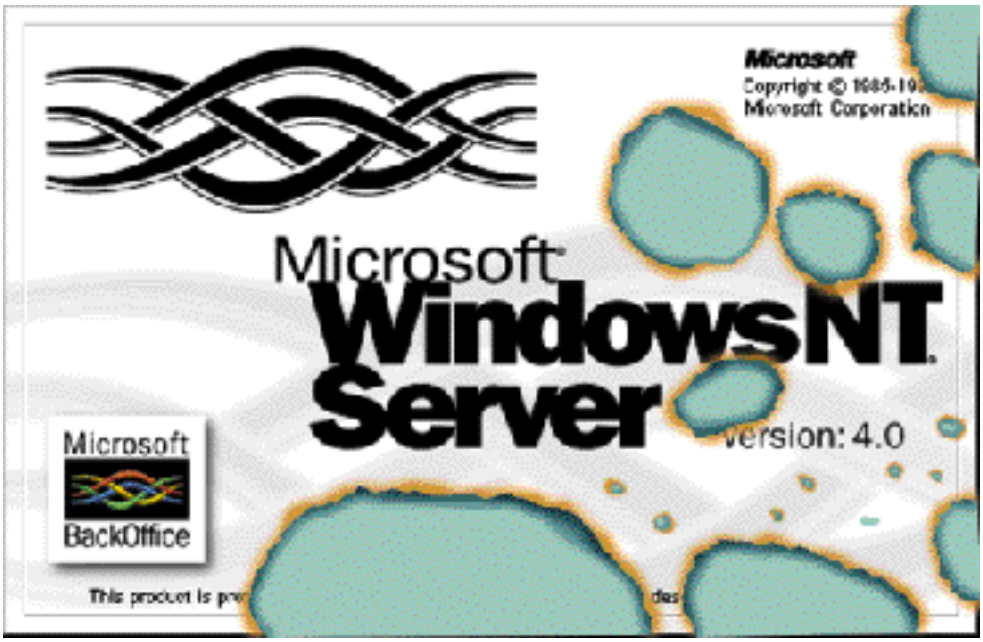

Zaradzić zarazie

Windows NT uważane jest za synonim bezpiecznego systemu. Jak dalece jednak wersja NT 4.0 odporna jest na ataki wirusów? Analizy i próby wykazują różne działanie systemu w zależności od typu wirusa. Jakie są mocne i słabe strony? Gdzie tkwią potencjalne źródła zagrożeń? Jakie środki profilaktyczne warto zastosować?

Ze względu na swoją architekturę system operacyjny Windows NT jest bardziej odporny na ataki wirusów komputerowych niż MS-DOS, Windows 3.1x czy Windows 95. Nie jest również w tej chwili znany żaden przykład 32-bitowego wirusa napisanego specjalnie dla Windows NT. Dlatego artykuł odnosi się głównie do starych znajomych z systemu DOS. Przypominamy różne typy wirusów, sposób w jaki atakują, ze szczególnym uwzględnieniem ich zachowania w systemie NT.

Fachowcy wiedzą, że odporność systemu zależy od mechanizmów stosowanych przez konkretnego wirusa. Przeprowadzane próby czy spekulacje miały na celu wykazanie, że istnieją generalne zależności dla różnych typów wirusów. Stwierdzenie, że wirusy typu makro mogą rozprzestrzeniać się na platformie Windows NT w takim samym stopniu, w jakim czynią to w innych systemach operacyjnych, nie wymaga dogłębnych studiów.

Windows NT najłatwiej zaatakować podczas startu

Ciągle jedną z bardziej rozpowszechnionych grup pod względem liczby infekcji są wirusy ładowania początkowego, które atakują MBR – Master Boot Record lub PBR – Partition Boot Record. Każda dyskietka posiada rekord wprowadzający (boot record). Zajmuje on pierwszy sektor na dyskietce i zawiera ważne dla systemu operacyjnego informacje, określające zawartość dyskietki. Znajduje się w nim program pierwotny, którego funkcją jest ładowanie systemu operacyjnego z dyskietki. Jeżeli komputer ładuje system operacyjny z napędu dyskietek, przeszukuje Master Boot Record i próbuje uruchomić zawarty w nim program. Częstym błędem popełnianym przez użytkowników jest pozostawianie dyskietek w napędzie po skończonej pracy. Daje to wirusom szansę wykorzystania ładowania początkowego do zarażenia komputera. W konsekwencji wirus zastępuje oryginalną procedurę inicjującą własnym programem pierwotnym. Umożliwia to wirusowi przejęcie kontroli nad komputerem zaraz po jego włączeniu. W następnej kolejności wirus może infekować dysk twardy, niszczyć dane, doprowadzać do zawieszania się systemu lub wywoływać inne efekty. Często wirus „przyczaja się", ładując system operacyjny, zaś niszczycielską działalność przeprowadza w późniejszym terminie.

Proces startowania systemu może być celem ataków wirusów MBR, ponieważ system NT nie posiada kontroli nad tym, co dzieje się z komputerem w pierwszej fazie uruchamiania. Ładowanie systemu z zainfekowanej dyskietki stanowi zatem potencjalne źródło infekcji MBR dysku twardego komputera za pomocą klasycznych technik infekowania. Zwiększa się liczba wirusów wykorzystujących tę drogę infekcji i należy oczekiwać dalszego jej wzrostu w przyszłości.

Interesujące jest stwierdzenie, jak przebiega proces ładowania początkowego pod NT z zainfekowanym MBR. Ponieważ w pierwszej fazie Windows NT jeszcze nie jest załadowany, wirus, który raz dostał się do MBR, może instalować się w tej fazie rezydentnie w pamięci. Jest on podobnie jak w DOS-ie startowany jako program w opcji real mode i posiada pełną kontrolę nad komputerem. Niektóre wirusy, jak np. Michelangelo albo Onehalf, mogą już na tym etapie oddziaływać destrukcyjnie na system NT.

Po instalacji wirusa następuje przekazanie dalszej kontroli oryginalnemu MBR, który z kolei oddziałuje na bootrecord systemu NT. W dalszej kolejności wywoływany jest program NT loader ładujący resztę systemu operacyjnego NT. Procesor przełączany jest w tryb protected mode i dodatkowo ładowane są sterowniki dysków NT, pracujące również w protected mode. Są one wykorzystywane do obsługi wszelkich

▶ 113

Drogi infekcji

Oto typowa sekwencja rozprzestrzeniania się wirusa ładowania początkowego, który zainfekował program pierwotny dyskietki:
1.komputer został włączony, względnie zresetowany
2.komputer stwierdził obecność dyskietki w napędzie dyskietek i w konsekwencji ładuje z dyskietki oraz startuje program pierwotny, który jest w tym przypadku programem wirusa
3.program pierwotny wirusa wykrywa pierwszy aktywny dysk twardy w komputerze i infekuje jego główny rekord wprowadzający (Master Boot Record – MBR), względnie jeden z jego logicznych rekordów (Partition Boot Record – PBR) aktywnej partycji
4.wirusowa procedura inicjująca instaluje się rezydentnie w pamięci
5.procedura ta ładuje kopię oryginalnego programu pierwotnego i uruchamia go
6.komputer startuje „normalnie"
7.wirus aktywny w pamięci infekuje kolejne dyskietki w miarę korzystania z napędu dyskietek.

funkcji dostępu do dysków. Oryginalne procedury BIOS-u włącznie z potencjalnie podłączonymi do nich wirusami nie są wykonywane podczas startu systemu. W konsekwencji wirus typu MBR nie jest w stanie rozprzestrzeniać się poprzez infekowanie dalszych dyskietek z chwilą przejęcia kontroli przez system NT.

Niektóre wirusy, np. ripper, posiadają zdolność podczepiania się w systemie DOS lub Windows 95 pod funkcje bezpośredniego dostępu do dysków twardych poprzez BIOS i manipulowania, względnie niszczenia danych w trakcie operacji dostępu do dysku. Dotyczy to także pierwszej fazy bootowania w systemie NT do chwili przejęcia kontroli przez sterowniki NT. Po przejęciu kontroli wirus nie ma szans dokonywania dalszych destrukcyjnych operacji.

Wirusy ładowania początkowego są mniej niebezpieczne

Wirusy ładowania początkowego posiadające funkcję stealth nie są w stanie funkcjonować po załadowaniu systemu NT, ponieważ wyłączany jest dostęp do wirusowego, rezydentnego programu obsługi dysku. Umożliwia to łatwe wykrycie tych wirusów, lecz nie zabezpiecza przed innymi zagrożeniami. Przykładem może być wirus typu stealth atakujący MBR, jakim jest wirus Monkey. Niszczy on tablicę partycji w zainfekowanym sektorze MBR. W efekcie, zainfekowany napęd może być niedostępny dla Windows NT. System ten, by określić dostępne napędy logiczne, wczytuje tablicę partycji za pomocą własnych sterowników. Ponieważ następuje to w protected mode, pomijany jest mechanizm obsługi dysku wirusa, który nie jest w stanie udostępnić informacji z zachowanej przez niego kopii oryginalnej tablicy partycji, tak jak to czyni w DOS-ie. Koniec końców NT wczytuje zniekształconą tablicę partycji i nie potrafi określić napędów logicznych.

Generalnie można powiedzieć, że dopóki wirus typu bootrecord nie manipuluje tablicą partycji lub nie posiada innych specjalnych efektów uruchamianych podczas procesu bootowania przed załadowaniem systemu NT, nie będzie miał wpływu na pracę tego systemu.

Typowe metody rozprzestrzeniania się wirusów atakujących PBR to bootowanie z zainfekowanej dyskietki albo uruchamianie programu-nośnika (konia trojańskiego) z poziomu DOS-a, który wpisuje wirus w sektor ładowania aktywnej partycji. Podobnie jak wirusy atakujące MBR, nie są zdolne do powielania się w systemie NT.

Okres od włączenia komputera do przejęcia kontroli przez system operacyjny NT stanowi jednak źródło potencjalnych niebezpieczeństw ze strony wirusów tego typu i należy liczyć się w przyszłości ze wzrostem liczby takich infekcji. Nie jest również wykluczone pojawienie się w przyszłości programów napisanych dla środowiska NT, które będą w stanie modyfikować zawartość PBR. Infekcje spowodowane przez atakujące PBR wirusy wieloczęściowe nie są wykluczone, o ile komputer poza NT może startować w innym systemie operacyjnym, np. DOS albo Windows 95.

W przypadku stosowania systemu opartego na FAT, jeżeli wirus zapisał oryginalny bootrecord na końcu dysku i nie podjął żadnych kroków zabezpieczających, rekord ten może zostać nadpisany przez Windows NT. Konsekwencją będzie zawieszenie się systemu podczas bootowania, ponieważ wirus nieodwołalnie będzie próbował załadować i uruchomić nadpisany, a więc zniszczony oryginalny bootrekord. Niektóre wirusy próbują obejść to niebezpieczeństwo markując zarezerwowane sektory jako uszkodzone lub zajęte. Wirusy, które niszczą bądź podmieniają zawartość bloku parametrów BIOS-u (BPB – BIOS Parameter Block), mogą prowadzić do analogicznych problemów jak opisany wirus Monkey. Typowe wirusy atakujące PBR nie powinny jednak powodować żadnych dodatkowych problemów w systemie NT opartym na FAT. Są one bowiem nieaktywne od momentu przejęcia kontroli przez sterowniki Windows NT.

Istotne cechy Windows NT mające wpływ na odporność systemu

- Serwisy systemowe Windows NT nie odwołują się do rezydentnego jądra DOS-a (DOS kernel).
- Windows NT pozwala na zastosowanie trzech różnych systemów zarządzania plikami: systemu bazującego na tablicy FAT, nowego systemu NTFS dla serwerów oraz systemu MAC.
- NT umożliwia ograniczenie praw do plików w powiązaniu z prawami użytkowników, co może zapobiec rozprzestrzenianiu się infekcji wirusów plików typu fast infector na pliki innych użytkowników.
- NT nie odwołuje się do funkcji BIOS-u celem przeprowadzania wszelkich operacji dostępu do dysków na poziomie sprzętowym, lecz wykorzystuje własne, specyficzne sterowniki programowe NT pracujace w trybie chronionym.
- NT automatycznie zapobiega próbom bezpośredniego zapisu na dysk przez dowolny program wykonywany w oknie DOS.

Dodatkowym źródłem potencjalnych zagrożeń infekcją bootrecordu jest opcja umożliwiająca instalację Windows NT w istniejącej partycji DOS lub Windows 95, opartej na FAT. Użytkownik może wtedy uruchomić system operacyjny Windows NT albo DOS (lub Windows 95). Windows NT tworzy podczas instalacji kopię zapasową bootrekordu DOS/Win 95 i zachowuje go w pliku BOOTSEC.DOS w katalogu głównym partycji DOS/Win 95. W następnej kolejności NT zamienia dotychczasowy bootrekord, bazujący na swoim własnym FAT. Każdorazowo podczas startu systemu użytkownik pytany jest przez program ładujący, który system operacyjny ma zostać wystartowany. W przypadku wyboru DOS/Windows 95 program ten ładuje i uruchamia oryginalny bootrekord zawarty w pliku BOOTSEC.DOS. Jeżeli jednak rekord ten był zainfekowany przez wirusa, i to przed zainstalowaniem Windows NT, to przy każdym starcie systemu DOS/Windows 95 wirus przejmować będzie kontrolę nad systemem. Może przy tym pozostać niewykryty w przypadku uruchamiania NT.

Nieco odmienna sytuacja ma miejsce w przypadku używania systemu plików NTFS. Program instalacyjny NT umieszcza podczas instalowania zdolnej do bootowania partycji NTFS program ładujący system operacyjny w kilku sektorach następujących bezpośrednio po bootrekordzie NTFS. Podczas bootowania MBR wczytuje i uruchamia PBR, który z kolei wczytuje się wraz z tymi dodatkowymi sektorami programu ładowania do pamięci. Na kompletną procedurę ładującą i uruchamiającą system operacyjny składają się więc bootrekord NTFS oraz obejmujący dodatkowe sektory program ładujący.

Wirus atakujący bootrekord NTFS nadpisuje efektywnie pierwszy sektor wielosektorowego programu ładowania początkowego niszcząc ważne dane czy procedury. Konsekwencją jest następujący przebieg bootowania:

- Komputer zostaje włączony lub zresetowany.
- Podczas bootowania NTFS komputer ładuje i uruchamia oryginalny MBR. Następnie uruchamiana jest procedura ładowania początkowego MBR, która z kolei ładuje i przekazuje kontrolę zarażonemu wirusem rekordowi PBR aktywnej partycji NTFS.
- Wirus instaluje się w pamięci i oddaje kontrolę oryginalnemu rekordowi PBR NTFS, który jest odzyskiwany z kopii zachowanej przez wirus na końcu dysku.
- W tym stadium procedura z niezainfekowanego bootrekordu NTFS próbuje załadować kompletną procedurę ładującą, na którą składają się oryginalny

▶ 11

bootrekord NTFS i następujące po nim sektory. Jednakże pierwszy sektor wielosektorowego programu ładowania początkowego zastąpiony został przez wirusowy PBR. Ładowana i uruchamiana jest więc uszkodzona kopia programu ładowania początkowego, składająca się z wirusowego PBR i następującej po nim pozostałości oryginalnych sektorów ładowania początkowego.

- Uruchomienie uszkodzonego programu prowadzi do zawieszenia się systemu.

Większość wirusów atakujących PBR będzie więc prowadzić do zawieszenia się systemu, uniemożliwiając start NT. Wyjątek stanowić mogą wirusy posługujące się techniką stealth.

Wirusy plików wykonywalnych również działają w NT

Wirusy plików wykonywalnych DOS należą do drugiej grupy wirusów rozpowszechnionych na wolności. Zainfekowany program jest modyfikowany przeważnie tak, że wirus przejmuje kontrolę nad komputerem od momentu wystartowania tego programu przez użytkownika lub system operacyjny.

Wirus wyszukuje wtedy i infekuje inne dostępne pliki uruchamialne – co określane jest mianem infekcji bezpośredniej. Określone funkcje DOS, odpowiedzialne za stworzenie efektywnego i szybkiego mechanizmu orientowania się wśród licznych plików i katalogów, służą wirusowi do skutecznego wyszukiwania i infekowania nowych plików. Te same funkcje DOS wykorzystuje np. program narzędziowy umożliwiający szybkie wyszukanie plików zawierających konkretny ciąg znaków. O skuteczności takiego mechanizmu określanego również w literaturze angielskojęzyczej jako tzw. „fast infector" świadczyć może przykład eksperymentalnej infekcji za pomocą wirusa VBASIC. W ciągu ok. 45 sekund od rozpoczęcia infekcji był on w stanie zainfekować wszystkie (!) pliki typu COM na dysku twardym o pojemności 1,2 GB.

Inną drogą infekcji, często stosowaną przez wirusy plików uruchamialnych, jest dodatkowe instalowanie się rezydentnie w systemie operacyjnym. Umożliwia to wirusowi kolejno infekowanie plików uruchamialnych systemu operacyjnego bądź innych programów w trakcie uruchamiania, kopiowania itp. Od tego momentu każde zgłoszenie do systemu operacyjnego wykonane przez użytkownika lub inny program, celem uruchomienia albo udostępnienia określonego pliku jest przerywane przez wirus, który przejmuje kontrolę nad komputerem.

NT a inne systemy

Windows NT jest bardziej odporne na ataki wirusów niż DOS, Windows 3.1x lub Windows 95. Nie oznacza to jednakże, że wirusy nie są w stanie zagrozić NT. Przykładowo wirusy typu makro mogą rozprzestrzeniać się bez przeszkód, podobnie jak to czynią w innych systemach. Wirusy typu bootsektora, aczkolwiek nie mogą się powielać, doprowadzić mogą do znaczących uszkodzeń wolumenów NT. Szczególnie podatne są instalacje umożliwiające bootowanie w dwóch systemach NT i DOS lub Windows 95.

Po zakończeniu swojej działalności, program wirusowy może przekazać kontrolę z powrotem zainfekowanemu programowi tak, że użytkownik nie będzie w stanie stwierdzić na pierwszy rzut oka żadnych nieprawidłowości.

Większość wirusów infekujących pliki uruchamialne funkcjonuje „poprawnie" w oknie DOS Windowsa NT. Obydwie grupy (infekcji bezpośredniej oraz stealth) zachowują się jednakże w różny sposób pod Windows NT.

Wirusy infekcji bezpośredniej, np. POLISH-1063, działają dokładnie w taki sam sposób, jak czynią to standardowo pod DOS-em, dopóki używają standardowych funkcji DOS-a emulowanych pod NT. Wyjątkiem mogą być wirusy starsze odwołujące się do wcześniejszych wersji DOS-a lub, po prostu, źle napisane.

Generalnie, wirus plików uruchamialnych typu rezydentnego może pozostawać rezydentnie w granicach wyznaczonych przez okno DOS-a w Windows NT. Po zainstalowaniu się rezydentnie w oknie DOS-a, jest on zdolny do infekowania innych, dostępnych lub uruchamianych programów pod warunkiem, że użytkownik posiada odpowiednie prawa do modyfikowania docelowego pliku. Wirus nie jest natomiast zdolny do przemieszczenia się do innego okna ze względu na odseparowane, chronione obszary pamięci każdego okna DOS-a. Oczywiście nic nie chroni użytkownika przed uruchamianiem zainfekowanego programu w dowolnej liczbie okien DOS-owych.

Następnie, jeżeli wirusowi uda się zainfekować command shell (użytkownik musi posiadać uprawnienia do jego modyfikacji) używany w oknach DOS NT (standardowo CMD.EXE), to użytkownik za każdym razem otwierając nowe okno DOS-a będzie automatycznie ładować rezydentnie wirus do obszaru pamięci przydzielonego do danego okna.

Dodatkowo NT umożliwia użytkownikowi uruchamianie dowolnych programów dla środowisk Windows spod okna DOS-a. Jeżeli wirus przejął obsługę żądań EXECUTE poprzez command shell NDOS.COM, to potencjalnie jest w stanie zainfekować każdy uruchamiany program Windows. Jednakże taki DOS-owy wirus przeważnie infekując komponent DOS pliku w formacie EXE dla Windows (tzw. Windows New Executable – NE EXE lub Windows Portable Executable – PE EXE) nadpisuje lub niszczy komponent Windows umieszczony na końcu pliku.

Wirusy typu stealth potrafią ukrywać swoją obecność przed użytkownikiem. Wirus infekujący doczepia swoją kopię na końcu programu infekowanego powodując wzrost jego wielkości o długość kodu wirusa. Ponieważ użytkownik mógłby zauważyć tę zmianę, wirus „koryguje" długość pliku tak, by system operacyjny meldował pierwotną długość zainfekowanego pliku. Oczywiście podgląd kodu binarnego takiego programu za pomocą edytora binarnego ujawniłby obecność wirusa na końcu, ale kto z użytkowników wpadnie na taki pomysł, dopóki wirus nie powoduje odczuwalnego spadku wydajności komputera czy zakłóceń w działaniu programów?

Elementarne środki bezpieczeństwa

- Skonfigurować komputer tak, by zawsze startował z dysku twardego, a nie z przypadkowo pozostawionych w napędzie dyskietek.
- Przed instalacją Windows NT w istniejącej partycji DOS lub Windows 95 sprawdzić ją dobrym programem antywirusowym.
- Utworzyć podczas instalacji dyskietki bezpieczeństwa (Windows NT Emergency Disks) i aktualizować je po każdej zmianie konfiguracji systemu.
- W przypadku stosowania partycji opartych na FAT ograniczyć możliwość bootowania spod DOS-a oraz stosowania niesprawdzonych źródeł jak np. dyskietki dla niepowołanych osób.
- W przypadku partycji NTFS wykorzystać oferowany mechanizm protekcji plików i katalogów dla istotnych plików.
- Prowadzić bieżącą kontrolę za pomocą dobrego skanera antywirusowego.

Uwaga na wirusy towarzyszące

Odmienny mechanizm ukrywania się stosuje grupa wirusów reprezentowana przez wirus MONKEY. Zasadą jest utworzenie i umieszczenie gdzieś na dysku kopii oryginalnego rekordu wprowadzającego (boot record). Uruchomienie dowolnego

▶ 117

programu narzędziowego celem wykrycia nieprawidłowości w MBR, spowoduje jedynie podanie przez wirusa zachowanej kopii oryginału MBR. Pozornie wszystko będzie w porządku. Technika tego wirusa funkcjonuje poprawnie pod DOS, Windows 3.1x, Windows 95. Generalnie, wirusy tego typu są w stanie ukrywać swoją obecność wyłącznie, jeżeli są obecne i aktywne w pamięci.

Wirusy tego typu funkcjonować będą także pod Windows NT, o ile nie odwołują się do nieudokumentowanych funkcji DOS, które nie są zaimplementowane w emulacji DOS-a NT. Wirus będzie zdolny do ukrywania się przed innymi wywoływanymi programami (systemem), jednakże wyłącznie z tego samego okna DOS.

Wirusy towarzyszące stanowią wyjątek, ponieważ nie dołączają się do żadnych plików. Atakują one pliki typu EXE wykorzystując określoną kolejność w uruchamianiu plików przez system operacyjny DOS. Po wpisaniu nazwy programu (bez rozszerzenia) interpreter zleceń COMMAND.COM uruchamia najpierw zawsze plik typu COM. Niektóre z tych wirusów dodatkowo zaopatrują tak utworzone pliki w atrybut hidden, aby utrudnić ich wykrycie.

Wirusy towarzyszące występują głównie w dwóch odmianach: jako rezydentne oraz wirusy bezpośredniej infekcji. Wszystko, co powyżej napisano o takich typach wirusów, odnosi się również do tej rodziny. Będą one działać pod NT poprawnie tak długo, jak długo interpreter poleceń stosowany przez okno DOS NT pozostaje kompatybilny odnośnie kolejności uruchamiania plików w stosunku do interpretera DOS (COMMAND.COM) – co aktualnie ma miejsce.

W chwili obecnej pliki danych np. typu DOC czy XLS obok danych w postaci tekstu, grafik, itp. zawierać mogą uruchamialne programy makro. A wszędzie tam gdzie są programy, rodzi się możliwość napisania programu wirusowego. Większość wirusów pisana jest w języku niskiego poziomu – asemblerze. Język ten limituje ich zdolność do prawidłowego funkcjonowania na komputerach różnych typów. Takiego ograniczenia nie posiada język programowania makro, będący w istocie niezależnym od platformy DOS, Windows czy MacOS. Dodatkowo jest on dobrze udokumentowany i stosunkowo łatwy do opanowania. Dlatego wirusy makro napisane dla aplikacji pracujących pod Windows 3.1x lub Windows 95 funkcjonować będą również pod Windows NT, o ile aplikacja macierzysta funkcjonuje poprawnie w tym otoczeniu.

Windows NT umożliwia ograniczenie dostępu do dokumentów dla osób niepowołanych, zmniejszając potencjalne ryzyko infekcji. Możliwość taką daje system ochrony NT na poziomie plików (prawa dostępu). W każdym razie, wirusy makro mogą rozprzestrzeniać się czy to przez e-mail, czy też na drodze nieograniczonego dostępu do dokumentów w sieci.

Wirusów pisanych dla NT (na razie) nie ma

Odrębny temat to wirusy pisane specjalnie pod konkretne środowisko Windows. I tak liczbę wirusów napisanych specjalnie pod Windows 3.1x szacuje się dziś na ok. 15. Potwierdzone meldunki mówią jednakże wyłącznie o jednym z nich rozprzestrzeniającym się na wolności – wirusie TENTACLE, rozprzestrzenionym poprzez Internet. Ta grupa na pewno będzie wykazywała typową dla wirusów tendencję wzrostową. Funkcjonowaniem odpowiadają one wirusom DOS-owym. Różnica tkwi w celu infekcji. Podczas gdy wirusy DOS koncentrują się na atakowaniu plików typu EXE, COM i SYS, celem dla tych wirusów są wyłącznie uruchamialne pliki Windows w tzw. formacie Windows New Executable (NE EXE). Jest to nowy format pliku typu EXE zawierający dwa niezależne elementy: standardowy program DOS typu EXE o dopuszczalnej wielkości do 640 KB, pokazujący typowo meldunek „Ten program wymaga Microsoft Windows" w przypadku uruchomienia spod DOS oraz uruchamialny komponent typu Windows posiadający odrębny format. Jeżeli program uruchamiany jest spod Windows, to właśnie ta część kodu jest aktywowana. Jest ona również celem ataku wirusów napisanych specjalnie pod Windows 3.1x i umożliwia im ich rozprzestrzenianie się. Na uwagę zasługuje fakt, że teoretycznie plik typu NE EXE może być zainfekowany niezależnie przez dwa wirusy: jeden typu DOS i drugi typu Windows 3.1x.

Większość wirusów napisanych pod Windows 3.1x funkcjonować będzie poprawnie także w otoczeniu NT, ponieważ daje ono możliwość poprawnego funkcjonowania programów napisanych pod Windows 3.1x.

Przykładowo, jeden z wirusów laboratoryjnych, który stosuje DOS-owy interfejs protected mode, instaluje się jako Windows TSR i „podczepia" się pod serwis systemowy EXECUTE PROGRAM Windows 3.1x. Wirus wykorzystujący ten serwis będzie także funkcjonował pod Windows NT z takim ograniczeniem, że będzie w stanie infekować wyłącznie inne aplikacje typu Windows 3.1x, uruchamiane pod NT.

Wirusy Windows 3.1x typu infekcji bezpośredniej – będą rozprzestrzeniać się bez ograniczeń, ponieważ Windows NT symuluje serwisy Win 3.1, stosowane do znajdowania i modyfikacji plików.

Dlaczego nie stwierdzono jak dotąd na wolności żadnego 32-bitowego wirusa, napisanego specjalnie pod NT? Jednym z czynników hamujących ich rozwój są wymagania sprzętowe samego systemu operacyjnego. Standardowe konfiguracje sprzedawanych dziś komputerów są niewystarczające, jeżeli chodzi o otoczenie dla programisty NT. Innym czynnikiem może być bardziej skomplikowana struktura plików uruchamialnych w porównaniu do innych systemów. Nie bez znaczenia jest też mała ilość powszechnie dostępnej dokumentacji opisującej 32-bitowe formaty plików, wymuszająca długotrwałe dochodzenie metodą prób i błędów.

Jak długo fakty powyższe stanowić będą barierę, jest rzeczą spekulacji. Praktyka uczy, że również w tym zakresie należy w przyszłości oczekiwać rozwoju, jaki miał miejsce w odniesieniu do poprzednich generacji wirusów.

Krzysztof Barszczewski

Wybrane typy wirusów

ładowania początkowego – zastępują oryginalną procedurę ładującą procedurą wirusową, co umożliwia im przejęcie kontroli i infekowanie MBR lub PBR zaraz po włączeniu komputera – nośnikiem może być zainfekowana dyskietka nie zawierająca żadnych plików!
plików wykonywalnych – celem ataków są głównie pliki typu COM, EXE, SYS, a podstawową techniką rozprzestrzeniania się jest dołączanie swej kopii do niezainfekowanych plików wykonywalnych
wieloczęściowe – łączą w sobie cechy wirusów ładowania początkowego i wirusów plików wykonywalnych
towarzyszące – tworzą plik o rozszerzeniu COM, o tej samej nazwie i w tym samym katalogu co atakowany plik EXE. Wykorzystują określoną kolejność w uruchamianiu plików przez system operacyjny DOS
stealth – jako programy rezydentne, przejmują część funkcji systemu zmieniając informacje tak, aby ukryć swoją obecność
makro – atakują pliki danych mogące zawierać uruchamialne programy pisane w języku makro, np. typu DOC, XLS.

Uwaga

CHIP CD 5/97

Dodatkowe informacje na temat bezpieczeństwa systemu Windows NT, narzędzia, skanery antywirusowe i inne materiały można znaleźć na dołączonym CD-ROM-ie w kategorii **Software/Bezpieczeństwo Windows NT**.