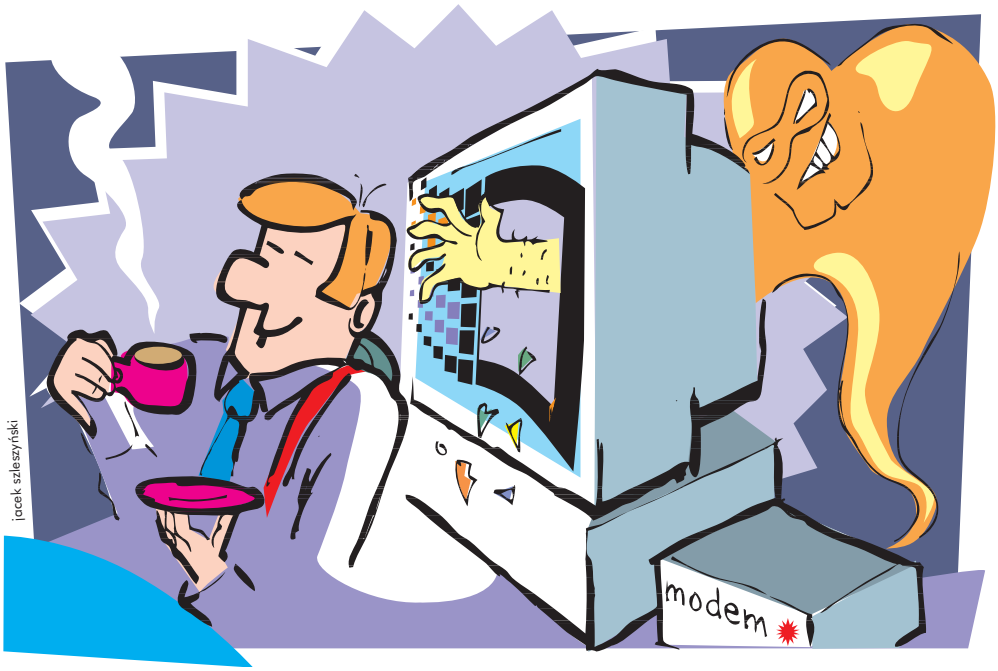


jacek szleszyński

Stan zagrożenia

Od pewnego czasu nie ustają dyskusje na temat bezpieczeństwa, a raczej ryzyka związanego z surfowaniem w Internecie z wykorzystaniem przeglądarek WWW. Niewiele osób zdaje sobie sprawę, że równie niebezpieczne, a może nawet bardziej, są mechanizmy sieciowe Windows 95 i NT.

Nie kończące się spory o bezpieczeństwo żeglowania po bezkresnych „wodach" Sieci koncentrują się zazwyczaj na zagrożeniu ze strony obiektów ActiveX (CHIP 6/97, s. 166), programów w języku Java czy JavaScript, błędach w przeglądarkach WWW i dodatkach do nich – plug-inach. Przytłaczająca większość użytkowników Internetu nie domyśla się nawet, że np. odwiedzając odpowiednio przygotowaną stronę WWW, pozwala na przechwycenie nazwy swojego konta sieciowego oraz używanego hasła!

W czasach, kiedy firmy Microsoft i IBM współpracowały przy tworzeniu oprogramowania sieciowego, opracowano protokół transmisji SMB (Server Message Block) bazujący na wykorzystywanym w Internecie TCP/IP i odpowiedzialny za dostęp do zasobów dyskowych i drukarek. Zaprojektowano go z myślą o sieciach opartych na NetBIOS-ie (komputery w nich pracujące z założenia nie miały komunikować się z maszynami spoza tej sieci), choć obecnie jest on używany przez Windows 95 i NT w przypadku połączeń wykorzystujących TCP/IP i IPX. Ten ostatni to podstawowy, a do niedawna jedyny, protokół sieciowy wykorzystywany w systemach NetWare firmy Novell.

Za pośrednictwem protokołu SMB serwer WWW może „skłonić" przeglądarkę WWW do identyfikacji, polegającej na podaniu przez nią nazwy użytkownika oraz hasła zabezpieczającego jego konto. W przypadku Windows 95 hasło może zostać przechwycone w postaci jawnej (!), a w NT zaszyfrowanej. Dotyczy to zarówno osób posługujących się *Internet Explorerem*, jak i *Netscape Navigatorem*, ale ten ostatni wydaje się mniej „podatny" na przekazywanie informacji o lokalnym komputerze.

Najgorsze jest to, że użytkownik nie zdaje sobie z tego sprawy, ponieważ proces autoryzacji przebiega w całości bez jego udziału. Na pocieszenie można dodać, że Microsoft pracuje już nad rozwiązaniem powyższego problemu i w najbliższym czasie możemy spodziewać się uaktualnienia systemu. Udostępniony niedawno *Service Pack 3* dla Windows NT 4.0 nie rozwiązuje opisanego błędu.

Dziurawe sieci

Użytkownikom pracującym w sieciach NetWare i przechowującym wszystkie ważne dane na serwerze może się wydawać, że zagrożenie ich nie dotyczy. Pomijając możliwość zainfekowania wirusem dysku lokalnego, istnieje znacznie większe niebezpieczeństwo. Większość osób – dla ułatwienia sobie życia – posiada to samo hasło na koncie sieciowym i w Windows. Dzięki temu, po przechwyceniu kodu dostępu z „95" dane z serwera „stoją otworem" przed hackerem czy sprytnym administratorem WWW.

Problem przechwytywania haseł łatwo rozwiązać w firmach podłączonych do Internetu poprzez router (urządzenie łączące sieć lokalną z Internetem). Wystarczy bowiem „nie wypuszczać" na zewnątrz pakietów z danymi zawierających nazwę i hasło użytkownika. Nie zabezpieczy nas to jednak przed włamywaczem pracującym w tej samej sieci lokalnej.

Najlepszym rozwiązaniem wykorzystywanym do odseparowania sieci lokalnej od Internetu jest tzw. zapora ogniowa (ang. firewall). To dedykowane oprogramowanie (czasem instalowane na osobnym komputerze), służy do filtrowania pakietów z danymi nadchodzących z Sieci w taki sposób, że do sieci za firewallem „dostają" się tylko ściśle określone przez administratora informacje (np. pakiety spod określonych adresów czy kierowane do konkretnych serwisów internetowych). Niestety, software ten znacznie obniża wydajność sieci.

ActiveX i Java(Script)

Technologia ActiveX i związane z jej użyciem ryzyko zostały obszernie opisane na łamach CHIP-a 6/97, s. 166. Przypomnimy tylko, że praktycznie wszystko czego dokonać można za pomocą klawiatury i myszy na lokalnej maszynie, daje się zrobić zdalnie – najczęściej bez naszej wiedzy – przez wczytanie odpowiednio spreparowanej strony WWW, zawierającej odpowiednią kontrolkę ActiveX.

W tym miejscu użytkownikom przyda się zapewne wskazówka, która pozwoli zwiększyć bezpieczeństwo nie rezygnując z dobrodziejstw nowej technologii, przynajmniej w „okienkach" NT. O ile całkowite uniknięcie zagrożenia wynikającego z korzystania z ActiveX w Windows 95

Zasady bezpieczeństwa

Zagrożenia „czyhającego” na użytkowników w Internecie nie da się praktycznie uniknąć, można jedynie znacznie je ograniczyć, stosując się do przedstawionych poniżej zasad:

- Jeżeli pracujesz w sieci, spytaj jej administratora w jaki sposób i czy w ogóle została zabezpieczona (firewall, filtrowanie pakietów itp.).
- Używaj innego hasła w sieci lokalnej i Windows 95/NT.
- W Windows NT załóż sobie osobne konto, przeznaczone tylko do surfowania po Internecie (z minimalnym poziomem uprawnień).
- W używanej przez Ciebie przeglądarce WWW wyłącz obsługę programów w językach Java i JavaScript.
- W Internet Explorerze ustaw poziom bezpieczeństwa na najwyższy i nie testuj nieznanych Ci ActiveX-ów, poczekaj aż zrobią to inni. Pamiętaj, że nawet tzw. bezpieczne (posiadające certyfikaty) kontrolki ActiveX mogą wyrządzić wiele szkód na Twoim komputerze.
- Przeglądaj pliki w formacie Acrobat Readera za pomocą *GSView* albo *Adobe Acrobata* w wersji nowszej niż *3.0*.
- Sprawdzaj, czy pobrane z Internetu lub przysłane Ci pocztą elektroniczną pliki nie zawierają wirusów. Zrób to zanim je uruchomisz albo zaczniesz przeglądać.
- Poufne dane przesyłaj w postaci zaszyfrowanej.
- Sprawdzaj czy dokumenty edytorów tekstu i arkuszy kalkulacyjnych nie zawierają wirusów typu makro.
- Czytaj informacje prasowe i listy dyskusyjne zawierające informacje na temat błędów i „dziur” w systemach operacyjnych, protokołach sieciowych, przeglądarkach WWW oraz plug-inach.

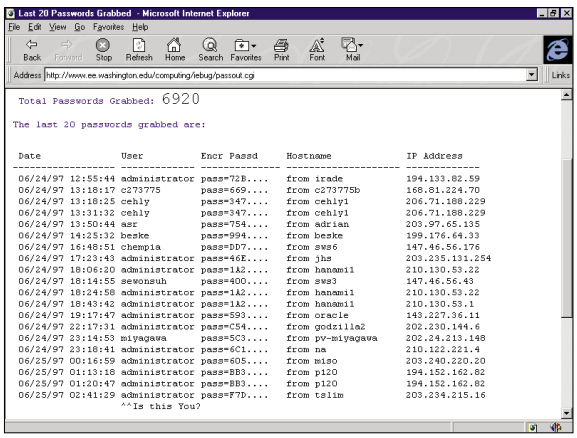
wydaje się niemożliwe, to w przypadku NT ograniczenie wspomnianego ryzyka jest dość proste. Wystarczy utworzyć nowe konto użytkownika z minimalnym zakresem praw dostępu. W opisanym przypadku rozmiar ewentualnych szkód zostanie ograniczony ramami uprawnień konta, z którego wykonywane było surfowanie po Sieci.

Mimo, że projektanci Javy od samego początku zadbali o bezpieczeństwo pracy w Sieci, nie dodając do specyfikacji języka mechanizmów pozwalających na dostęp do sieci i dysku lokalnego, to co jakiś czas powtarzają się sygnały o „destrukcyjnych atakach” programów w Javie. O ile nam wiadomo, wszystkie przypadki „agresji” opierały się na niedoskonałej implementacji mechanizmów bezpieczeństwa w przeglądarkach WWW. Zupełnie innym problemem jest niedoskonałość JVM (Java Virtual Machine) – modułu odpowiedzialnego za wykonywanie aplikacji w języku Java. Wprawdzie firma Sun twierdzi, że wykryta luka jest trudna do wykorzystania przez hackerów i nie ma większego znaczenia, to Microsoft prezentuje w tej sprawie odmienną opinię.

Kiepskie to jednak pocieszenie dla osób, które utraciły w ten sposób swoje dane. W celu zwiększenia bezpieczeństwa systemu operacyjnego powinno się więc wyłączyć w przeglądarce WWW obsługę aplikacji w językach Java i JavaScript, tylko że nie jest to rozwiązanie, którego byśmy oczekiwali.

Niebezpieczne przeglądarki WWW

Na stronie WWW *http://www.cybersnot.com/iebug.html* znajdują się przykłady, pokazujące jak z łatwością można wykorzystać błędy w zakresie bezpieczeństwa Internet Explorera 3.0(1). Jeżeli wykorzysta się fakt, że program ten używa plików o rozszerzeniach LNK i URL do uruchamiania programów, to wystarczy kliknięcie na „złośliwym” przycisku, znajdującym się stronie WWW, aby wystartować dowolny program z dysku użytkownika. Wprawdzie trzeba znać pełną ścieżkę dostępu do wywoływanej aplikacji, ale w przypadku programów będących częścią „95” nie sprawi to trudności (jak wielu użytkowników zmienia w czasie instalacji domyślną lokalizację katalogu „okienek” – **C:\WINDOWS**?). Opisana wada, podobnie jak usterka pozwalająca za pomocą odpowiedniego komponentu ActiveX na obniżenie poziomu bezpieczeństwa przeglądarki WWW Microsoftu, zostały usunięte w Internet Explorerze 3.02 i nie powinno się używać starszych wersji tego programu.



***http://www.ee.washington.edu/computing/iebug/passout.cgi* – oto przykład „inteligentnej” strony WWW, która podaje nam, jaki jest identyfikator naszego konta, adres IP i jakiego używamy hasła w Windows NT (w postaci zaszyfrowanej)**

Użytkownicy Netscape Navigatora, także powinni mieć się na baczności. Popularny plug-in *Shockwave*, wykorzystywany m.in. do tworzenia animacji na stronach WWW, zainstalowany w aplikacji firmy Netscape może być bowiem nadużywany do czytania dowolnych plików z dysku lokalnego i poczty elektronicznej. Co więcej, za pomocą tej aplikacji internetowy pirat jest w stanie uzyskać dostęp do stron WWW (także w sieciach Intranet), do przeglądania których ma prawo użytkownik. Ta ostatnia właściwość Shockwave’a dotyczy także współpracy z przeglądarką WWW Microsoftu.

Wszystkie wymienione błędy w bezpieczeństwie sieciowym zaobserwowano zarówno w Windows 95 i NT, jak i na komputerach Macintosh. Więcej na ten temat przeczytać można na stronie WWW *http://www.webcomics.com/shockwave*. Firma Macromedia sama poinformowała o niebezpieczeństwie i oferuje poprawioną wersję plug-ina, nazwaną *security-enhanced*, pod adresem *http://www.macromedia.com/shockwave/download*.

Złośliwa dokumentacja

Mało który użytkownik zdaje sobie sprawę, że czytając dokumentację w postaci elektronicznej, w formacie Adobe Acrobat, ryzykuje utratę części, a nawet całej zawartości dysku twardego. Alarmujące informacje na ten temat znaleźć można już od kilku miesięcy na łamach list dyskusyjnych (np. comp.text.pdf).

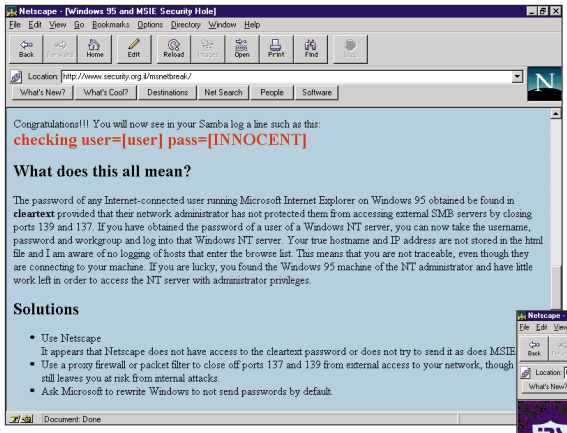
Zagrożenie wynika z faktu, że specyfikacja formatu Acrobat, pozwala na umieszczanie w plikach .PDF obiektów zdolnych do wywoływania poleceń systemu operacyjnego (np. **del**, **move**), a nawet uruchamiania programów! Możliwość „ataku” ze strony odpowiednio spreparowanego dokumentu jest dość wysoka, ponieważ format firmy Adobe stał się standardem zapisu dokumentacji w postaci elektronicznej, a darmowe przeglądarki plików PDF, np. *Acrobat Reader*, dostępne są dla większości systemów operacyjnych.

Niebezpieczeństwo dotyczy na razie wyłącznie użytkowników pracujących w Windows (3.1x, 95 i NT), ponieważ tylko z tego środowiska można w praktyce uruchamiać dowolne programy i wywoływać polecenia systemu operacyjnego

▶ 78

za pomocą obiektów w plikach PDF. Należy pamiętać, że potencjalny dywersant nie musi tworzyć nowego pliku w formacie Acrobat, ale może tak zmodyfikować istniejący, aby np. przyciski nawigacyjne zamiast powodować przejście do nowej strony, kasowały wybrane pliki albo formatowały dysk. Co więcej, dzięki możliwości wywoływania funkcji pozwalających na uruchamianie poleceń systemowych w momencie otwierania dokumentu, już sama próba odczytu plików Acrobata mogłaby prowadzić do tragedii.

Firma Adobe zapowiedziała nową wersję (*3.0.1*) Acrobata, która ma rozwiązać problem „nadużywania" plików PDF. Póki co lepiej korzystać z innych przeglądarek formatu Acrobat, np. *GSView 2.1* (*ftp://ftp.cs.wisc.edu/ghost/rjl/gsview21.zip*), w której nie zaimplementowano obsługi obiektów, zdolnych do wywoływania poleceń systemowych i zewnętrznych aplikacji.



http://www.security.org.il/msnetbreak – pod tym adresem użytkownicy Internet Explorera pracujący w Windows 95 mogą przeczytać o grożących im niebezpieczeństwach i metodach zabezpieczenia się przed atakiem z zewnątrz

Najnowsze informacje w języku polskim o niebezpieczeństwach związanych m.in. z surfowaniem po Internecie znaleźć można na stronie http://www.ibs.net.pl/

Inwazja wirusów

O komputerowych „szkodnikach" pisaliśmy już na łamach CHIP-a wielokrotnie (CHIP 5/96, s. 68 i 72, CHIP 5/97, s. 110). Przy opisywaniu problemów bezpieczeństwa w powiązaniu z Internetem nie sposób jednak pominąć nowych możliwości, jakie otwiera przed twórcami „mikrobów" Sieć. Mimo coraz powszechniejszego stosowania oprogramowania antywirusowego liczba infekcji stale rośnie. Wynika to tylko częściowo ze wzrostu liczby użytkowników komputerów. Rozprzestrzenianie się wirusów dzięki Internetowi stało się znacznie prostsze, a potencjalny zasięg infekcji ogranicza tylko liczba maszyn podłączonych do Sieci. Do „zarażenia" może dojść w wyniku odwiedzenia strony WWW i kliknięcia odpowiedniego przycisku, uruchomienia albo wczytania pobranego z serwera FTP pliku itp. Infekcje często wynikają bezpośrednio z braku wyobraźni i niskiego poziomu wiedzy o metodach rozprzestrzenienia się wirusów.

Wielokrotnie można spotkać się z przypadkami, kiedy użytkownik najpierw uruchamiał aplikację, a dopiero później weryfikował czy ściągnięty program nie jest zawirusowany. Inny przykład nonszalancji to kontrola plików w postaci „spakowanej", skanerem antywirusowym nie „rozumiejącym" użytego formatu kompresji. Ostatnimi czasy upowszechnił się jeszcze jeden przypadek lekkomyślności: otwieranie dokumentów, np. *Worda* i *Excela*, bez sprawdzenia czy nie zawierają one wirusa typu makro. Wspomniane „robaki" odpowiadają za największą liczbę infekcji wśród użytkowników Windows. Czy znacie kogoś kto sprawdza każdy plik pobrany albo przesłany do niego za pomocą poczty elektronicznej? Tylko taka osoba ma prawo czuć się bezpieczna.

Zupełnie inna kwestia, to skąd wziąć program antywirusowy nadążający za masowo pojawiającymi się wirusami, skoro codziennie odwiedzamy dziesiątki stron WWW, a na każdej z nich może czyhać niebezpieczeństwo. Zapewnienie sobie całkowitej ochrony nie jest możliwie, ale postępując zgodnie z zasadami zawartymi w artykułach o wirusach komputerowych (oraz w ramce na poprzedniej stronie *Zasady bezpieczeństwa*) możemy znacznie ograniczyć ryzyko infekcji i utraty danych. Niektórzy producenci oferują już programy antywirusowe, automatycznie uaktualniające bazy wirusów przez Internet (np. Symantec), ale nawet takie aplikacje nie zapewniają pełnego bezpieczeństwa. Zanim nowy wirus zostanie wykryty i dodany do bazy „szkodników" mijają dni, a nawet tygodnie.

Zagrożone dane

Ze względu na coraz częstsze przesyłanie strategicznych informacji przez Sieć popularne staje się szyfrowanie danych. Niestety, wielu użytkownikom wydaje się, że oferowane przez typowe aplikacje biurowe zabezpieczenie treści dokumentu hasłem, gwarantuje pełne bezpieczeństwo. Trudno o większą naiwność. W Internecie znaleźć można „łamacze" haseł do praktycznie wszystkich dokumentów utworzonych przez różne wersje typowych programów biurowych, np. Worda i Excela.

Podobnie przedstawia się bezpieczeństwo plików zaszyfrowanych popularnymi programami do kompresji danych, jak *ARJ* czy *PKZip*. W zależności od użytego klucza i rodzaju plików rozkodowanie danych przez dobrego hackera zajmuje zazwyczaj od kilkunastu minut do kilku godzin. Dostępne w Sieci „łamacze" skompresowanych zbiorów działają równie skutecznie, ale ze względu na mało „inteligentną" metodę postępowania potrzebują znacznie więcej czasu. Do przesyłania poufnych danych należy korzystać wyłącznie z narzędzi posługujących się nowoczesnymi algorytmami kodowania, np. PGP (Pretty Good Privacy).

Dylemat: ładniej czy bezpieczniej?

Każdy użytkownik, w szczególności pracujący w Windows, powinien odpowiedzieć sobie na następujące pytanie: co jest dla niego ważniejsze; bezpieczeństwo, a może wygoda i multimedia w czasie surfowania? Równocześnie trzeba zdawać sobie sprawę z tego, że zapewnienie całkowitej ochrony nie jest możliwe, chyba że zrezygnujemy całkowicie z usług Sieci. Nie wolno zapominać, że prędzej czy później znajdzie się hacker, który złamie najwymyślniejsze zabezpieczenia, odkryje kolejną lukę w przeglądarce WWW albo protokole sieciowym, dzięki czemu uzyska dostęp do twoich danych. Jedyne co można zrobić, to zmniejszyć zagrożenie stosując się do rad zamieszczanych w Internecie i niniejszym artykule.

Robert I. Bielecki