kasy, by kupić jakąś drobnostkę (np. paczkę dyskietek w sklepie komputerowym), ale tym razem za własna gotówkę, tłumacząc — „zapomniałem jeszcze tego kupić, ale już nie będziemy się bawili z kartą, zapłacę gotówką". Nawet gdy sprzedawca będą później przesłuchiwany przez specjalistów z Polcardu, nie przypomni sobie cardera, który wyglądał jak normalny klient.

Generalnie jest to metoda mocno ryzykowna, chyba, że carder ma znajomego w sklepie z interesującym go towarem i umówi się z nim do spółki. Przychodzi wtedy jak jest mało ludzi i robi, co trzeba. Oczywiście jak ma elektroniczny terminal i nie uzyska autoryzacji, to nic nie może zrobić, bo mu Polcard nie wypłaci pieniędzy i będzie na tym stratny. Gdy jednak ma „ żelazko", to transakcja ma duże szanse. Carder zabiera towar, idzie do domu. Odpala koledze działkę, żeby też coś z tego miał, w końcu on też trochę ryzykuje. Zawsze jednak carder ma opracowany plan B. Jest taka możliwość, że w sklepie zjawią się panowie wynajęci przez Polcard lub Policja. Stanie się tak, jeśli carder będzie miał duży debet (np. 5 000 zł). Dlatego carder ma zawsze przygotowaną dobrą historyjkę dla sprzedawcy czy pracowników Polcardu. W ten sposób zyskuje on na czasie.

Jeśli karta płatnicza lub zachowanie klienta wzbudza jakiekolwiek podejrzenia, sprzedawca musi zadzwonić do Centrum Autoryzacji Polcardu i podać hasło „KOD 10". Carder wie, że oznacza ono niebezpieczeństwo i brak możliwości jawnego przekazywania informacji. Pracownik Polcardu będzie wówczas zadawał pytania tak sformułowane, by odpowiedź na nie brzmiała TAK lub NIE. Więc, jeśli usłyszy, że sprzedawca gdzieś dzwoni i mówi „KOD 10", a potem ciągle tak lub nie, to zostawia wszystko i znika jak kamfora.

Carding przez telefon

Drugą metodą wykorzystania skradzionej karty przez cardera jest możliwość zrobienia zakupów przez telefon. Carderzy wiedzą, że w godzinach rannych na niektórych programach telewizyjnych reklamowane są TV Shop lub TeleMarkety. To właśnie one padają ich łupem. Niestety sprzedawany jest tam towar wątpliwej jakości, wiec jest to metoda niezbyt zyskowna. Można też kupować przez telefon, ale przede wszystkim carder musi wiedzieć, pod jaki numer dzwonić i co tam sprzedają. Tu przydają się zagraniczne gazety z Empiku. Potrzebna jest dosyć dobra znajomość angielskiego, gdyż należy pamiętać o tym, że sprzedawca w USA będzie podejrzliwy, gdy dowie się, że ktoś z Polski zamawia coś u niego. Ogólnie rzecz biorąc metoda ta jest bardzo kosztowna (chyba, że carder jest przy okazji phreakerem) i dosyć skomplikowana. Jednak zakup taki jest jak najbardziej możliwy i carder wykorzystuje taką sytuację. Jest tu potrzebna „pewna" znajomość social engineering'u. Carder musi przecież zwieść rozmówcę. Zachowuje się spokojnie, wypytuje trochę o produkt... Daje sprzedawcy możliwość na to, aby go zachęcał do zakupu. Po przyjęciu zamówienia paczka jedzie do cardera. Po kilku dniach (w Polsce) lub tygodniach (w USA) dostaje on awizo. Najczęściej załatwia sobie taki adres pocztowy, gdzie można łatwo awizo wyjąć, np. ktoś wyjechał z mieszkania i osoba opiekująca się mieszkaniem wybiera listy raz na tydzień. W odróżnieniu od metody „sklepowej" pojawia się tutaj problem odbioru paczki. Łączy się to z bezpośrednim spotkaniem z kurierem (oni nie są raczej niebezpieczni) lub z osobą na poczcie. I tu jest gorzej. Jeśli paczka przyjdzie na pocztę, to listonosz przynosi do domu kwitek uprawniający do odbioru — jest na nim imię, nazwisko i adres. Na poczcie potrzebny jest więc jakiś dokument do pokazania... Oczywiście carder nigdy nie zamawia na własne nazwisko, więc potrzebny mu jest fałszywy dokument.

Sprzedaż wysyłkowa

Wiadomym jest, że można płacić kartą kredytową za towary z katalogów firm wysyłkowych, a jedynym problemem, jaki się pojawi może być kwestia autoryzacji karty.

Sprzedaż przez Internet

Jest to ulubiona forma zakupów wszystkich carderów. Zamówienie jest w 100% elektroniczne, nigdzie nie widać twarzy cardera i nie trzeba się nigdzie podpisywać.

Zawsze może się wyprzeć złożonego zamówienia. Jeśli dodatkowo carder pójdzie do kawiarenki internetowej i stamtąd złoży zamówienie bardzo trudno mu będzie udowodnić winę.

W dzisiejszych czasach przez Internet można kupić właściwie wszystko — dobra fizyczne (hardware, itp.), lecz również usługi (np. konto poczty elektronicznej lub hasło na stronie WWW). Firma GoldenHawk sprzedaje na swojej stronie świetny program do nagrywania płyt. Możliwości są praktycznie nieskończone i zależy to

tylko i wyłącznie od inwencji twórczej cardera. Jeśli zamówi coś niematerialnego, jak np. e-mail albo software odpada kwestia odbioru. Po prostu dostaje konto na serwerze albo ściąga software. Przy zamawianiu towaru odbiór wygląda tak samo jak przy zamówieniu telefonicznym. Dostaje awizo, idzie na pocztę i odbiera.

W tej profesji ryzyko jest dosyć duże. Carder wie, że musi być sprytniejszy od sprzedawcy, musi wyprzedzać go zawsze, co najmniej o dwa posunięcia.

Zabezpieczenia

To jest bardzo ważny element działalności cardera. Jeśli zamawia przez Internet to najczęściej używa DialUp-ów powszechnego dostępu (np. TPsa) lub idzie do kawiarenki internetowej, gdzie jest całkowicie anonimowy. Jeśli zamawia przez telefon to tylko z budki telefonicznej. Najczęściej nie zamawia bezpośrednio na swoje nazwisko, ale na matkę, ojca, kolegę czy miejsce pracy lub na fałszywe dokumenty. Nie kupuje w swoim rodzimym kraju. Zabezpiecza go to przed wizytą policji czy właściciela karty kredytowej.

5 przykazań cardera

Carderzy mają kilka złotych zasad, które gwarantują im sukces, anonimowość i bezpieczeństwo. Oto one:

- Bądź ostrożny, nie chwal się każdemu tym, co robisz — im mniej osób wie, im mniej jest to popularne, tym bezpieczniejsze;
- Przy zamawianiu staraj się trochę odwlec zakup, by wyglądać bardziej wiarygodnie;
- Zamówienie wysyłaj zawsze faxem;.
- Nie bądź nachalny nie zamawiaj z jednej firmy zbyt wielu pozycji;
- Używaj tylko pewnych kart.

Wpadka

W razie niespodziewanej wizyty miłych panów, carder ma przygotowaną jakąś dobrą odpowiedź. Często używa kilku ustalonych wcześniej sformułowań:

- „Nic nie wiem. Nie posiadam karty kredytowej ani komputera”.
- „Kolega z IRCa powiedział, że jest bogaty i da mi numer swojej karty w formie prezentu”;
- „To jakiś złośliwiec zrobił sobie kawał. Nic nie wiem”.

Najczęściej carder udaje trochę niezorientowanego i przestraszonego. I na tym się sprawa zamyka. Nic mu nie można zrobić. Jeśli zamówił przez Internet lub z budki towar na cudze nazwisko, awizo przyszło nie jego adres, odebrał towar z fałszywym

dokumentem, to nie ma żadnego dowodu na to, że to on. Dlatego tak ważne jest, aby działania przeprowadzać poza miejscem swojego zamieszkania.

Wirusy komputerowe

Jeszcze do niedawna pojęcie *wirus* kojarzyło się nam wszystkim głównie z epidemią grypy, która prawie każdej zimy daje się we znaki setkom tysięcy ludzi. Niestety, słowo to weszło również do języka komputerowego. Określa się nim groźną „plagę", która szybko się rozprzestrzenia i bardzo dokucza użytkownikom komputerów.

Idea wirusów komputerowych została przedstawiona dużo wcześniej przed pojawieniem się pierwszego komputera osobistego. W roku 1959 L.S. Penrose opublikował w czasopiśmie «Scientific American» artykuł o samo powielających się strukturach mechanicznych. Sposoby ich aktywacji, powielania, mutacji i przechwytywania zostały przedstawione na prostym dwuwymiarowym modelu. Ideę tę zaimplementował później w kodzie maszynowym IBM 650, L.G. Stahl. W tamtych czasach tylko wielkie firmy i instytucje rządowe mogły sobie pozwolić na ogromne, trudne w obsłudze i niewiarygodnie drogie maszyny liczące. Dwudziestego lipca 1977 roku powstał pierwszy (przeznaczony dla prywatnych użytkowników) komputer osobisty Apple II. Rozsądna cena, przyjazny interfejs użytkownika i prostota konstrukcji spowodowały wielką popularność *jabłka*. Łączna ilość sprzedanych egzemplarzy tego komputera osiągnęła trzy miliony, nie licząc wyprodukowanych na całym świecie klonów (takich jak Pravetz 8M/C, Agat itp.). Było to wielokrotnie więcej niż wynosiła sprzedaż komputerów innych firm. Od tej pory miliony ludzi zyskało możliwość pracy z komputerem. Nic więc dziwnego, że w tym momencie pojawiły się także pierwsze prototypy obecnych wirusów komputerowych. Stało się tak, gdyż dwa główne warunki umożliwiające ich tworzenie zostały spełnione: pojawiła się przestrzeń życiowa oraz działalność wirusów mogła mieć groźne konsekwencje. Z upływem czasu znacząco wzrosła liczba komputerów oferowanych dla prywatnych użytkowników. Równocześnie ze sławnymi pięciocalowymi dyskietkami pojawiły się pierwsze dyski twarde; nastąpił szybki rozwój sieci lokalnych, jak również transmisji danych poprzez sieć telefoniczną. Pojawienie się pierwszych banków danych tzw. BBS-ów (*Bulletin Board Systems*) znacznie uprościło wymianę informacji pomiędzy użytkownikami. Niektóre BBS-y przekształciły się później w wielkie serwisy Internetowe (CompuServe, America-On-Line itp.). W tym momencie spełniony został kolejny warunek rozprzestrzeniania się wirusów: czynnik ludzki. Wiele niezależnych osób i gangów hakerskich zaczęło się specjalizować w tworzeniu wirusów.

Lata dziewięćdziesiąte stały się okresem najintensywniejszego rozkwitu wirusów komputerowych. Miliony osób na całym świecie z własnej woli lub z konieczności stało się użytkownikami komputerów. Umiejętność obsługi stała się nieodzownym atutem każdej wykształconej osoby. Rozwój technik przesyłania informacji stworzył idealne warunki dla powstawania wirusów. Na początku wirusy były tworzone w wielkich, coraz to większych ilościach, jednak ich „jakość" pozostawiała wiele do życzenia. W chwili obecnej sprawa przedstawia się odwrotnie, prymitywni prekursorzy są zastępowani nowymi szczepami wirusów posiadającymi zdolność do adaptacji się w nowych warunkach. Dzisiejsze wirusy nie tylko niszczą pliki, MBR,

restartują system czy też odgrywają nieszkodliwe melodie, niektóre z nich mogą nawet zniszczyć informacje zapisane w BIOS na płycie głównej. Sposoby i techniki ich kodowania, powielania i rozprzestrzeniania zadziwiają nawet najbardziej doświadczonych specjalistów w tej dziedzinie.

Jest oczywiste, że technologie tworzenia wirusów będą się udoskonalać wraz z rozwojem technicznym ludzkości. W przyszłości nikt nie będzie mógł powiedzieć, że jest w stu procentach zabezpieczony przed atakami komputerowych bakcyli.

Musimy zdawać sobie sprawę z tego, że wirusy komputerowe stoją na pierwszym miejscu wśród najbardziej destrukcyjnych programów komputerowych. Mogą one powodować nie tylko odmowę obsługi (DoS), ale też niszczyć dane. Co więcej — niektóre wirusy (chociaż jest ich niewiele) mogą zniszczyć system komputerowy.

W obliczu Internetu stanowią szczególne zagrożenie — programy te są bowiem najbardziej niebezpieczne, w chwili, gdy znajdą się w środowisku sieciowym, a żadne środowisko nie pasuje lepiej do tego określenia niż Internet.

Wirus komputerowy

Wirus komputerowy jest programem, który przyłącza się do plików na komputerze, jaki atakuje. Wówczas oryginalny kod wirusa zostaje dopisany do zawartości niektórych plików w systemie. Proces ten nazywamy infekcją. Zainfekowany plik staje się nosicielem i sam może infekować inne pliki. Ten proces nazywamy replikacją. Poprzez proces replikacji wirus rozprzestrzenia się na całym dysku twardym, doprowadzając do infekcji całego systemu. Często oznaki tego procesu są niezauważalne — przynajmniej do czasu zanim nastąpi całościowa infekcja, ale wówczas jest już za późno.

Proces replikacji wirusa komputerowego można porównać do rozprzestrzeniania się wirusów biologicznych. Zarażona jednostka (nosiciel) przemieszcza się i wchodzi w interakcje z innymi jednostkami, które w efekcie zaraża, niekiedy zdarza się, że proces rozprzestrzeni się w postępie geometrycznym i nastąpi epidemia (zakażenie całej populacji czy też — całego systemu komputerowego).

Pliki narażone na infekcję

W ostatnich latach powstały tysiące wirusów komputerowych. Mają one różną budowę i atakują różne typy plików (choć początkowo atakowały z reguły pliki wykonywalne). Gdy plik wykonywalny z doczepionym wirusem zostanie uruchomiony będzie infekować inne pliki, doprowadzając w krótkim czasie do zainfekowania całego systemu. Z racji tego, że otworzenie nawet pojedynczej aplikacji w środowisku Windows powoduje uruchomienie kilku, czy nawet kilkunastu plików wykonywalnych, proces replikacji postępuje lawinowo.

Oprócz wirusów infekujących pliki wykonywalne istnieje mnóstwo wirusów rezydujących w plikach danych. Są to tzw. wirusy makr, infekujące między innymi pliki dokumentów generowanych przez edytor Microsoft Word i arkusz kalkulacyjny Excel. Takie wirusy zazwyczaj atakują globalne szablony dokumentu, ostatecznie uszkadzając każdy otwarty dokument edytora Word lub arkusza kalkulacyjnego Excel.

Trzecią grupą plików, które mogą zostać zainfekowane, są sterowniki urządzeń. Dotyczy to głównie starszych systemów operacyjnych — takich jak kombinacja DOS/Windows 3.11.

Powstawanie wirusów

Twórcami wirusów są przeważnie:

- Młodzi-gniewni;
- Specjaliści do spraw bezpieczeństwa systemów;
- Programiści.

Każda grupa kieruje się innymi pobudkami. Młodzi ludzie piszą wirusy dla zabawy lub rozgłosu. Czasem — dlatego że nie pracują oni jeszcze w przemyśle informatycznym i część z nich uważa, że jeśli stworzą szczególnie błyskotliwego wirusa to ich umiejętności programistyczne zostaną zauważone i docenione.

W przeciwieństwie do nich eksperci do spraw bezpieczeństwa tworzą wirusy na zamówienie (testowanie nowych metod zabezpieczeń danych).

Autorami przeważającej liczby wirusów są programiści-zapaleńcy z krajów Europy Wschodniej. W Internecie możemy znaleźć fascynujący dokument opisujący fenomen rozkwitu grup programistów piszących wirusy komputerowe. Powstały nawet specjalne BBS-y służące wymianie pomysłów, kodów źródłowych i doświadczeń w tej mierze. Opracowanie to**,** zatytułowane „Bułgarskie i rosyjskie fabryki wirusów" (*The Bulgarian and Soviet Virus Factories*) sporządził Vesselin Bontchev — dyrektor Laboratorium Wirusologii Komputerowej przy Bułgarskiej Akademii Nauk w Sofii. Dokument zamieszczony jest pod adresem:

http://www.drsolomon.com/ftp/papers/factory.txt.

Wielu programistów tworzy wirusy z wykorzystaniem środowisk wyższego rzędu lub też pojedynczych aplikacji, specjalnie zaprojektowanych do generowania ich kodu. Takie pakiety programowe są dostępne w Internecie. Oto nazwy kilku z nich:

- Virus Creation Laboratories;
- Virus Factory;
- Virus Creation 2000;
- Virus Construction Set;

- The Windows Virus Engine.

Zestawy te są na ogół łatwe w obsłudze i pozwalają na stworzenie wirusa prawie każdemu zainteresowanemu. (Zupełnie inaczej niż dawniej, gdy potrzebna była do tego spora wiedza programistyczna). Dzięki temu liczba znanych wirusów „na wolności" zwiększa się gwałtownie z każdym niemal dniem.

Elita

Jeśli ktokolwiek spotkał kiedyś wirusa łatwo zauważy, że — jak na program o tak znacznych możliwościach — jest on niewiarygodnie mały. Powodem tego jest fakt, że większość wirusów pisana jest w języku maszynowym. Język maszynowy, zwany również asemblerem, jest językiem niskiego poziomu i w związku z tym programy w nim napisane są objętościowo niewielkie.

Klasyfikacja języków programowania na nisko czy wysoko poziomowe zależy jedynie od stopnia ich pokrewieństwa z językiem maszynowym (język maszynowy składa się z wyrażeń numerycznych, przedstawianych głównie w kodzie zerojedynkowym). W językach wysokiego lub średniego poziomu stosuje się symboliczny zapis komend z zastosowaniem prostych słów zapożyczonych z języka angielskiego i matematyki, tak jak w podstawowej komunikacji międzyludzkiej. Języki programowania Basic, Pascal i C należą do języków średniego poziomu. Za ich pomocą „mówimy" maszynie o znaczeniu poszczególnych funkcji, ich przeznaczeniu i sposobach realizacji zadań. Znajomość programowania w kilku językach jest przywilejem elity hakerskiej.

Działanie

Większość wirusów działa podobnie jak programy rezydentne (TSR). Pozostają one „w gotowości" monitorując aktywność systemu. Jeśli napotkają na działanie spełniające określone dla wirusa kryteria (na przykład uruchamiany plik wykonywalny) „wkraczają" do akcji przyłączając się do aktywnego programu.

Najlepszym sposobem na zademonstrowanie tego procesu jest opisanie działania wirusów głównego modułu rozruchowego (MBR) dysku twardego.

Wirusy głównego modułu rozruchowego (MBR)

Podstawowe procedury, za sprawą których startuje system, są zapisywane w początkowym sektorze dysku, zwanym głównym modułem rozruchowym MBR *(Master Boot Record*). Logicznie blok ten jest umiejscowiony na zerowym cylindrze, zerowej głowicy i pierwszym sektorze nadrzędnego dysku twardego systemu, lub w bloku zerowym (przy stosowaniu adresowania LBA).

Blok MBR przechowuje również kluczowe informacje, odnoszące się do struktury dysku (opisuje logiczną strukturę dysku zwaną tabelą partycji).

W trakcie inicjowania działania systemu są odczytywane i weryfikowane dane zawarte w układzie CMOS. Przykładowo — jeśli domyślny dysk twardy (z którego inicjowane jest działanie systemu operacyjnego) ma rozmiar l GB, a w BIOS-ie wskazano 500 MB, wtedy system nie uruchomi się i pojawi się komunikat o błędzie. Podobnie sprawdzana jest pamięć RAM (pod kątem błędów parzystości). Jeżeli nie zostaną odkryte żadne błędy, rozpocznie się właściwy proces ładowania systemu, który zaczyna się odczytem zawartości bloku MBR. Sytuacja ta zmienia się diametralnie wówczas, gdy główny moduł uruchomieniowy zostaje zainfekowany przez wirusa.

Eksperci z firmy McAfee, wiodącej w sprzedaży oprogramowania antywirusowego, wyjaśniają:

„Wirusy, które infekują główny moduł rozruchowy i sektor ładowania początkowego (MBR/BS) dysku twardego i dyskietek są najbardziej popularne, ponieważ stosunkowo łatwo taki wirus stworzyć. Przejmują kontrolę nad komputerem z bardzo niskiego poziomu, często są „utajnione" (wirusy „stealth"). Osiemdziesiąt procent telefonów do działu pomocy technicznej firmy McAfee dotyczy problemów z tego typu wirusami.

Wirusy głównego modułu rozruchowego działają szczególnie podstępnie, ponieważ atakują dyskietki przy każdym ich użyciu. Stąd wszechobecność tych wirusów, jako że przenoszą się one bardzo łatwo z komputera na komputer — właśnie za pomocą zainfekowanych dyskietek".

Załóżmy, że posiadamy niezainfekowany MBR. Infekcja następuje w momencie uruchamiania systemu z „zainfekowanej" dyskietki. Wtedy kod wirusa ładuje się do pamięci (na ogół nie do obszaru pamięci górnej, gdyż znanych jest zaledwie kilka wirusów, które rezydują w tym obszarze). Wirusy, które można znaleźć w tej części pamięci, to najczęściej te, które dostały się tam wraz z załadowaniem uprzednio zainfekowanego pliku sterownika czy programu rezydentnego.

Po załadowaniu do pamięci, wirus odczytuje informację o partycjach z bloku MBR. Niektóre z programów wirusowych posiadają procedurę sprawdzającą poprzednie infekcje modułu MBR (także te dokonane przez inne wirusy). Zakres tej procedury jest zazwyczaj ograniczony w celu zachowania zasobów pamięci. Wirus, który sprawdzałby dużą ilość innych wirusów, musiałby być większy, a zatem łatwiej wykrywalny, trudniejszy do przenoszenia itd. Jakby na to nie patrzeć, wirus zawsze zastępuje informację zawartą w głównym module rozruchowym przez swoją własną, zmodyfikowaną wersję tego bloku.

Większość wirusów bootsektora zawiera procedurę zachowującą oryginalny MBR w innym miejscu na dysku twardym. Działanie to nie jest bynajmniej miłym gestem ze strony autora wirusa, który przewidział możliwość przywrócenia stanu sprzed infekcji, lecz wynika z konieczności — informacje zawarte w bloku MBR są niezbędne do wystartowania systemu. Tak więc wirus przechwytuje odwołania systemu do MBR i podstawia jego właściwą wersję zapisaną w innym miejscu na dysku, co pozwala mu pozostawać

w ukryciu. Taki wirus nazywamy wirusem utajnionym (stealth).

Większość wirusów nie niszczy danych, lecz infekuje jedynie dyski lub pliki. Jest jednak wiele sytuacji, w których powodują one zakłócenia w pracy systemu (dotyczy to np. zainfekowanych sterowników). Nie oznacza to jednak, że destrukcyjne wirusy nie istnieją.

Zgodnie z danymi opracowanymi na podstawie bazy wirusów Rady do spraw Bezpieczeństwa Systemów Komputerowych CIAC przy Departamencie Energii USA pierwszym, wykrytym w 1986 roku wirusem „na wolności" był Brain. Był on wirusem bootsektora rezydującym w pamięci komputera. Raport bazy informował:

„Wirus ten infekuje tylko bootsektory dyskietek 360 KB. Kod wirusa może spowodować uszkodzenie plików na dyskietce lub uszkodzenie tablicy alokacji plików FAT. Działanie wirusa ogranicza się do dyskietki, nie infekując dysku twardego".

W rok później, to znaczy w 1987, pojawiło się wiele nowych wirusów, które poczyniły znaczne szkody. Jednym z nich był Merrit, który niszczył tablice FAT na dyskietkach. Przeszedł on wiele transformacji i doczekał się licznych odmian, z których najniebezpieczniejsza — zwana Golden Gate — potrafiła sformatować dysk twardy.

Rodzaje wirusów komputerowych

Wirusy komputerowe to programy, które są zdolne do kopiowania i rozprzestrzeniania się w systemach komputerowych i sieciach bez zezwolenia. Wirusy komputerowe dzielą się na następujące grupy:

- Wirusy plikowe (file viruses);
- Boot-wirusy (boot viruses);
- Wirusy polimorficzne (polymorhic viruses);
- Wirusy ukrywające się (stealth viruses);
- Wirusy rezydentne a nierezydentne;
- Inne rodzaje.

Wirusy plikowe (file viruses)

Wirusy plikowe kryją się w następujących typach plików: pliki wsadowe (pliki .bat), pliki systemowe (pliki z rozszerzeniami sys lub bin włączając w nie *Io.sys* i *MSDOS. sys*) i binarne pliki uruchamialne (pliki z rozszerzeniami exe i com). Kilka wirusów plikowych może także infekować pliki z danymi. Dużo rzadziej wirusy te mogą infekować pliki zawierające kody źródłowe programów, biblioteki czy też moduły obiektowe.

Boot-wirusy (boot viruses)

Wirusy te infekują sektory startowe dyskietek i twardych dysków. Generalnie podczas infekowania dysku, wirus kopiuje oryginalne dane z bootsektora do jakiegoś innego wolnego sektora dysku. Jeśli rozmiar wirusa przekracza rozmiar sektora, tylko pierwsza część wirusa będzie znajdować się w zainfekowanym sektorze. Inne jego części będą rozmieszczone w wolnych sektorach dysku.

Następnie wirus kopiuje informacje o systemie (tablicę partycji dysku w przypadku dysków twardych i blok BIOS Parameter w przypadku stacji dysków) przechowywane w oryginalnym programie ładującym i zapisuje je do bootsektora.

Wirusy polimorficzne (polymorhic viruses)

Wirusy polimorficzne są trudne do wykrycia, ponieważ ich różne próbki nie wyglądają tak samo. Często dwie próbki tego samego wirusa polimorficznego nie mają ze sobą nic wspólnego. Ten polimorfizm może być osiągnięty poprzez zakodowanie wirusa lub przy użyciu różnych dekoderów.

Wirusy ukrywające się (stealth viruses)

Wirusy te przechwytują odwołania systemu operacyjnego do zainfekowanych plików lub sektorów dysku i zastępują dane, które byłyby widziane, jeśli pliki lub sektory nie były zainfekowane. Poprzez te działania wirusy ukrywają swoją obecność.

Wirusy rezydentne a nierezydentne

System może być zainfekowany przez wirusa rezydentnego, który umieszcza w pamięci RAM rezydentny fragment. Fragment ten przejmuje odwołania systemu, co umożliwia wirusowi infekowanie plików lub bootsektorów w czasie, gdy następuje do nich dostęp. Wirusy rezydujące w pamięci przerywają swą działalność tylko wtedy, gdy użytkownik wyłączy lub zresetuje zainfekowany system. (Niektóre wirusy potrafią przetrwać reset systemu). Wirusy nie rezydujące w pamięci nie infekują pamięci RAM i są aktywne tylko przez ograniczony czas. Niektóre wirusy umieszczają w pamięci RAM małe, rezydentne programy, które nie są odpowiedzialne za rozprzestrzenianie wirusa.

Inne rodzaje wirusów

Wirusy komputerowe mogą być klasyfikowane według różnych kryteriów. Wirusy towarzyszące (companion viruses) nie zmieniają plików. Tworzą one dla plików *exe* pliki towarzyszące, które mają taką samą zawartość lecz rozszerzenie *com*. Wirus okupuje plik *com* zamiast modyfikować plik *exe*. Na przykład, jeśli istnieją obydwa pliki *com* i *exe* z tą samą nazwą, DOS uruchomi plik *exe.* Oznacza to, w momencie, gdy użytkownik będzie próbował uruchomić plik *exe,* wystartuje towarzyszący mu plik *com*, który uaktywni wirusa, a następnie uruchomi plik *exe*. Robaki (worms) są wirusami, które rozprzestrzeniają się używając sieci komputerowych. Podobnie jak wirusy towarzyszące, nie zmieniają one plików czy też sektorów. Ładują się do pamięci z sieci komputerowej, szukają adresów sieciowych innych komputerów i przesyłają swoje kopie pod te adresy. Wirusy pasożytnicze (parasitic viruses) mo-

dyfikują sektory dysku lub zawartość plików. Rozprzestrzeniają się, gdy zarażone dyski lub kopie zarażonych plików są ładowne w innych komputerach. Wszystkie wirusy, które nie należą do dwóch poprzednich klas są wirusami pasożytniczymi i stanowią jeden z najniebezpieczniejszych i najpowszechniejszych wirusów.

Prawdopodobieństwo „nabycia" wirusa poprzez Internet jest niewielkie (co nie znaczy, że zerowe). Wszystko zależy od miejsca w Sieci, z którego korzystamy. Jeśli mamy zwyczaj odwiedzania „ciemnych zaułków" Internetu, powinniśmy zachować szczególną ostrożność przy ładowaniu nieznanych plików. Chodzi tutaj zwłaszcza o grupy dyskusyjne sieci Usenet, a w szczególności te grupy, na których publikuje się materiały zastrzeżone i nielegalne, na przykład pirackie programy lub pornografię. Zatem pobranie jakiegokolwiek archiwum z takiej grupy może narazić nas na niebezpieczeństwo infekcji wirusowej. Analogicznie sytuacja przedstawia się w grupach dyskusyjnych dystrybuujących narzędzia do łamania zabezpieczeń innych programów (tzw. cracki).

Większość wirusów pisana jest dla komputerów o architekturze sprzętowej zgodnej ze standardem IBM, w szczególności dla systemów operacyjnych DOS, Windows, Windows NT, Windows 95/98. Zatem w sieci składającej się z komputerów pracujących na wymienionych systemach z dostępem do Internetu wirusów bagatelizować nie można.

W praktyce nie istnieją metody pozwalające na ograniczenie użytkownikom możliwości ściągania plików ze względu na ich zawartość. Wprowadzanie administracyjnych zakazów niczego nie zmieni, gdyż zawsze znajdzie się taki użytkownik, który się do nich nie zastosuje. Zaleca się zatem instalację rezydentnych programów antywirusowych na wszystkich komputerach sieci.

Aby dowiedzieć się więcej na temat wirusów należałoby spędzić trochę czasu na studiowaniu zbiorów wirusów w Internecie. Zbiorów takich jest kilka, zawierają wyczerpujące informacjami na temat dotychczas odkrytych wirusów. Najbardziej kompletną i użyteczną wydaje się być baza wirusów prowadzona przez Radę CIAC: *http://ciac.llnl.gov/ciac/CIACVirusDatabase.html.*

W zbiorze, na który wskazuje powyższy odnośnik, znajdziemy wirusy uporządkowane według nazw oraz platform, na których występują. Od razu można zauważyć, że większość z nich pisana jest dla systemów operacyjnych firmy Microsoft, w szczególności dla środowiska DOS. Nie znajdziemy tam żadnych informacji na temat wirusów dla platformy Unix (choć mogą się ukazać później). Niedawno pojawiły się doniesienia o istnieniu wirusa o nazwie Bliss działającego w systemie Linux.

W sieci toczy się dyskusja na temat klasyfikacji Blissa. Trudno rozstrzygnąć, czy jest on wirusem czy koniem trojańskim. Większość dyskutantów skłania się jednak ku zaliczeniu go do grupy wirusów, gdyż twierdzą oni, że Bliss kompiluje się bez problemów na innych odmianach systemów unixowych. Jedyny znany program narzędziowy, który sprawdza system na obecność wirusa, napisany został przez Alfreda Hugera i mieści się pod adresem: *ftp://ftp.secnet.com/pub/tools/abliss.tar.gz.*

Prawdopodobieństwo, że nasz system zostanie zarażony tym wirusem jest nikłe. Autor programu zastosował odpowiednie zabezpieczenia, umożliwiające rozpakowanie archiwum i użycie wirusa tylko zaawansowanym programistom. Jednakże, jeśli znajdziemy go w swoim systemie, powinniśmy wysłać wiadomość do grupy dyskusyjnej z opisem okoliczności i ewentualnych strat, jakie program wyrządził w zaatakowanym systemie.

Warto wyjaśnić przyczyny zjawiska, powodującego takie dysproporcje w ilości wirusów opracowywanych na poszczególne platformy systemowe. Otóż w systemie Unix i jego pochodnych istnieją procedury kontroli dostępu umożliwiające administratorowi przydzielanie praw do poszczególnych plików zapisanych na dyskach komputera. Zatem można wskazać że dany plik może być zapisywany przez użytkownika A, ale już nie przez użytkownika B. Z powodu tych zabezpieczeń wirus w takim środowisku ma bardzo ograniczone możliwości rozprzestrzeniania.

Jak by nie patrzeć, w Internecie wirusy stanowią poważne zagrożenie. Zwłaszcza dla użytkowników DOS lub któregokolwiek z systemów Windows. Istnieje kilka programów narzędziowych, które pozwalają zabezpieczyć system przed ich atakiem.

Ochrona

Dokładnie tak jak w przypadku ochrony zdrowia najlepsze rezultaty dają wcześniejsze działania zapobiegawcze. Przestrzegając kilku zasad możesz znacznie zmniejszyć prawdopodobieństwo infekcji. Trzeba więc:

- Nabywać tylko legalne oprogramowanie;
- Tworzyć dyskietkę startową, kopiować na niej programy antywirusowe (wersje dla DOS) i zabezpieczyć ją przed zapisem;
- Regularnie tworzyć kopie zapasowe plików;
- Sprawdzać wszystkie dyskietki przed użyciem; nie można uruchamiać niesprawdzonych plików (w szczególności pobranych z sieci komputerowych);
- Ograniczyć liczbę osób upoważnionych do korzystania z plików;
- Regularnie przeprowadzać kontrolę antywirusową komputera korzystając tylko z najnowszego oprogramowania oraz baz danych z uaktualnionymi antywirusowymi.

Wykrycie wirusa

Gdy w systemie komputerowym zagości wirus, można zauważyć, że:

- Uruchamianie niektórych programów jest znacznie wolniejsze;
- Niektóre pliki (w szczególności te, które są uruchamiane) zwiększają swój rozmiar;
- Pojawiają się nowe pliki nieznanego pochodzenia;

- Ilość wolnej pamięci RAM zmniejsza się z nieznanych powodów;
- Występują nieoczekiwane komunikaty lub dźwięki;
- System staje się niestabilny;
- System nagle się resetuje.

Co należy wtedy robić?

Jeśli mamy program antywirusowy należy przetestować cały komputer, a następnie spróbować „wyleczyć" zarażone obiekty. Warto zaznaczyć, że podczas leczenia programem antywirusowym zarażone pliki mogą ulec uszkodzeniu. Dlatego jeżeli wirus zaatakował bardzo ważne dokumenty, przed podjęciem próby „leczenia" należy wykonać ich kopię.

Jeżeli program antywirusowy nie wykryje żadnego zagrożenia, a wyżej opisany symptomy dalej występują, trzeba się upewnić, czy zainstalowane są najnowsze bazy antywirusowe.

Programy antywirusowe

Wszystkie zaprezentowane programy są godne polecenia (gdy któryś z nich nie został ujęty na tej liście, nie musi to oznaczać, że jest nieskuteczny). W chwili obecnej istnieją setki programów, co zmusza do przeprowadzenia selekcji.

Najważniejsze z nich to:

- *VirusScan*
  VirusScan dla Windows 95 napisany w firmie McAfee, odnaleźć można pod adresem: *http://www.nai.com/default_mcafee.asp*
- *Thunderbyte Anti-Virus*
  Thunderbyte Anti-Virus dla Windows 95 odnajdziemy w Internecie pod adresem: *http://www.thunderbyte.com*
- *Norton Anti-Virus*
  Ten program przeznaczony jest dla DOS, Windows 95 i Windows NT firmy Symantec. Można go odnaleźć pod adresem: *http://www.symantec.com/avcenter/index.html*
- *ViruSafe*
  Virusafe napisany przez Eliashim figuruje pod adresem: *http://www.eliashim.com/*
- *PC-Cillin II*, PC-Cillin II, autorstwa Check-It odnajdziemy pod adresem: *http://www.checkit.com/*
- *FindVirus v7.68*
  Program firmowany przez Dr Solomona przeznaczony jest dla systemu DOS. Odnajdziemy go w Internecie pod adresem:

- *http://www.drsolomon.com/*
- *Sweep*, Sweep dla Windows 95 i Windows NT sygnowany przez Sophos, znajdziemy pod adresem: *http://www.sophos.com/*
- *Iris Anti-Virus Control*. Program antywirusowy firmy Iris Software odnajdziemy pod adresem:*http://www.irisav.com/*
- *Norman Virus Control*, Norman Virus Control autorstwa firmy Norman Data Defense System znajduje się pod adresem: *http://www.norman.com/*
- *F-PROT Professional Anti-Virus Toolkit*,F-PROT Professional Anti-Virus Toolkit autorstwa Data Fellows odnajdziemy pod adresem: *http://www.datafellows.com/*
- *The Integrity Master*
  The Integrity Master napisany przez firmę Stiller Research znajduje się pod adresem: *http://www.stiller.com/stiller.htm*

Istnieją setki programów antywirusowych. Powyżej wyszczególniono te, które są łatwo dostępne w Internecie i często uaktualniane. To ważna kwestia, gdyż każdego dnia pojawiają się na świecie nowe wirusy, a ich autorzy stosują coraz bardziej wyrafinowane techniki i algorytmy.

Dla administratorów starszych systemów operacyjnych przydatne mogą okazać się zestawione poniżej narzędzia (nie zawsze bowiem mamy możliwość zastosowania programu antywirusowego napisanego na Windows 95) wchodzące w skład kolekcji programów dla MS-DOS Simtel.Net. W archiwum Simtel.Net można znaleźć między innymi programy umożliwiające wykrycie i eliminację wirusa z naszego systemu. Zbiory te znajdują się pod adresem: *http://oak.oakland.edu/simtel.net/msdos/virus.html.*

Z kolei kolekcję programów dla Windows 3.x Simtel.Net, która zawiera zbiór programów antywirusowych dla systemów Windows 3.x przyjrzeć można pod adresem: *http://oak.oakland.edu/simtel.net/win3/virus.html.*

Warezy — czyli piractwo komputerowe

Przemierzając bezkresne zasoby Internetu osoby dobrze wtajemniczone mogą natknąć się na jeszcze inny rodzaj działalności sieciowego undergroundu — *warezy*. Są to pirackie wersje komercyjnego oprogramowania użytkowego (apps, utils) lub gier (games*)*. Dostępne są na dziesiątkach serwerów, zaś odnośniki do nich znajdują się na wielu stronach WWW. Często bywa tak, że w Internecie dostępna jest już nielegalna wersja programu, którego premiera ma się dopiero odbyć (nie jest to bynajmniej wersja beta). Tak było w przypadku Windows 98 czy chociażby Windows 2000, którego kopia była dostępna na jednym z serwerów już na miesiąc przed oficjalną premierą.

Większość warezowców traktuje swoją działalność jako walkę wymierzoną przeciwko producentom oprogramowania. Zazwyczaj kupując jakiś towar mamy możliwość sprawdzenia go lub nawet jego zwrotu, jeżeli nie spełnił naszych oczekiwań. Nie dotyczy to jednak oprogramowania (istnieją co prawda wersje próbne programów, ale nie każdy musi mieć do nich dostęp). Innymi słowy — często jesteśmy zmuszeni do kupowania przysłowiowego kota w worku. Z tego powodu dystrybucja warezów jest bezpłatna. Każdy może je skopiować, sprawdzić zalety danego programu i jeżeli jest nim usatysfakcjonowany pobiec do sklepu i kupić wersję legalną. Ideologia poniekąd słuszna, aczkolwiek nie znam takiego człowieka, który mając nielegalną wersję AutoCada wyłoży 10 000 zł po to tylko, aby mieć czyste sumienie. Dlatego też ideologia ta nie przemawia do producentów oprogramowania, FBI i szeregu organizacji antypirackich. Ale nie musi, bo — dopóki prawo nie ulegnie modyfikacji — warezowcy są wciąż bezkarni.

Wystarczy zajrzeć do Usenetu, aby przekonać się, jak prężna jest to dziedzina internetowej przestępczości. Dziewięć największych grup warezowych z *alt.binaries.warez* czy *alt.binaries.warez.ibm-pc* na czele generuje blisko 30% całego ruchu w Usenecie (informację te podaję za OpNet). Microsoft Office Pro and Visual C++, Autodesk 3D Studio MAX, SoftImage 3D, SoundForge, Cakewalk Pro Audio, Word Perfect, Adobe Photoshop i wiele innych programów dystrybuowanych jest za darmo.

Na kanałach IRC (FreeWarez, Warez96, Warez4Free, WarezSitez, WarezAppz, WarezGamez) będących niekiedy kanałami prywatnymi, warezowcy wymieniają doświadczenia i wiedzę. Często skupiają się w grupy, np. Pirates With Attitude (PWA), DOD, The Inner Circle czy Razor 1911. Mają też swoich idoli. Tak jak dla hakerów idolem jest Kevin Mitnick, tak dla warezowców mitem stał się David LaMacchia, student inżynierii w Massachusetts Institute of Technology, który wykorzystał dwa tamtejsze BBS-y (CYNOSURE I i CYNOSURE II) w celu dystrybucji nielegalnego oprogramowania. W chwili jego aresztowania przez FBI znajdowało się na nich oprogramowanie wartości ponad miliona dolarów. FBI udało się go aresztować w 1995 roku, ale sąd miał poważny problem z wydaniem wyroku, albowiem nie był w stanie udowodnić mu czerpania korzyści materialnych ze swojego procederu ani nawet jego ukrywania. W efekcie David LaMacchia pozostał na wolności.

Antypirackie organizacje, takie jak Software Publishers Association czy Business Software Alliance, szacują, że każdego dnia do Internetu trafiają nielegalne kopie programów wartości blisko 5 000 000 dolarów.

Powszechnie wiadomo, że Polsce plaga piractwa komputerowego zakorzeniła się bardzo głęboko. Nie da się ukryć, że społeczeństwo kradzież cudzej pracy w dalszym ciągu uważa za coś normalnego. Sprzedając zatem okupiony ciężką pracą program firmie XYZ (licencja jednostanowiskowa), producenci oprogramowania mają prawie pewność, że program ten rozprzestrzeni się po wszystkich oddziałach firmy XYZ, a być może nawet „rozejdzie się" po firmie YZX. Według danych BSA w samym tylko 1998 roku 80% oprogramowania zainstalowanego na polskich komputerach pochodziło z nielegalnych źródeł. Można z tego wyciągnąć wniosek, że około 80% zysku z każdego sprzedanego programu jest tracone bezpowrotnie na rzecz piratów. To z tego właśnie powodu polskim producentom oprogramowania

wciąż brakuje pieniędzy na tworzenie lepszych aplikacji, a najlepsi informatycy wyjeżdżają z kraju.

Przeciwdziałanie

Prowadzone przez wielkie zachodnie firmy kampanie, odwołujące się do uczciwości oraz straszące użytkowników restrykcjami prawnymi odnoszą niewielki skutek, bo ludzie i tak kopiują wszystko, co się tylko da. Mało dają również promocje w rodzaju: „jeżeli masz piracką kopię, oryginał kupisz za pół ceny".

Wydaje się więc, że pozostaje tylko jedna możliwość: stosowanie w sprzedawanych programach odpowiednich procedur, chroniących przed nielegalnym kopiowaniem. Wymaga to jednak oderwania informatyków od wykonywanej przez nich pracy i zaangażowania w żmudne tworzenie systemu skomplikowanych zabezpieczeń, co znacznie podniesie koszt zabezpieczonych aplikacji. Pojawia się zatem kolejne pytanie: czy to się opłaci? Nie jest prawdziwe twierdzenie, że użytkownicy komputerów są biedni, gdyż zwykle stać ich na zakup komputerów, więc legalne oprogramowanie nie powinno stanowić problemu. Piractwo jest raczej skutkiem tego, że większość ludzi zastanawia się nad tym, dlaczego należy płacić za coś, co można mieć za darmo. Wystarczy więc utrudnić proceder nielegalnego kopiowania, a dotychczasowi „złodzieje" będą zmuszeni zakupić oryginalny system finansowo-księgowy, kadry, płace, obsługę produkcji, edytor tekstu, arkusz kalkulacyjny, program do nauki języków czy nową grę. Pojawia się jednak pytanie o to, jak zabezpieczać aplikacje.

Generalnie są dwie metody zabezpieczania software'a:

- Programowa;
- Sprzętowa.

Można zastosować zabezpieczenie, takie jakie stosuje większość dużych firm (przy pierwszej instalacji na dyskietkach instalacyjnych zostaje zapisywana informacja o użytkowniku). W takiej sytuacji każdy, kto spróbuje skopiować tak przetworzone dyskietki, zostaje zdemaskowany i wtedy już wszyscy będą wiedzieli kto był tym „dobrym" piratem i pozwolił „ukraść" odpowiednie programy. Jednak ta metoda jest mało skuteczna. Wystarczy bowiem zrobić kopię dyskietek instalacyjnych przed pierwszą instalacją i nie ma problemu.

Można jeszcze inaczej. Załóżmy, że firma XYZ, producent znanego programu, tworzy logiczny błąd na dyskietce, co powoduje, że nie można go skopiować ani za pomocą programu DISKCOPY, ani DISKDUPE, ani żadnym innym wynalazkiem crackerów. Paradoksalnie jednak wystarczy skopiować z dyskietki plik *xyz.exe*, by dysponować do woli piracką wersja programu. Warto dodać, że dyskietki Microsoft Windows 95 zapisane są w większym formacie i początkujący użytkownicy komputerów (a takich jest większość) nie potrafią pokonać tej bariery. Wielu producentów gier dostarcza swoje produkty z obszernymi instrukcjami, które są często wykorzystywane jako swego rodzaju zabezpieczenia (pewne wybrane słowa z tych instrukcji są zapamiętane w postaci zaszyfrowanej w programie, który w odpowied-

niej chwili wyświetla komunikat „ proszę podać słowo I, z wiersza 10, strony 25”). Użytkownicy nie posiadający takich instrukcji, są wtedy zwykle skazani na zakup oryginalnych gier albo zdobycie i skserowanie wszystkich książek sprzedawanych razem z grami. Wydawałoby się, że będzie to skuteczne utrudnienie dla piratów. Niestety powyższy typ zabezpieczenia nie zdaje egzaminu w powiązaniu z programami dla biznesu, gdyż na stronach internetowych pełno jest gotowych porad przygotowanych przez komputerowych zapaleńców dotyczących tego, jak odbezpieczyć daną grę czy program komputerowy.

W związku z powyższym wydaje się więc, że dobrym rozwiązaniem byłoby powiązanie wielu różnych metod zabezpieczania oprogramowania przed nielegalnym kopiowaniem. Uczyniło tak już wiele firm, stosując oprogramowanie umożliwiające zabezpieczenia aplikacji różnymi metodami. Może to wyglądać następująco:

- Instalowane dane są spakowane w archiwach na dyskietkach instalacyjnych i tylko program instalujący potrafi przeprowadzić instalację, czyli rozpakować te archiwa;
- Pierwsza dyskietka instalacyjna jest sformatowana niestandardowo, przez co nie jest możliwe skopiowanie całej jej struktury (można jedynie skopiować znajdujące się na niej pliki);
- Przed przeprowadzeniem instalacji, program instalujący sprawdza, czy jest startowany z oryginalnej dyskietki (tj. sformatowanej w odpowiedni sposób) oraz czy nie został przekroczony limit dozwolonych instalacji;
- Po rozpakowaniu archiwów, program instalujący zakłada w katalogu docelowym instalacji plik z kluczem, w którym są zapisane w formie zaszyfrowanej: nazwa i numer seryjny pierwszego dysku twardego komputera (jedynie program instalujący potrafi wygenerować klucz);
- Zainstalowana aplikacja zawsze przed uruchomieniem testuje, czy jest startowana z komputera, w którym parametry pierwszego dysku twardego są takie same jak zapisane w kluczu.

Należy zwrócić uwagę na fakt, że powiązując te wszystkie metody zabezpieczenia ze sobą można sprawić, że oprogramowania nie będzie w stanie skopiować nie tylko przeciętny użytkownik, ale również „zawodowym” pirat. Dzieje się tak, ponieważ:

- Żaden pirat nie potrafi skopiować pierwszej dyskietki instalacyjnej za pomocą prostych tricków;
- Nie potrafi też skopiować zainstalowanych aplikacji ze względu na to, że nie może odtworzyć klucza w innym systemie komputerowym;
- Nie może też z „pożyczonych” dyskietek instalacyjnych wykonać nieograniczonej liczby instalacji ze względu na ustalone limity.

Co wiec może zrobić pirat komputerowy? Przede wszystkim użyć Debuggera do śledzenia pracy programu. Nie jest banalna sprawa, gdyż tam również czyhają zastawione na niego pułapki. Przytłaczająca większość piratów lub słabych crackerów zostanie powstrzymana tymi zabezpieczeniami i sprzedaż legalnego oprogramowa-

nia może zasadniczo wzrosnąć, ponieważ potencjalni piraci będą zmuszeni do uczciwości.

Zabezpieczenia sprzętowe

Stosować można rozmaite zabezpieczenia sprzętowe. Może to być na przykład karty wkładana do komputera lub podłączana do złącza szeregowego (tzw. *klucz sprzętowy*). Aplikacja wysyła do takiej karty losowe dane, po czym sama również je przetwarza według pewnego algorytmu. Gdy otrzyma wynik, porówna go z wynikiem wysłanym przez kartę i jeśli te dane będą się różniły — aplikacja przerwie swoje działanie i na ekranie pojawi się komunikat: „Aplikacja skopiowana nielegalnie, proszę skontaktować się z firmą XYZ, tel. 0 — XX XXXX XX". Stosując zabezpieczenie sprzętowe tego typu, nie potrzeba już wykorzystywać żadnych innych, ponieważ aplikacja i tak będzie przywiązana do wybranego komputera. Poza tym nawet zaawansowani hakerzy-crackerzy będą mieli trudności ze zrozumieniem tego, jakie dane wchodzą i wychodzą z karty.

O wiele skuteczniejszymi i inteligentniejszymi zabezpieczeniami sprzętowymi są *karty mikroprocesorowe,* takie same jak stosowane w telefonach komórkowych GSM (SIM). Każda taka karta jest swoistym mikrokomputerem, gdyż dysponuje własnym mikroprocesorem oraz pamięcią. Rozmiarem natomiast nie różni się od kart magnetycznych stosowanych w automatach telefonicznych (cześć użytkowa jest nawet kilka razy mniejsza). Każdy komputer może dysponować czytnikiem takich kart (urządzenie wkładane w miejsce stacji dyskietek), gdyż wszyscy użytkownicy mają własne karty. Aplikacja może więc łatwo „rozpoznać" z kim ma do czynienia i w odpowiedni sposób zareagować. Na każdej karcie mogą być zapisane różne informacje: numer, imię, nazwisko, prawa dostępu, priorytet ważności użytkownika, stopień w firmie. Nie można także zapomnieć o *pastylkach szyfrujących* przydatnych wszędzie tam, gdzie trwa transmisja ważnych danych, gdyż wielkie firmy muszą się przecież liczyć ze szpiegostwem przemysłowym.

Szkoda, że nie wszyscy zdają sobie z tego sprawę, że w dzisiejszych czasach informacja jest na wagę złota (o nią przecież głównie walczą hakerzy), ale gdy ktoś im ukradnie np. bazę danych kontrahentów i podkupi klientów za cenę o symboliczną złotówkę mniejszą, wtedy na pewno zrozumieją. Znane są przecież przypadki podłączania laptopów do sieci komputerowych i wykradanie cennych danych. W dzisiejszej dobie nawet płytki CD są kopiowane nielegalne za pomocą nagrywarek, które stają się coraz tańsze. Jednak i tę płytę można zabezpieczyć, a wtedy tylko kosztujące krocie maszyny kopiujące potrafią sobie poradzić z zabezpieczeniami. A na takie nie każdego pirata komputerowego stać. Natomiast w nowym standardzie dysków DVD *(Digitali Video/Versatible Disk)* o znacznie podwyższonej pojemności (4-8 GB) jest już niejako „z urzędu" przewidziane miejsce na zabezpieczanie dysków przed nielegalnym kopiowaniem. Chociaż jak pokazał czas nawet ten standard nie oparł się crackerom, którzy stworzyli słynny już dzisiaj program DeCSS, pozwalający na kopiowanie na dysk twardy całej zawartości filmu z płyty DVD. Przedstawiciele przemysłu filmowego byli zaskoczeni, gdy okazało się, że sprytni programiści znaleźli sposób na zdjęcie blokady chroniącej filmy zapisane na nowym nośniku. Do tej pory sądzono, że wykorzystane systemy zabezpieczeń są wy-

starczające do uniemożliwienia hakerom i piratom wykonywania nielegalnych kopii. Teraz program o nazwie DeCSS, dostępny bezpłatnie w Internecie, potrafi odblokować informacje zapisane na płycie. Dzięki temu możliwe stało się kopiowanie zawartości DVD-Video (płyt z filmami) na twarde dyski komputerów i wykonywanie kolejnych, nielegalnych kopii lub odtwarzanie ich w domu. Pojawienie się programu oczywiście nie bardzo spodobało się przedstawicielom przemysłu filmowego. Stowarzyszenie MPAA (*Motion Picture Association of America*) natychmiast wystąpiło do wszystkich administratorów stron WWW oferujących program DeCSS z prośbą o usunięcie go z serwerów. Jednocześnie zagrożono sięgnięciem po tzw. Digital Millenium Copyright Act, czyli obowiązujące od roku przepisy zabraniające produkowania, dystrybucji lub sprzedaży narzędzi umożliwiających łamanie zabezpieczeń. „MPAA podchodzi bardzo poważnie do każdego przypadku łamania prawa i wykorzystania technologii do niszczenia zabezpieczeń przed kopiowaniem" — powiedział na konferencji prasowej Rich Taylor, rzecznik stowarzyszenia. Digital Millenium Copyright Act umożliwia nałożenie na przestępcę kary w wysokości 2 500 dolarów grzywny za jednokrotne skopiowanie zabezpieczonego materiału. Jednocześnie MPAA nie zamierza ścigać użytkowników oprogramowania DeCSS, którzy będą kopiować płyty DVD.

Tymczasem użytkownicy przejęli pojawienie się DeCSS z ogromnym zainteresowaniem. W ciągu kilku dni — zanim akcja MPAA doprowadziła do wycofania programu ze stron internetowych — narzędzie to trafiło do tysięcy użytkowników. Z samej tylko strony *CNet Download.com* pobrano DeCSS podobno ponad 5 000 razy. Klienci zgadzają się bowiem, że powinni mieć prawo wykonywania kopii płyt DVD na swój własny użytek. Sam program prawdopodobnie nie zostanie wycofany ze wszystkich serwerów w Internecie. Największe i najpopularniejsze strony WWW poświęcone sprawom DVD-Video i DVD-Audio (m.in. *DVD Utilities Network* i *DVD Information Site*) wprawdzie pozbyły się go po nerwowej reakcji MPAA, jednak jest on dostępny na mniejszych, prywatnych stronach oraz za pośrednictwem grup dyskusyjnych.

Nie jest to pierwszy przypadek, gdy pojawiły się kłopoty z zabezpieczeniami dysków DVD. Możliwość tworzenia cyfrowych duplikatów — bez utraty jakości — była dla piratów zbyt silną pokusą. Nie przeszkodziły im bariery techniczne (m.in. szyfrowanie zapisu, antypirackie przepisy prawne). Pierwsze płyty DVD z pirackimi kopiami amerykańskich filmów pojawiły się w Azji, a konkretnie w Hongkongu. Najpierw kopiowano animowane filmy disneyowskie — „Bambi", „Pinokio" i „Kopciuszek". Wkrótce po nich pojawiły się inne —„Przeminęło z wiatrem" oraz „Titanic". Płyty — w pudełkach i z nadrukiem producenta można kupić w legalnie działających sklepach z filmami i płytami audio. Wytwórcą pirackich kopii DVD była tajwańska firma Eversion, specjalizująca się w wydawaniu materiałów stworzonych przed 1965 rokiem. Według obowiązującego prawa, materiały takie nie mogą korzystać z ochrony prawnej i można je kopiować do woli. Co najciekawsze, filmy wytwórni Disneya oraz „Titanic" nie pojawiły się wtedy jeszcze oficjalnie na płytach DVD. Wytwórnie filmowe pracują dopiero nad przeniesieniem ich na cyfrowe krążki. Zostały one zatem skopiowane ze zwykłych kaset wideo lub z płyt LaserDisc — popularnych w Azji i w Stanach Zjednoczonych. Z wysoką — cyfrową jakością zostało natomiast skopiowane przez piratów „Przeminęło z wiatrem". Wybór

i wprowadzenie satysfakcjonującego producentów płyt DVD systemu ochrony zawartości przed kopiowaniem był dla konsorcjum DVD najważniejszym problemem przed wprowadzeniem standardu na rynek. Pod koniec 1996 roku udało się członkom konsorcjum uzgodnić metody ochrony danych. Obecnie wykorzystywane są trzy formy zabezpieczenia płyt DVD przed nielegalnym kopiowaniem — Analog Copy Protection, Copy Generation Managment System i Content Scrambling System.

Analog Copy Protection — to zestaw dwóch metod zabezpieczeń opracowanych przez firmę Macrovision w celu ochrony filmów na kasetach VHS. Polega on na zakłócaniu sygnału wyjściowego oraz osłabieniu informacji o kolorze. Dzięki temu na kopiach z DVD wykonanych na ponad 95% modelach domowych magnetowidów obraz będzie słabo widoczny.

Copy Generation Managment System — pozwala producentowi na ustalenie, jak wiele kopii (zwykle jedna) może być wykonanych z jednego dysku. Uniemożliwia to zatem wykonywanie kolejnych generacji kopii. Wykorzystywane do kopiowania urządzenia muszą być jednak wyposażone w odpowiednie oprogramowanie.

Obie wymienione metody zabezpieczeń przed kopiowaniem mogą jednak zostać ominięte przez piratów dysponujących odpowiednią wiedzą i sprzętem.

Content Scrambling System — wykorzystuje technologie kodowania informacji do „szyfrowania" danych na DVD. Wszystkie odtwarzacze muszą być jednak wyposażone w urządzenie, które potrafi odszyfrować informacje CSS. Właśnie ten kod udało się złamać autorom oprogramowania DeCSS, co daje każdemu użytkownikowi komputera wyposażonego w czytnik DVD możliwość dowolnego kopiowania płyt DVD na swój twardy dysk.

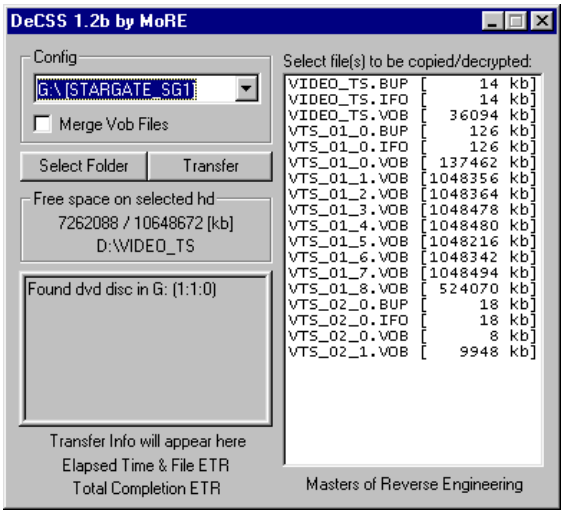
Pierwszą rzeczą, którą zatem musi zrobić pirat komputerowy jest pozyskanie odpowiedniego oprogramowania, które bez większego problemu dostępne jest w Internecie. Nie trzeba chyba dodawać, jak ważny jest zakup odpowiedniego sprzętu komputerowego, w który musi być wyposażony „rasowy" pirat. Później zaopatruje się on w programy:

- DeCSS;
- VobDec;
- FlasKMPEG DVD Selector;
- SubRip;
- DVD Subripper.

I tak rozpoczyna się kopiowanie VOB-ów na dysk twardy własnego komputera. Operację tę może przeprowadzić w różny sposób, np. za pomocą programów DeCSS lub VobDec.

DeCSS

Pirat uruchamia program i wybiera w polu *Config* swój napęd DVD (w którym powinna znajdować się oczywiście płyta DVD). Zaraz potem widzi listę plików znajdujących się na płycie. Zaznacza wszystkie pliki (zakodowane są tylko VOB-y, ale DeCSS skopiuje wszystkie pliki bez względu na to, czy są one zakodowane, czy nie). Następnie naciska przycisk *Select Folder*, aby wybrać katalog, w którym mają być umieszczone skopiowane pliki. Wcześniej zakłada na dysku folder *VIDEO_TS* (np. *c:\VIDEO_TS*), który powinien się znajdować w głównym katalogu. Umożliwi to oglądanie filmów przez odtwarzacze łącznie z menu i wszystkimi możliwościami DVD (bez problemu działa to z programem Cinemaster i dość dobrze z WinDVD). Wystarczy zmienić w tych odtwarzaczach literę oznaczającą napęd na literę dysku, na którym znajduje się folder *VIDEO_TS*. Następnie pirat naciska przycisk *Transfer* i po pewnym czasie, (który jest uzależniony od szybkości napędu i długości filmu) otrzymuje kopię płyty DVD na twardym dysku.



Można to zrobić jeszcze inaczej. Wystarczy przekopiować pliki filmu (czyli te oznaczone jako *VTS_0x_x.VOB*), jak i pojedyncze pliki, co jednak utrudni znacznie dalsze dekodowanie. Przy okazji nazewnictwo plików znajdujących się w folderze *VIDEO_TS* na płycie DVD (katalog *AUDIO_TS* jest zazwyczaj pusty) wygląda następująco:

Część dotycząca ekranów początkowych (np. prawa autorskie itp.):

- *VIDEO_TS.BUP* — backup pliku IFO (niekodowany);
- *VIDEO_TS.IFO* — dane nawigacyjne (niekodowany);
- *VIDEO_TS.VOB* — ekrany początkowe (np. prawa autorskie).

Właściwy (pierwszy) film:

- *VTS_01_0.BUP* — backup pliku IFO (niekodowany);
- *VTS_01_0.IFO* — dane nawigacyjne (niekodowany);
- *VTS_01_0.VOB* — napisy z filmu (zapisane jako obrazki);
- *VTS_01_1.VOB* — pierwszy plik filmu;
- *VTS_01_2.VOB* — drugi plik filmu;
- *VTS_01_3.VOB* — trzeci plik filmu itd...

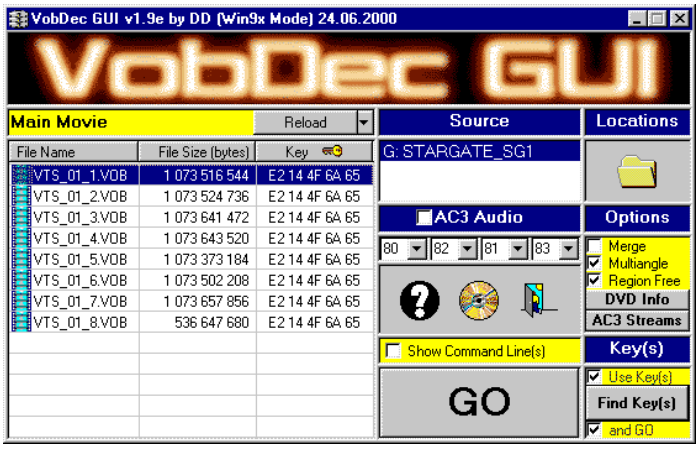
(Ewentualnie) drugi film:

- *VTS_02_0.BUP* — backup pliku IFO (niekodowany);
- *VTS_02_0.IFO* — dane nawigacyjne (niekodowany);
- *VTS_02_0.VOB* — napisy z filmu (zapisane jako obrazki);
- *VTS_02_1.VOB* — pierwszy plik drugiego filmu itd...

Pliki w formacie *VOB* mają zazwyczaj długość około 1048 MB, a mniejszy jest jedynie plik znajdujący się na końcu pierwszej warstwy DVD i ostatni plik *VOB* filmu. Jeśli na DVD znajduje się kilka filmów (np. trailery, filmy o filmie), to oznaczone są one kolejnymi numerami w 6 literze nazwy. DeCSS jest pierwszym programem do kopiowania plików z DVD na dysk i jest już dość stary, ale znacznie wygodniejszy w obsłudze niż VobDec. DeCSS nie naprawia plików zawierających sceny oglądane z kilku widoków (czyli multiangle) i czasami ma kłopoty z kopiowaniem niektórych płyt. Jeśli nie działa, to niekiedy pomaga wyłączenie DMA w ustawieniach napędu DVD.

VobDec

W przeciwieństwie do DeCSS przy dekodowaniu program ten nie korzysta ze sprzętowego dekodera w napędzie. Dekodowanie odbywa się wyłącznie programowo. Program ten nie posiada własnego GUI (interfejsu graficznego) i działa w jedynie w oknie DOS-owym. Z tego powodu przygotowano dla niego kilka nakładek graficznych. Chyba najlepszą jest VobDec GUI, który dostępny jest aktualnie w wersji 1.9e. Aby całość działała odpowiednio, pirat dogrywa do katalogu (w którym znajduje się VobDec GUI) zawartość archiwum z właściwym VobDeciem. Po uruchomieniu nakładki powinien pojawić się ekran podobny do tego, który został przedstawiony na poniższym rysunku.



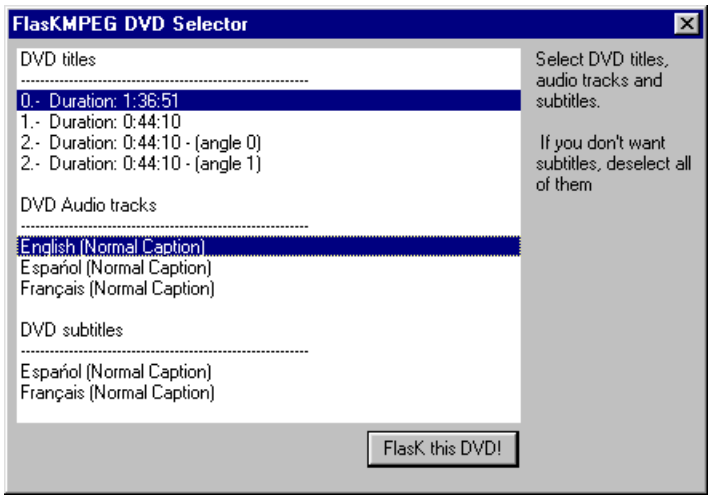
Następnie automatycznie zostanie wykryty napęd DVD i w oknie po lewej stronie zostanie wyświetlona zawartość płyty. Wówczas należy zaznaczyć interesujące pliki (najczęściej wszystkie) i kliknąć ikonę teczki w części oznaczonej jako *Locations*. W tym oknie trzeba określić położenie właściwego VobDeca, jak również katalogu wyjściowego, do którego zostaną przekopiowane wszystkie VOB-y. Teraz w zasadzie wystarczy kliknąć ikonę płyty CD i czekać na zakończenie kopiowania. VobDec GUI posiada także kilka dodatkowych opcji, takich jak dekodowanie filmów w systemie MultiAngle (np. „Maska Zorro", „Matrix"), usuwanie kodowania regionów, zgrywanie ścieżek AC3, jednak do prostego zgrywania filmu DVD wystarczy ustawić opcje tak, jak to pokazano w powyższym przykładzie.

Po wykorzystaniu jednego z tych dwóch programów pirat komputerowy ma na dysku kilka plików VOB. Co robi dalej? Zabiera się za właściwe dekodowanie. Ale do tego celu używa już innego programu — FlasKMPEG DVD Selector.

Kodowanie

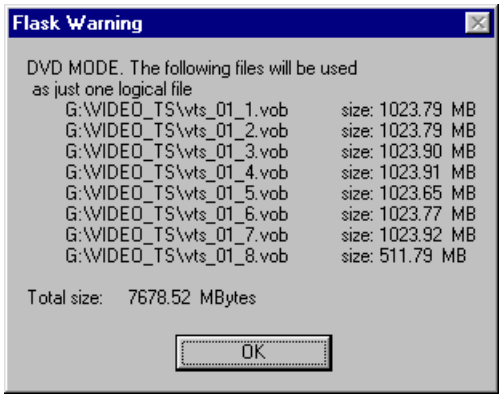
Jeśli pirat ma już na dysku kilka VOB-ów, a ponadto parę dziwnych plików, zabiera się za właściwe kodowanie filmu. Uruchamia program FlasK MPEG DVD Selector. Teraz — w zależności od tego, czy zgrywał całą płytę, czy tylko VOB-y — musi wybrać właściwy sposób wczytywania filmu.

Jeśli przegrywał całość (czyli pliki z rozszerzeniem *VOB* i *IFO*), to wybiera *File/Open DVD File* (opcja ta pojawiła się w najnowszej wersji FlasK MPEG DVD Selector, więc nie jest jeszcze przetłumaczona na język polski). Wybiera plik z rozszerzeniem *.ifo* (zazwyczaj *vts_01_0.ifo*) i pojawia się okno podobne do tego przedstawionego na rysunku.

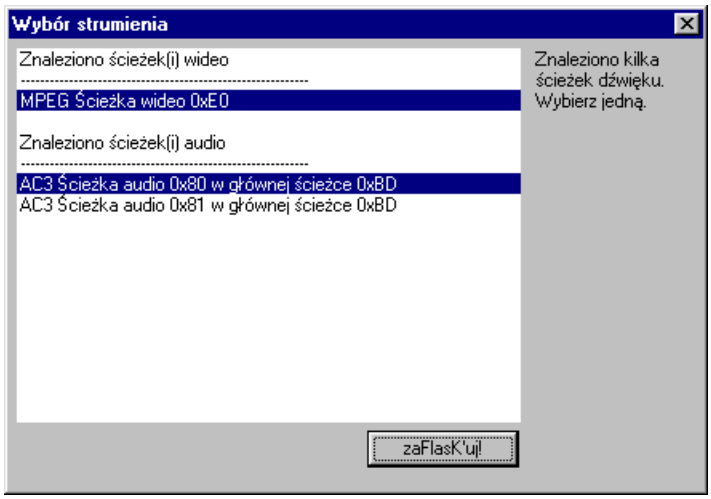


W oknie tym zaznacza, który film ma być kodowany (opcja: *DVD titles)*, ścieżkę dźwiękową (opcja: *DVD Audio Track)* i napisy, które w tym programie są nakładane bezpośrednio na film i wyglądają identycznie, jak podczas oglądania go za pomocą odtwarzacza DVD. Niestety w obecnej wersji FlasK MPEG DVD Selector nie działają jeszcze tak jak powinny wszystkie opcje, więc pewnie trzeba będzie poczekać na wersję z pełnym numerem. Kolejnym krokiem będzie zaznaczenie właściwego języka w polu *DVD subtitles*. Kiedy wszystko jest już wybrane należy kliknąć *FlasK this DVD*.

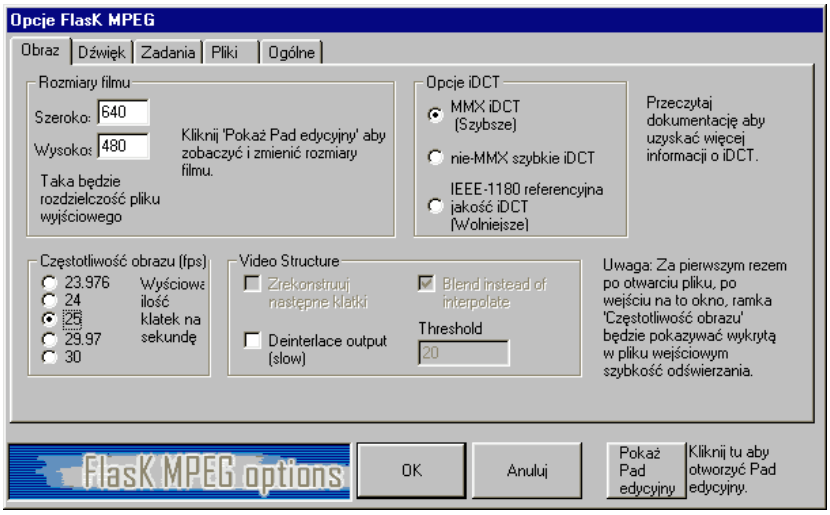
Nieco inaczej wygląda cała sprawa, jeśli pirat zgrał tylko VOB-y. Wówczas wybiera on *File/Open DVD File,* zaznacza pierwszego VOB-a (czyli np. *vts_01_1.vob*), a Flas KMPEG DVD Selector automatycznie znajdzie pozostałe pliki filmu i potraktuje je jak jeden duży plik (potwierdzi to wyświetlając planszę taką jak na poniższym rysunku).



Teraz wystarczy nacisnąć *OK*. Wówczas może się pojawić dodatkowe okno,

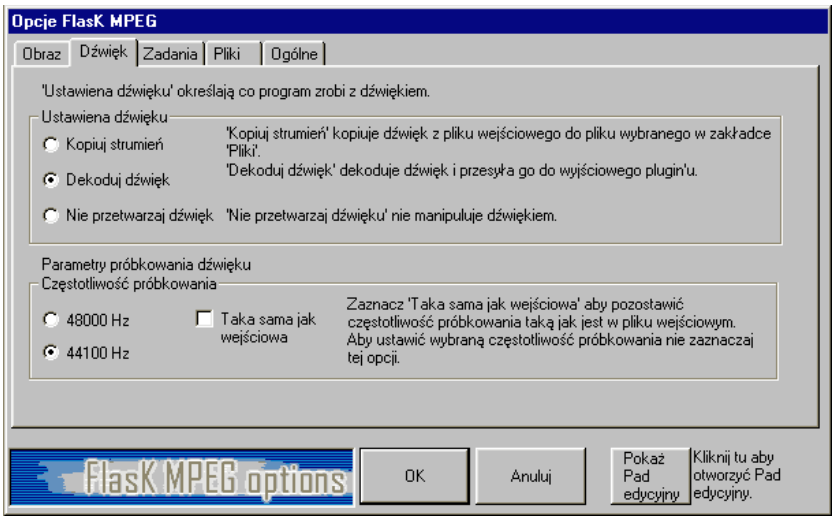


w którym należy wybrać film lub ścieżkę dźwiękową (ale tylko w wypadku, kiedy VOB zawiera ich więcej niż jedną). Dźwięk w języku angielskim ma zazwyczaj kod 0x80. I tak można się zająć ustawianiem opcji. Na początku trzeba wybrać *Opcje/Ogólne ustawienia/Obraz*. Pojawia się wówczas okno takie jak na rysunku.



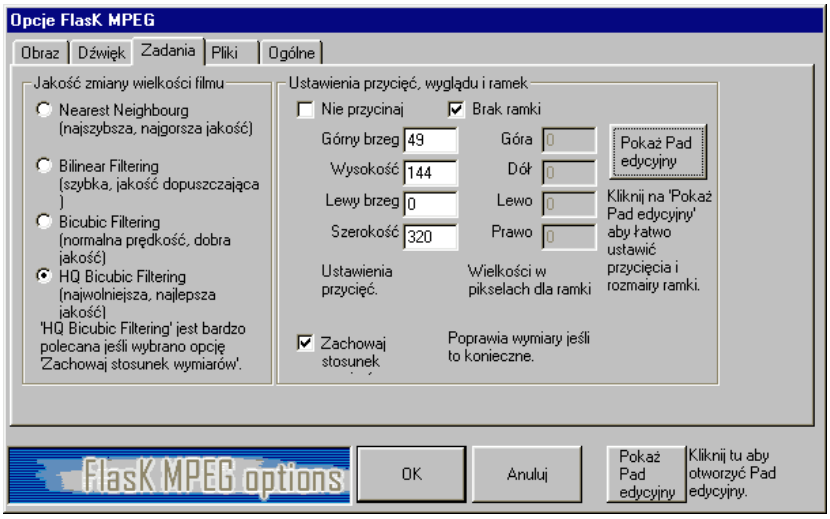
Należy w nim ustawić wynikową rozdzielczość filmu. Częstotliwość obrazu w zasadzie jest określana automatycznie, jednak najlepiej ją sprawdzić. W przypadku regionu 2. będzie to najczęściej 25 klatek na sekundę (ewentualnie 24 klatki). Pozostałe opcje najlepiej pozostawić bez zmian. Trzeba pamiętać, że im większa jest rozdzielczość tym lepiej, ale większe są także wymagania w stosunku do procesora i karty graficznej. Filmy przegrane w rozdzielczości 640x480 da się oglądać w zasadzie dopiero na Celeronie powyżej 433 (na słabszych tylko z bardzo dobrą grafiką).

Druga zakładka to *Dźwięk*.



Tu zaznacza się, czy dźwięk ma być dekodowany, kopiowany do osobnego pliku, czy zupełnie pomijany. Na początku lepiej nie łączyć dźwięku z wygenerowanym *AVI*, więc dobrze jest wybrać *Dekoduj dźwięk*. Częstotliwość próbkowania uzależniona jest od tego, czy dźwięk będzie kodowany do *MP3* czy do *WMA*/ DivX) Audio. W pierwszym przypadku można więc zaznaczyć *Taka sama jak wejściowa*, co w praktyce oznacza najczęściej 48 000 Hz. W przypadku WMA/DivX Audio trzeba ustawić częstotliwość 41 000 Hz.

Kolejna zakładka to *Zadania*.

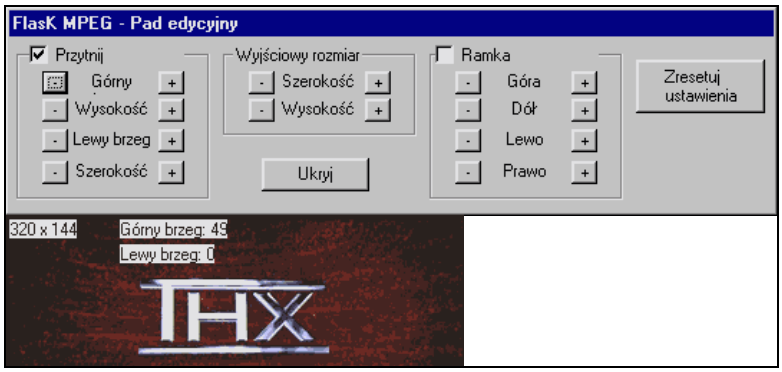


Tutaj ustawia jakość skalowania obrazu. Można ją pozostawić bez zmian. Po prawej stronie dostępne są opcje dotyczące rzeczywistej rozdzielczości obrazu. Filmy w 2. regionie dostępne są w zasadzie w trzech wielkościach (a dokładnie w trzech pro-

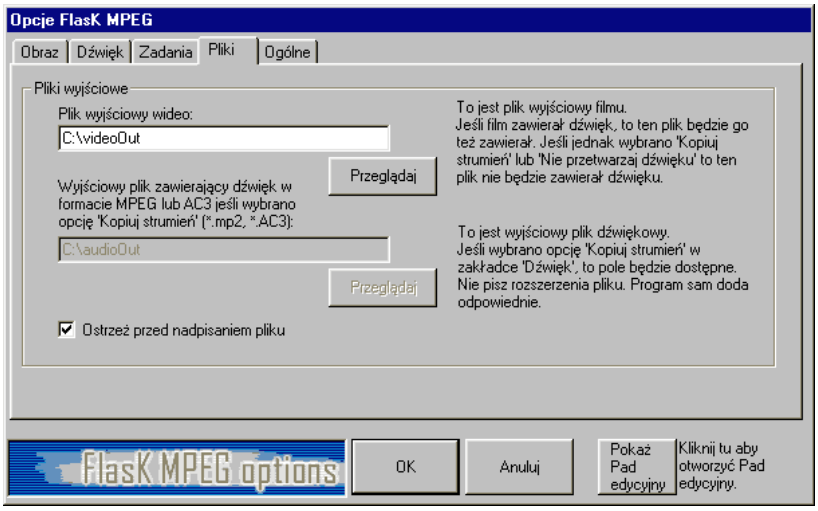
porcjach szerokości obrazu do jego wysokości). Chodzi tutaj o tzw. „aspect ratio". Mamy więc proporcje: 4/3, 16/9 i 24/10.

Na rysunku przedstawiony został kadr filmu 25/10, który będzie wyświetlany na ekranie 4/3, czyli na monitorze lub zwykłym telewizorze (czarne pasy przemalowane zostały na zielono). Oczywiście kodowanie takiego obrazu jest czystym marnotrawstwem czasu i miejsca na dysku, więc FlasK umożliwia wycięcie zbędnych fragmentów obrazu (odtwarzacze automatycznie dodadzą te pasy podczas odtwarzania nie zmieniając jego proporcji). Po korekcie obraz zakodowany będzie więc wyglądał tak jak na rysunku.

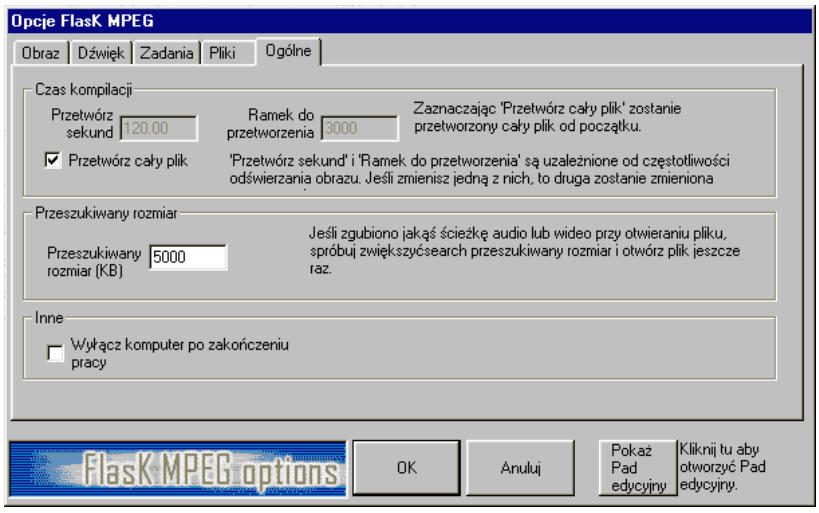
W przypadku filmu o proporcjach 16/9 pasy są oczywiście mniejsze, ale ich także można się pozbyć. Wycinanie to ma tę dodatkową zaletę, że zmniejsza zapotrzebowanie na moc procesora przy odtwarzaniu. Są trzy formaty: 4/3, 16/9 i 25/10 (innym oznaczeniem stosowanym na opakowaniach płyt DVD jest odpowiednio: 1,33:1, 1,78:1 i 2,35:1). W przypadku 4/3 nie można niczego zmienić, więc należy zaznaczyć opcję *Nie przycinaj*. Dla filmu 16/9 (zakładając, że ma on mieć rozdzielczość 640 x 480 pikseli) trzeba wyłączyć tę opcję i w polu *Górny brzeg* wpisać 64, a *Wysokość* określić jako 352. Dla filmu 25/10 te wartości będą się przedstawiały odpowiednio — 98 i 288. Oczywiście trzeba je traktować orientacyjnie. Do precyzyjnego ustawiania służy *Pad edycyjny*, który dostępny jest pod przyciskiem *Pokaż pad edycyjny*). Wygląda on tak jak na rysunku.



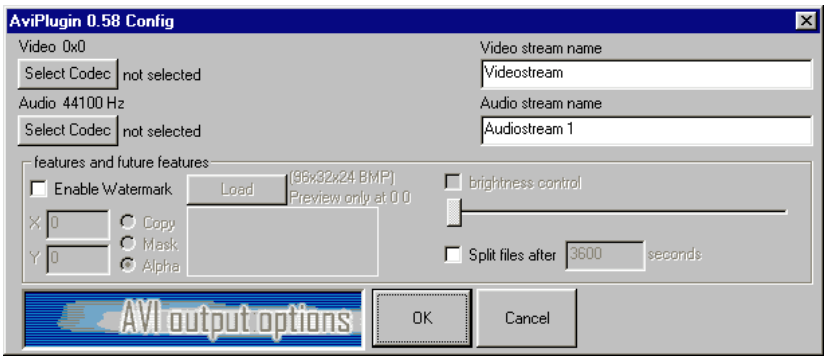
Po zamknięciu *Pada edycyjnego*, należy przejść do zakładki *Pliki*.



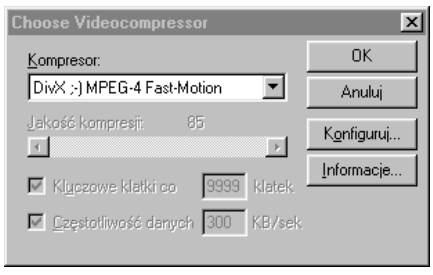
Tutaj trzeba podać nazwę i położenie pliku z wygenerowanym filmem i dźwiękiem (jeśli zamiast dekodowania pirat zdecydował się na kopiowanie). Warto także zaznaczyć opcję zabezpieczającą przed przypadkowym nadpisaniem pliku. Kolejnym krokiem jest przejście do ostatniej zakładki w tym oknie — *Ogólne*.



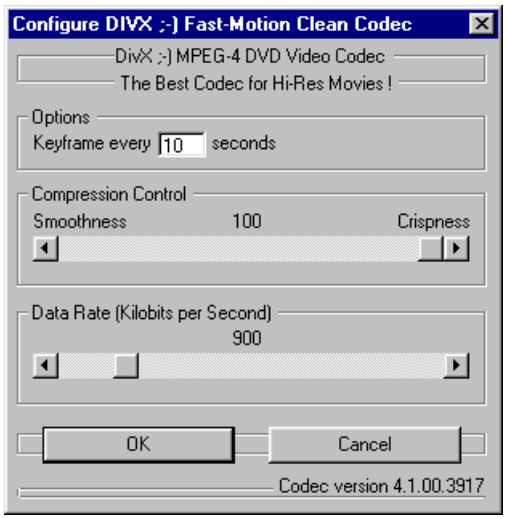
Tutaj w zasadzie nic nie trzeba zmieniać. Opcje (od góry) dotyczą: zgrywania x sekund lub x klatek filmu, obszaru przeszukiwania VOB-a i automatycznego wyłączania komputera po zakończeniu kodowania (komputer zostanie wyłączony, jeśli pakowanie zostanie przerwane). Kiedy zostały już ustawione wszystkie opcje, czas wybrać kodeki do obrazu i dźwięku (czyli formaty zapisu wewnątrz pliku *AVI)*. Wyboru dokonujemy po zaznaczeniu w menu *Opcje/Opcje formatu wyjsciowego*. Pojawi się wówczas takie okno jak na rysunku.



Kodek obrazu można wybrać klikając górny przycisk *Select Codek*. Wtedy pojawi się okno, takie jak przedstawiono na rysunku.



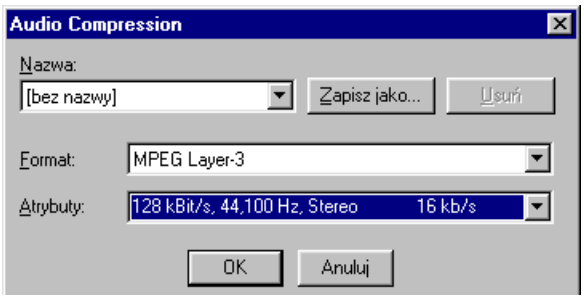
Wybiera oczywiście *DivX MPEG-4* i w zależności od rodzaju pakowanego filmu — *Fast* lub *Low-Motion*. W zasadzie nie ma aż tak dużej różnicy między tymi kodekami. *Low-Motion* nadaje się lepiej do filmów pozbawionych szybkich scen akcji, ale za to wolne sceny wyglądają dobrze. Pliki uzyskiwane przy użyciu kodeka *Low-Motion* są zazwyczaj znacznie większe od generowanych przez *Fast* i wymagają do płynnego odtwarzania nieco silniejszego komputera. Po wybraniu kodeka pirat musi zaznaczyć opcję *Konfiguracja*.



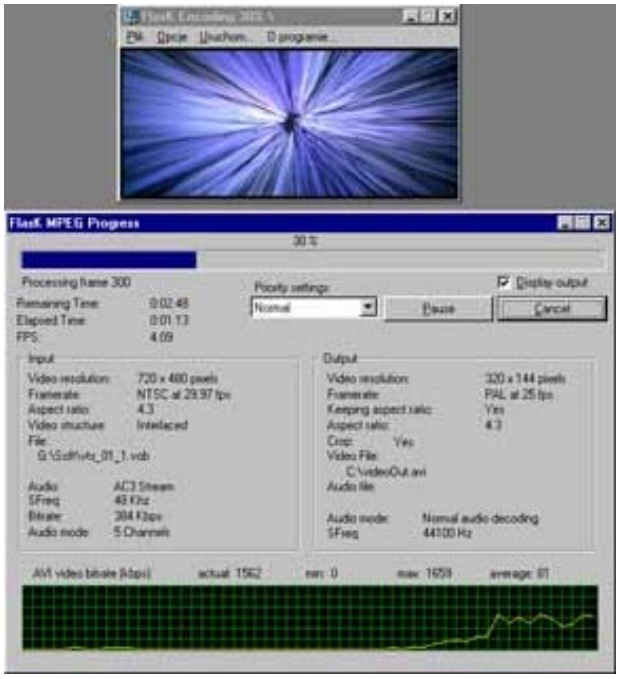
Jej możliwości są następujące (od góry): *Keyframe every x seconds* — określa, co ile sekund należy generować klatkę kluczową (najlepiej niczego tu nie zmieniać). Niżej znajduje się *Compression Control,* do której również nie należy wprowadzać żadnych zmian. Na dole ukryta jest najważniejsza opcja — *Data rate*. Od jej ustawienia zależy zarówno jakość filmu, jak i jego wielkość. Parametrem tym definiujemy, ile ma zajmować jedna sekunda filmu.

Oczywiście im większa wartość, tym lepsza jakość, ale także więcej megabajtów. W określaniu tej wielkości z pomocą przychodzą różne programy ustalające tę wartość za nas. Podobno najbardziej wiarygodne wyniki uzyskuje się z „dvd2 mpeg4 bitrate calculator", którego w całej okazałości można podziwiać na poniższym rysunku.

W górnym oknie pirat wpisuje zwykle długość filmu w minutach, niżej bitrate dźwięku, trzecie okno dotyczy kilku ścieżek dźwiękowych (czyli należy zostawić), a w ostatnie — planowanej wielkość pliku (czyli w przypadku 1 płyty CDR 650 lub 700). W dolnym oknie powinien pojawić się właściwy bitrate. Nie wszystko jednak jest takie proste. DivX to format o zmiennym bitrate'cie, co oznacza, że jeśli nic się nie dzieje na ekranie to prawie nic nie jest zapisywane na dysku. Mimo że wyniki tego programu są najbliższe prawdzie, w przypadku kodeka *Fast* można spokojnie dodać jeszcze 50-100, a film i tak okaże się mniejszy niż w założeniu. Dalej pirat wpisuje bitrate, klika dwa razy *OK* i „bierze się" za kodowanie dźwięku. W tym celu klika przycisk *Select Codek*.



I tutaj ma nieco większe możliwości wyboru. Może użyć albo *MPEG Layer—3* (popularny *MP3* dysponujący szeroką gamą bitrate'ów i kodujący w częstotliwości 48 000Hz), albo posłużyć się *DivX Audio* (złamany WMA z jednym tylko działającym ustawieniem: *64 kbps*, *44 kHz*, *stereo for DivX*, *8kb/s* w 44 100 Hz, który przy nieznacznie gorszej jakości dźwięku jest o połowę mniejszy od bitrate'a MP3-128 kbps i dodatkowo koduje do 6 razy szybciej). Pirat wybiera, klika *OK*. W oknie *AviPlugin'a* może jeszcze ustawić opcję nagrywania na kodowany obraz swojego loga. Znowu klika *OK* i w ten sposób doszedł do końca konfiguracji programu FlasK. Teraz wystarczy, że wybierze *Uruchom.../Konwersję* i podziwia wykonywane właśnie kodowanie.



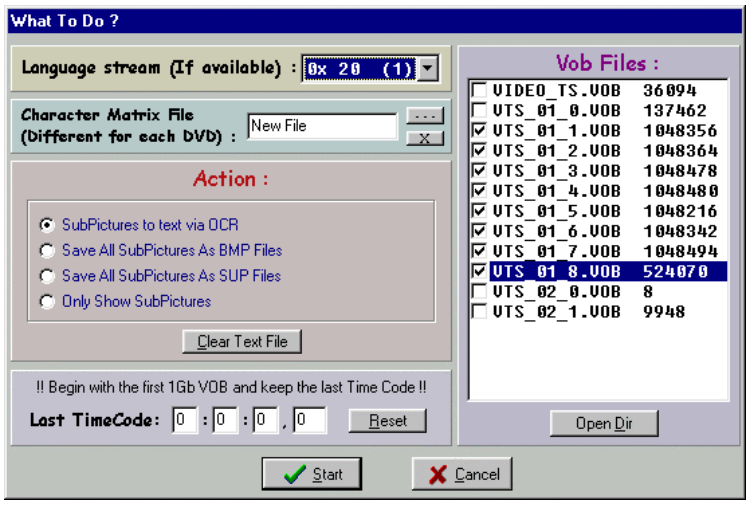
Powiększenie po klknięciu

Często jeszcze pirat wyłącza podgląd (*Display output*) i przyspiesza tym sposobem kodowanie o około 0,5 klatki na sekundę. W oknie tym można wyczytać wiele innych ciekawych informacji (przewidywany czas zakończenia, rozdzielczość, częstotliwość obrazu, aktualny, średni i największy bitrate). A po kilku czy kilkunastu godzinach na dysku pirata pojawi się gotowy film w formacie DivX! Teraz spokojnie może przejść do następnego etapu pirackiego procederu, czyli do przygotowania odpowiednich napisów.

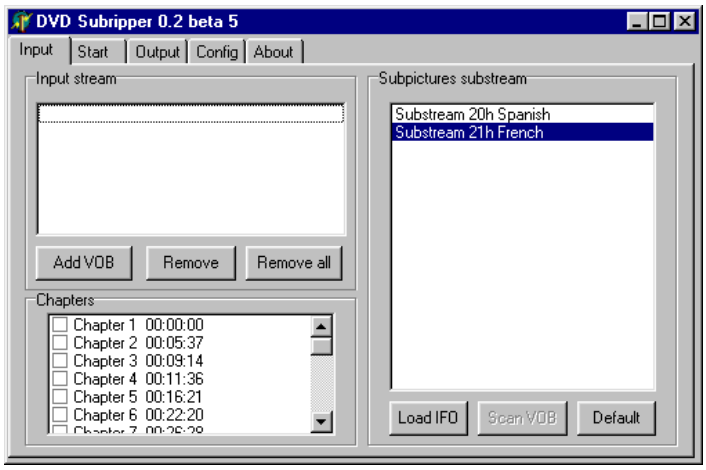
Przygotowywanie napisów

Istnieje kilka ciekawych programów do ripowania (wyciągania) napisów z plików *VOB*, jednak chyba najlepszym (powodującym najmniej błędów w tekście i zachowującym prawidłowe kody czasowe) jest program SubRip. Dobry pirat ma go na pewno. Uruchamia zatem SubRipa i wybiera z menu opcję *Open Vob(s)*. Pojawi się takie okno jak na rysunku na następnej stronie.

Wybiera *Open Dir* i wskazuje katalog, w którym znajdują się pliki *VOB* z filmem. Następnie w powyższym oknie zaznacza „ptaszkami" pliki, z których chce wyciągnąć tekst. Opis nazewnictwa plików na płytach DVD znajduje się w opisie DeCSS-a. Najlepiej zachować takie zaznaczenia jak powyżej.



Następnie pod *Language stream (If avaliable)* pirat musi wybrać język, który ma być wyciągnięty z pliku. Tutaj musi wiedzieć, jaki kod ma język, który chce wyciągnąć. Można próbować zrobić to losowo, jednak należy pamiętać, że w VOB-ie mogą znajdować się aż 32 języki, a zmiana języka wymaga użycia kombinacji *Ctrl-Alt-Del, co wiąże się z* „zabiciem" programu. Kod łatwo można sprawdzić w innym programie — DVD Subripper. Wystarczy uruchomić program i nacisnąć przycisk *Load IFO*, a później wybrać plik (najczęściej będzie to *VTS_01_0.IFO), by* pojawił się w oknie spis wszystkich języków zawartych w VOB-ach wraz z ich kodami jak widać na rysunku poniżej.

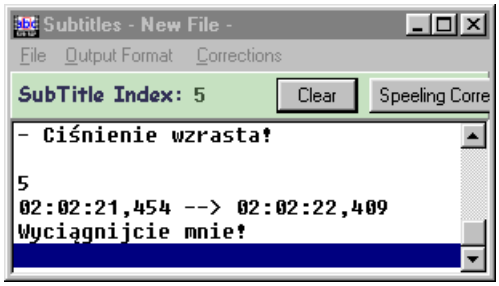


Teraz wystarczy, że pirat wybierze ten kod w SubRipie i gotowe. Opcji *Character Matrix File* lepiej jest nie zmieniać. Plik „Matrix" zawiera definicje znaków. Ponieważ na różnych filmach używane są różne czcionki o różnych wielkościach, więc w praktyce matryca dotyczy tylko jednego filmu. Następnie w polu *Action* pozostawiamy „*SubPictures to text via OCR*", czyli „zamiana obrazków zawierających napisy na tekst". Pozostałe opcje nie są już potrzebne. Istnieje możliwość

zmiany czasu, od którego zaczyna się ripowanie. Przydatne jest, gdy pirat z góry planuje podział filmu na dwie płyty DVD. Jeśli już wszystko będzie ustawione, to można przejść do właściwego ripowania. Wystarczy kliknąć *Start*. Program zacznie przeszukiwać VOB-a i kiedy znajdzie pierwszy napis, pojawi się okno (w tym momencie widać, czy wybrał właściwy kod języka). Dalej pirat wybiera właściwy kolor, który będzie następnie modyfikowany. Napis musi być biały na czarnym tle.

Następnie naciska *OK*. Pojawia się następne okno, w którym musi „powiedzieć" programowi, jaką literkę wyświetla w czerwonej obwódce. W poniższym przykładzie jest to „p". W ten sposób program będzie się pytał o każdą kolejną literę (tylko raz), aż będzie znał wszystkie. Ponieważ rozpoznawanie odbywa się na zasadzie porównywania wzorów graficznych, program będzie pytał za każdym razem, kiedy znajdzie nieznany wzorzec. Czasami litery się sklejają i wtedy trzeba wpisać np. „dyn".

Pirat wpisuje zatem „p" i naciska *Enter*. I to wszystko. Kiedy program zna już większość liter, to działa samodzielnie i wtedy pirat już tylko podziwia linie z tekstem wyskakujące oknie przedstawionym na rysunku.



Kiedy program obrobi już wszystkie VOB-y, piratowi pozostaje jedynie zapisać macierz i plik z napisami. Robi się to wybierając z menu *File* opcję *Save as*.

W głównym oknie w menu *Character Matrix* pod pozycją *Save Character Matrix File* pirat zapisuje macierz znaków.

Zawsze może się zdarzyć, że trzeba będzie powtórzyć ripowanie lub zgrywać napisy z filmu z identycznymi czcionkami. Kiedy pirat ma już napisy w pliku tekstowym (są one zapisane w dość nieczytelnym formacie, z którego korzysta chyba tylko jeden program — SubPictures Viewer), musi je jeszcze przerobić na jakiś bardziej przydatny format. W chwili obecnej najpopularniejszym formatem jest format playera MicroDVD, który jest jednocześnie najlepszym odtwarzaczem wszelkich filmów. W tym momencie z pomocą przychodzi program SubConvert, który przetwarza napisy.

Jego obsługa jest prosta. W polu *SubRip file* wybiera się świeżo zapisany plik tekstowy (nie matrycę) i ustawia właściwy *Framerate*, czyli ilość klatek wyświetlanych na sekundę (musi być zgodna z ustawieniem w FlasK, bo inaczej napisy nie będą wyświetlane we właściwych momentach). Właśnie w takich przypadkach przydają się opcje *Add this time to each subtitle* — czyli opóźnienie wyświetlania napisu, jak i *Make every hour longer by* — czyli niech każda godzina będzie dłuższa o... Kiedy więc pirat ustawi już właściwy *Framerate,* może kliknąć *Save* i już prawie gotowe. Dlaczego prawie? Ponieważ ripowanie tekstu jest nadal dalekie od doskonałości (np. zdarza się, że spacje pojawiają się tam, gdzie ich być nie powinno). Największym jednak błędem jest rozpoznawanie dużej litery I (i) jako l (L). Więc po zakończeniu ripowania pirat przegląda plik tekstowy w jakimś edytorze i poprawia zauważone błędy. Kiedy już poprawi tekst przechodzi do najprzyjemniejszej części piractwa, czyli oglądania gotowego filmu.

Oglądanie gotowego filmu w formacie DivX

Jest wiele różnych programów do odtwarzania filmów z napisami, jednak jak na razie bezkonkurencyjny pod względem jakości obrazu, wyświetlania napisów i ogólnej obsługi jest Micro DVD Player.

Wygląd tego programu jest wzorowany na odtwarzaczu DVD-PowerDVD Player. Jeśli pirat chce szybko zobaczyć efekty kodowania (z napisami) wystarczy, że kliknie przycisk *c* i kolejno wybierze — plik z filmem, plik z dźwiękiem (czyli ten sam) i plik tekstowy z napisami. Napisy pojawią się dopiero po przejściu do oglądania na pełnym ekranie (przycisk *f*). Czasami trzeba je jeszcze dodatkowo włączyć przyciskiem *d*. Nieraz zdarza się też, że obraz podczas oglądania na pełnym ekranie dziwnie się zatrzyma. Trzeba wówczas wywołac opcje (ikona z młotkiem po prawej stronie) i w części dotyczącej napisów (*Subtitles)* wyłączyć *Transparent Subtitles*. Jeśli film odtwarza się prawidłowo, napisy pojawiają się we właściwym momencie,

a film zmieści się na płycie, pirat może już uruchomić nagrywarkę. Oczywiście najlepiej jest, gdy film będzie startował automatycznie po włożeniu płyty do napędu, a płyta będzie zawierała wszystkie programy.

Wiele z zamieszczonych tu informacji zaczerpniętych zostało z witryn internetowych, takich jak na przykład: *http://www.republika.pl/robert_n/* lub *http://www.ftpdvd.so.pl.*

Epilog

„Nie ma nic tak odległego,
by było poza naszym zasięgiem,
ani tak ukrytego,
by nie dało się odkryć.”
Kartezjusz

„Jestem hakerem — cybernetycznym żołnierzem. Uważam, że granice należy przekraczać, zapory omijać, a tajemnice odkrywać. Nie robię tego dla zabawy, robię to dla poczucia, że przeskakując płoty i bariery rozstawione na szerokich, bezkresnych polach elektronicznej wiedzy, jak niegdysiejszy jeździec spełniam swoją od Boga daną wolność, której nikt nie ma prawa mi odebrać. W tym poczuciu potrafię odnaleźć godność i moją drugą tożsamość. Zdobywając dostęp do mocno strzeżonych tajemnic doznaję uczucia, jakiego jeszcze nigdy nie doznałem. Potrafię udowodnić, że jestem sprytniejszy od wszystkich jajogłowych z rządowych i prywatnych instytutów dla geniuszy. Zostałem wciągnięty w komputerowy Panteon. Zostałem zepchnięty na boczny tor i uzależniony od działającego jak narkotyk dostępu do informacji. Jak upiór wypijam potajemnie informację i czas transmisyjny z arterii wielkich korporacji i sieci komputerowych. I właśnie wtedy korporacje i rządy zaczęły na mnie polować. A — że polowanie było, jest i będzie trudne i kosztuje olbrzymie pieniądze, których wydatkowanie trzeba jakoś uzasadnić — przedstawiono mnie społeczeństwu i mediom jako jeźdźca atomowej apokalipsy, szpiega Imperium Zła, przestępcę groźniejszego od wszystkich mafiozów razem wziętych. A wszystko dlatego, że jestem hakerem...”

Głównym celem hakerów jest przynależność do elity. Każdy z nich chce wejść na najwyższy szczebel, ponieważ wejście tam daje siłę i potęgę. Ekonomia informacyjna rozwija się. Hakerzy handlują informacjami w nadziei zdobycia jeszcze większej ich ilości i dostania się do elity.

Haker zajmuje się swym niecnym procederem z różnych powodów. Warto jednak pamiętać, że hakerzy dźwigają cały bagaż wiedzy. Nie wszyscy są do siebie podobni, wielu z nich robi to dla prestiżu, wielu dla intelektualnej sprawności, a jeszcze inni dla przyczyn, które trudno sobie wyobrazić i zaakceptować. Niektórzy są bierni, ale dokonują innych zaskakujących czynów w sposób bardzo widowiskowy. Inni często żartobliwie mówią, że hakują dla zdobycia pięknych kobiet, a niektórzy robią to dla swojego kraju z pobudek patriotycznych. Czasem porównują to do gry sportowej, która powoduje zdrową rywalizacje i wydziela odpowiednią dawkę adrenaliny.

Ważne jest, aby rozumieć, że obok uniwersalnych przyczyn, każdy haker posiada własną, indywidualną motywację. Technologia komputerowa przyspiesza ludzką komunikację i teraz informacja może podróżować z szybkością światła. Hakerzy na końcach swoich palców posiadają siłę szybkości. Mają więc świadomość, że dzięki tym nieprzeciętnym umiejętnościom stoją ponad innymi ludźmi.

Koniec