Spis treœci AntiVirenKit 6

Czêœæ ogólna

Przygotowanie

- Analiza wirusów

Praca z AVK 6 dla Windows 3.X

Tajniki i sztuczki

Informacje o wirusach

Katalog wirusów

Wstêp

Zdecydowaliœcie siê Pañstwo, na ochronê przed wirusami programem AntiVirenKit 6.0. Zakupiliœcie Pañstwo produkt skupiaj¹cy wyniki oœmiu lat pracy nad wirusami, prezentuj¹cy najnowszy stan techniki programowania.

Dla ka¿dego ³atwy w obs³udze i jednoczeœnie odpowiadaj¹cy najwy¿szym wymogom bezpieczeñstwa - to odwieczne cele pracy G DATA Software, nad ulepszaniem AVK.

Poni¿sza wersja ³¹czy je, na dotychczas nie osi¹gniêtym poziomie. Aby Pañstwo byli zawsze na bie¿¹co, polecamy regularn¹ aktualizacjê programu przez SERWIS PRYWATNY lub jeszcze lepiej - SERWIS PROFESJONALNY.

AntiVirenKit od lat chroni niemieckie banki, urzêdy i zak³ady pracy przed niemi³ymi niespodziankami i mo¿liwymi stratami. **W Polsce od 1995 roku**. AntiVirenKit 6.0 jest tak pomyœlany, aby rozpoznawa³ nie tylko znane wirusy, ale tak¿e nowoœci, przy pomocy ró¿nych technik dzia³ania.

Zakup programu AntiVirenKit 6.0 by³ dobr¹ inwestycj¹. Przez lata bêdzie Pañstwu s³u¿y³ zapobiegaj¹c, a w razie wykrycia wirusa usuwaj¹c zagro¿enie. W przypadku powstania problemów, przys³uguje Pañstwu po³¹czenie z hotline (tzw. gor¹c¹ lini¹). W ten sposób dysponuj¹ Pañstwo, jedn¹ z najlepszych mo¿liwoœci programowej ochrony antywirusowej. W po³¹czeniu z Serwisem Profesjonalnym, maj¹ Pañstwo dodatkow¹ pewnoœæ otrzymania w ramach naszego serwisu ka¿dej nowej wersji aktualizacyjnej.

Powodzenia przy pracy z AntiVirenKit 6.0!

G DATA Software - lipiec 1996

G DATA Serwis

Co najwa¿niejsze:

Prosimy o przes³anie nam karty serwisowej!

Znajd¹ j¹ Pañstwo w opakowaniu oprogramowania. Otrzymaj¹ Pañstwo od nas kolorow¹ dyskietkê serwisow¹ z upowa¿nieniem do ¿¹dania kolejnych aktualizacji programu. Tylko w ten sposób mog¹ Pañstwo korzystaæ z nastêpuj¹cych udogodnieñ:

- SERWIS PRYWATNY
- SERWIS PROFESJONALNY
- Bezp³atny Hotline
- Serwis wirusów

Informacje dla Pañstwa o zmianach i nowoœciach.

Karta serwisowa zawiera z prawej strony pole, w którym deklarujemy chêæ uzyskania SERWISU PROFESJONALNEGO. Je¿eli nie przekonuj¹ Pañstwa zalety SERWISU PROFESJONALNEGO, prosimy przes³aæ nam kartê bez deklaracji.

SERWIS PROFESJONALNY, mo¿na wykupiæ w dowolnym, póŸniejszym terminie.

☞UWAGA: Ju¿ kilkumiesiêczna wersja nie gwarantuje pe³nej ochrony przed wirusami! Ka¿dy u¿ytkownik otrzyma od nas bezp³atnie po wys³aniu, kolorow¹ dyskietkê serwisow¹ z najnowsz¹ wersj¹ AVK. W ten sposób czas sk³adowania programu u dystrybutora czy sprzedawcy nie dzia³a na Pañstwa niekorzyœæ.

Jakoœæ naszych us³ug zale¿y w du¿ej mierze od tego, czy Pañstwo bêd¹ przestrzegaæ okreœlonych warunków. W ten sposób mo¿emy gwarantowaæ swobodny rozwój naszych us³ug serwisowych.

G DATA-Hotline

Hotline przys³uguje bezp³atnie wszystkim zarejestrowanym klientom. Pomaga przy wszystkich problemach, zwi¹zanych z AVK - telefonicznie, przez fax, lub Internet (e-mail: hotline@gdata.de - tylko w BRD).

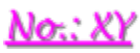
Telefon:	**0-966 / 42330**
Fax:	0-966 / 42333
e-mail:	hotline@gdata.de tylko BRD

W godzinach Hotline jeden z naszych specjalistów jest zawsze do Pañstwa dyspozycji. Otrzymaj¹ Pañstwo informacje o okreœlonych wirusach i ewentualnych œrodkach zaradczych. Abyœmy szybko mogli Pañstwu pomóc: prosimy podaæ numer rejestracji, numer wersji, oraz aktualne wersje DOS i Windows. Godziny po³¹czeñ:

W dni robocze 9.00 - 11.00 oraz 13.00 - 16.00

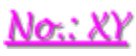
W innych godzinach pracy nie mo¿emy gwarantowaæ pomocy.

Przy wielu problemach rozwi¹zanie mo¿na znaleŸæ w tekstach pomocy i podrêcznikach. Prosimy spróbowaæ najpierw tej drogi rozwi¹zania problemu.



Numer wersji AVK

Numer wersji pomaga ustaliæ aktualnoœæ Pañstwa programu, a w razie problemu odpowiednio zareagowaæ. Numer wersji znaleŸæ mo¿na pod opcj¹ Info... lub na etykiecie (Label) kolorowej dyskietki serwisowej.



Numer rejestracyjny

W opakowaniu AVK znajduje siê karta rejestracji. Prosimy wype³niæ i odes³aæ do nas. Tylko tak mo¿emy Pañstwa zarejestrowaæ i pomóc w przypadku wyjaœnienia w¹tpliwoœci. Serwis pyta o numer rejestracji sprawdzaj¹c to¿samoœæ. Numer mo¿na znaleŸæ na pierwszej stronie podrêcznika. Prosimy podaæ numer rejestracyjny tak¿e przy zamawianiu SERWISU PROFESJONALNEGO.

Zapasowa dyskietka

W ka¿dej chwili mog¹ Pañstwo odes³aæ nam uszkodzone lub niefunkcjonuj¹ce dyskietki G DATA. Prosimy zamieœciæ zaadresowan¹, ofrankowan¹ kopertê zwrotn¹. Otrzymaj¹ Pañstwo zapasow¹ dyskietkê.

Porady wirusowe

W przypadku zauwa¿enia nowego wirusa lub dziwnego zachowania komputera, prosimy o przes³anie nam dyskietki z kopi¹ podejrzanego programu. Przeanalizujemy dyskietkê i dostarczymy Pañstwu jak najszybciej pomys³y na rozwi¹zanie problemu. Prosimy przesy³aæ dyskietki w sytuacjach proponowanych przez AVK. Oczywiœcie gwarantujemy pe³n¹ dyskrecjê co do przes³anych nam Pañstwa danych.

Aktualizacja programu

... podstawowa czynnoœæ przy obs³udze ka¿dego programu antywirusowego.. ¯aden inny program nie wymaga tak czêstej nowelizacji danych. Brak ka¿dej nastêpnej wersji, powoduje nierozpoznawanie oko³o stu nowych wirusów.

W obliczu coraz to nowych, inteligentniejszych wirusów, program ulega przestarzeniu i zapewnia ograniczon¹ ochronê. Rocznie wydajemy ok. 6-10 nowych wersji, z których ka¿da rozpoznaje ok. 100 nowych wirusów, czyli co 6-8 tygodni ukazuje siê nowa wersja. W Pañstwa interesie le¿y regularna aktualizacja programu aby rozpoznawa³ tak¿e nowe wirusy.

WA¯NE: Aby korzystaæ z naszego serwisu nale¿y wys³aæ nam wype³nion¹ kartê serwisow¹ (ostatnia strona podrêcznika). Tylko tak otrzymaj¹ Pañstwo kolorow¹ dyskietkê serwisow¹ upowa¿niaj¹c¹ do aktualizacji.

Istniej¹ dwa sposoby otrzymania aktualizacji:

- SERWIS PRYWATNY
- SERWIS PROFESJONALNY

Dyskietka serwisowa AVK

Kolorowa dyskietka serwisowa nie znajduje siê w pakiecie AVK!

Otrzymuj¹ j¹ Pañstwo po wys³aniu karty serwisowej AVK (znajduje siê w opakowaniu). Dyskietka ta zawiera najnowsz¹ aktualizacjê programu i bêdzie wymieniana na nowe w nastêpuj¹cy sposób:

SERWIS PRYWATNY
Prosimy wys³aæ w ramach serwisu prywatnego dyskietkê serwisow¹ z ofrankowan¹ kopert¹ zwrotn¹ (nie przesy³ajcie Pañstwo podrêcznika ani opakowania).

SERWIS PROFESJONALNY
W ramach serwisu profesjonalnego otrzymuj¹ Pañstwo automatycznie aktualn¹ wersjê AVK na nowej dyskietce. Nasza Firma cyklicznie przesy³a najnowsze wersje.

SERWIS PRYWATNY

Ten serwis przys³uguje wszystkim zarejestrowanym **osobom prywatnym** w cenie AVK 6. Po przes³aniu nam kolorowej dyskietki serwisowej (otrzymuj¹ j¹ Pañstwo w ramach serwisu) z ofrankowan¹ zaadresowan¹ kopert¹ zwrotn¹, otrzymaj¹ Pañstwo bezp³atnie now¹ dyskietkê serwisow¹ AVK.

☞WA¯NE: Wysy³amy tylko dyskietki kolorowe (prosimy nie wysy³aæ opakowañ ani podrêcznika!)

Prosimy koniecznie zamieœciæ wystarczaj¹co (w sensie kwoty) ofrankowan¹ kopertê zwrotn¹ z adresem. Zwracamy uwagê na wysokoœæ op³at pocztowych.

Ten serwis s³u¿y naszym u¿ytkownikom ju¿ od 1988, a w Polsce od 1995. Gwarantujemy sta³¹ aktualnoœæ Pañstwa programu. Uwaga: op³aty pocztowe ró¿ni¹ siê w zale¿noœci od formatu listu (przesy³ki dyskietek).

☞UWAGA: Chcielibyœmy wspomnieæ, ¿e ka¿da aktualizacja przez serwis prywatny wymaga inicjatywy Pañstwa. Aby utrzymaæ jakoœæ oferowanych us³ug na ¿¹danym poziomie, musz¹ Pañstwo œledziæ ka¿d¹ wyprodukowan¹ aktualizacjê, co wymaga czasu.

Dlatego proponujemy Pañstwu o wiele wygodniejszy i tak samo pewny sposób aktualizacji - Serwis Profesjonalny!

SERWIS PROFESJONALNY

Pominiêcie aktualizacji, mo¿e spowodowaæ powa¿ne szkody. Aby temu zaradziæ oferujemy Pañstwu pakiet **Serwis Profesjonalny**), umo¿liwiaj¹cy automatyczne przes³anie nowo powsta³ej wersji programu. Pakiet Serwis Profesjonalny, mo¿na uzyskaæ przy pomocy karty serwisowej. Serwis Profesjonalny wymaga odnowienia po up³ywie roku. Poinformujemy Pañstwa o up³ywie terminu wa¿noœci pakietu.
Umowa obowi¹zuje tylko rok: . Decyduj¹ Pañstwo sami czy j¹ przed³u¿yæ. Pakiet Serwisu Profesjonalnego mo¿na zamówiæ listownie lub telefonicznie (Faksem) niezale¿nie od daty zakupu. Polecamy go nie tylko profesjonalistom i Firmom ale tak¿e wszystkim u¿ytkownikom AVK. Serwis jest szczególnie przydatny, kiedy u¿ywamy komputera do pracy zawodowej, gdzie ochrona plików z danymi ma du¿e znaczenie. Koszty zakupu pakietu, nie przewy¿szaj¹ kosztów przesy³ania dyskietek i wk³adu pracy przy serwisie prywatnym!

Formularz SERWISU PROFESJONALNEGO

G DATA Software Sp. z o.o.
Serwis - nowelizacje
ul. 28 Lutego 34

78-400 Szczecinek

¯¹danie pakietu SERWIS PROFESJONALNY

Szanowni Pañstwo,

Chcia³bym za cenê 122,- Z³

○ zamówiæ
○ przed³u¿yæ (zakreœlamy wybran¹ pozycjê).
na okres jednego roku SERWIS PROFESJONALNY AVK
Otrzymam przy jego pomocy ka¿d¹ nowopowsta³¹ aktualizacjê AVK. Po up³ywie roku umowa wygasa i zdecydujê czy chcê j¹ przed³u¿yæ.

Proszê przes³aæ aktualizacjê i rachunek pod adres:

Firma: _____; (ewtl.)Numer klienta.: _____

Nazwisko : _____

Ulica: _____

kod, miejscowoœæ: _____, _____

Mój numer rejestracji: _____

W razie pytañ jestem uchwytny pod numereml.: _____ / _____.

Data, podpis: _____

Pismo VIREN-NEWS

VIREN-NEWS to czasopismo fachowe wydawane przez G DATA w Bochum. VIREN-NEWS mo¿na otrzymaæ w ramach serwisu profesjonalnego. Ka¿dy u¿ytkownik serwisu, otrzyma wraz z aktualizacj¹ najnowsze wydanie czasopisma.
W piœmie VIREN-NEWS poruszona jest tematyka ochrony danych przed wirusami. Informuje ono o wydarzeniach i trendach na scenie wirusowej, a tak¿e zawiera wskazówki G DATA w temacie wirusów itp.

Z³amanie warunków serwisu

Mo¿emy uskuteczniaæ nasze us³ugi tak d³ugo, jak tylko Pañstwo trzymaj¹ siê "regu³ gry". Z³amanie warunków umowy wliczamy w pañstwa koszta. Zaleg³e aktualizacje przeœlemy dopiero po uregulowaniu rachunków.

Prosimy o zrozumienie œrodków ostro¿noœci, podjêtych z wymienionych powodów. Ma to na celu utrzymanie porz¹dku w strukturze serwisu.

Przesy³anie dyskietek

Przesy³aj¹c nam dyskietki z podejrzeniem infekcji lub nieznanymi zmianami, prosimy pamiêtaæ:

- o napisaniu na dyskietce nazwiska i adresu
- o nieprzesy³aniu oryginalnych dyskietek AVK
- o za³¹czeniu numeru wersji AVK,

Prosimy przestrzegaæ tak¿e nastêpuj¹cych wskazówek:

- Wysy³anie listów poleconych itp., z regu³y nie ma sensu i jest nie wskazane.

- Dyskietki z opisami musz¹ byæ wys³ane jako listy.
- Do przesy³ek mo¿na u¿ywaæ zamiast normalnych kopert torebek powietrznych, które mo¿emy odes³aæ z powrotem. W tym przypadku nie musz¹ Pañstwo wysy³aæ koperty zwrotnej.

Plik tekstowy (AVK.TXT)

Z powodu dokonywania zmian i poprawek, nie jest mo¿liwe wydrukowanie podrêcznika zawieraj¹cego dok³adny opis. W celu umieszczenia wznowieñ i nowych informacji nie zawartych w podrêczniku utworzyliœmy plik AVK.TXT, informuj¹cy o aktualnym stanie produktu. Prosimy przejrzeæ ten plik przed uruchomieniem AVK 6!

Pliki AVK.TXT mo¿na wyœwietliæ nastêpuj¹cymi poleceniami DOS:

na ekranie:

TYPE A: AVK.TXT

lub wydrukowaæ:

TYPE A: AVK.TXT >PRN

W wersji Windows mo¿na to robiæ w³asnymi edytorami.

UWAGA: Staraliœmy siê unikn¹æ sprzecznoœci tekstów podrêcznika i pliku, w przypadku ich wyst¹pienia prosimy pamiêtaæ: teksty w pliku maj¹ pierwszeñstwo przed podrêcznikiem pomocy!

Analiza podstawowa

Przed instalacj¹...
W ¿adnym przypadku nie mo¿na instalowaæ AVK 6 (ani innego programu) kiedy analiza wstêpna wykaza³a obecnoœæ wirusa na dysku lub w pamiêci. Przekonajmy siê, czy nie zamelduje ona o wykryciu wirusów, a w przypadku ich wykrycia, czy usunie je dok³adnie.
Sposób przeprowadzenia analizy:

ANALIZA PODSTAWOWA (skrót)

1. Wy³¹czmy komputer na ok. piêæ sekund.
2. Wystartujmy z zabezpieczonej dyskietki.
3. PrzeprowadŸmy analizê twardego dysku.

Polecenie DOS: **AVK** [napêd]**:** (przewa¿nie: **AVK C:**)

Po zakoñczeniu analizy mo¿emy zainstalowaæ AVK 6.

Sporz¹dzanie dyskietki startowej

Bardzo czêsto pytaj¹ Pañstwo, co robiæ w przypadku zara¿enia bootsektora. Tak¿e dyskietki s¹ wtedy zara¿one. Aby zanalizowaæ komputer konieczna jest wolna od wirusów dyskietka startowa.

Jest ona tak¿e niezbêdna przy instalacji nowej aktualizacji programu. Tylko przy starcie z takiej dyskietki mo¿na mieæ pewnoœæ, ¿e w pamiêci nie ma wirusów. Dopóki w pamiêci rezyduje wirus, analiza i usuniêcie go nie jest mo¿liwe. Wirusy typu Stealth, mog¹ doprowadziæ do niezauwa¿enia wirusa w systemie. Z tej przyczyny radzimy sporz¹dziæ dyskietkê startow¹, zanim dojdzie do infekcji.

Sposób jej sporz¹dzenia znajd¹ Pañstwo w podrêczniku obs³ugi Windows.

U¿ycie AVK 6

Do czego s³u¿y AVK?

Zapoznali siê Pañstwo z problematyk¹ wirusów komputerowych i postanowili chroniæ swoje dane za pomoc¹ AVK 6.0. To by³a rozs¹dna decyzja, poniewa¿ AVK, zalicza siê do najlepszych programów antywirusowych œwiata. Gdyby coœ jeszcze nie by³o jasne :

UWAGA: Co miesi¹c ukazuje siê oko³o stu nowych wirusów. Oznacza to dezaktualizacjê wersji AVK po kilku miesi¹cach i zmniejszon¹ ochronê przed wirusami.

Dlatego te¿, otrzymali Pañstwo do zakupionej wersji pakiet serwisowy, który m.in. umo¿liwia nowelizacjê programu. Tylko w ten sposób mo¿emy gwarantowaæ Pañstwu pewn¹ i dobr¹ ochronê.

Jak czêsto uaktualniaæ program?

G DATA wydaje 6-10 nowelizacji rocznie. OdpowiedŸ jest prosta: dla skutecznej ochrony danych nale¿y zadbaæ, o otrzymanie ka¿dej aktualizacji (Upgrade), która siê uka¿e. Najlepiej umo¿liwia to SERWIS PROFESJONALNY. Aby Pañstwo nie zwlekali z aktualizacj¹, program sam siê o ni¹ upomni po oko³o 5-ciu miesi¹cach komunikatem, ¿e wersja jest przestarza³a i praca z AVK nie jest dalej bezpieczna. W tym wypadku nale¿y uaktualniæ program i pamiêtaæ o regularnej "pielêgnacji" programu w przysz³oœci.

Jak czêsto uruchamiaæ AVK?

Ka¿dy plik przeniesiony na twardy dysk (tak¿e CD-ROM) mo¿e byæ potencjalnym nosicielem wirusa. Nie ma regu³y ,jak czêsto uruchamiaæ program, ale pewnoœæ Pañstwa systemu spada wraz z ka¿d¹ now¹ instalacj¹ oprogramowania, czy nawet przyp³ywem danych.

Chcielibyœmy przedstawiæ wyniki ankiety przeprowadzonej wœród u¿ytkowników:

- SERWIS PROFESJONALNY
- 19% codziennie uruchamia AVK
- 45% raz w tygodniu
- 34% przy ka¿dej aktualizacji
- 2% rzadko

Uwa¿amy, ¿e powinni Pañstwo pod¹¿aæ œladem 64% u¿ytkowników i sprawdzaæ dane przynajmniej raz w tygodniu i przy ka¿dej operacji instalacyjnej.

Ogólne œrodki ochrony

Chcielibyœmy, ¿eby Pañstwo poprzez u¿ycie AVK 6.0, przyzwyczaili siê do niektórych wa¿nych czynnoœci zapobiegawczych. Prosimy, trzymaæ siê w miarê mo¿liwoœci wszystkich zaleceñ, dziêki czemu zmniejszy siê ryzyko infekcji wirusowej.

Oryginalne oprogramowanie

- U¿ywajcie Pañstwo tylko oryginalnego oprogramowania.
- Nale¿y pamiêtaæ o zabezpieczeniu oryginalnych dyskietek przed zapisem (otwory po obu stronach u góry).
- Prosimy sporz¹dziæ kopiê oryginalnego oprogramowania do u¿ytku codziennego.
- Przechowywaæ orygina³ oprogramowania w pewnym miejscu.

Prosimy sporz¹dziæ zapasow¹, nie zaka¿on¹ wirusem dyskietkê systemow¹.

Kontrola stacji dysków

- Przed ka¿dym uruchomieniem komputera nale¿y sprawdziæ, czy w stacji dysków, nie ma dyskietki (zagro¿enie zainfekowania BOOT sektora!), tak¿e przy dyskietkach bez systemu.

Wskazówka: Wielu problemów mo¿na unikn¹æ poprzez ustawienie sekwencji bootowania (startowania systemu) C:,A:. Mo¿na tego dokonaæ w menu CMOS-Setup (klawisz DEL w czasie bootowania).
UWAGA: Przy analizie podstawowej nale¿y przywróciæ sekwencjê A:, C:.

Backup

- Nale¿y regularnie sporz¹dzaæ wersjê Backup Pañstwa danych (kopie zapasowe)

W Firmach

- Prosimy unikaæ wprowadzania prywatnych programów i gier.
- Ka¿d¹ obc¹ dyskietkê nale¿y sprawdziæ.
- Analiza referencyjna powinna byæ przeprowadzana regularnie.
- Reagujmy na ka¿de nietypowe zachowanie komputera lub oprogramowania.

W wypadku infekcji wirusem

Prosimy upewniæ siê czy wszystkie napêdy zosta³y sprawdzone. Jeden pominiêty plik mo¿e zniweczyæ nasz¹ ca³¹ pracê.

Zauwa¿yli Pañstwo coœ nietypowego?
Na pytanie, czy to jest objaw zaka¿enia wirusem, nale¿y odpowiedzieæ "**TAK**" i przeprowadziæ analizê AVK 6.0 !

- Czy komputer Pañstwa w ostatnim czasie czêœciej siê zawiesza?
- Czy programy zachowuj¹ siê inaczej (czas startowania, szata graficzna, gubienie danych,

nieoczekiwane zmiany napêdów)?

- Czy dane z powodu rozmiarów nie mieszcz¹ siê na dysku?
- Czy zmienia siê obraz (kolor, ramki, rzadkie znaki i komunikaty)?
- Litery spadaj¹" z ekranu, zmiana znaków na klawiaturze?
- G³oœnik wydaje dziwne dŸwiêki, piski, melodie?
- Pamiêæ dysku twardego zape³nia siê w niewyt³umaczalny sposób?
- Czy po poleceniu CHKDSK C: uzyskujemy komunikat o uszkodzeniu dysku (spróbujmy uruchomiæ komputer z innej dyskietki i ponownie u¿yæ CHKDSK C:)?

Wymogi sprzêtu i oprogramowania

AVK pracuje w trzech wersjach systemowych: DOS, Windows 3.x i Windows'95. W ka¿dym przypadku wymagane jest przynajmniej 640 KB pamiêci operacyjnej. Przy u¿yciu graficznej wersji DOS, w pamiêci nie mog¹ rezydowaæ ¿adne inne programy. Narzêdzia rezydencyjne mo¿na umieœciæ w pamiêci rozszerzonej przez HIMEM.SYS. Wersja dla Windows 3.x, przeznaczona jest dla Windows od 3.1, zalecany jest minimum procesor 386 oraz 2MB, a najlepiej 4MB RAM i wiêcej.

Okno g³ówne

Okno g³ówne dla wersji Windows 3.X AVK 6, sk³ada siê z nastêpuj¹cych elementów:

- Sterowanie programem
- Wybór pliku
- Wiersz statusu z numerem wersji
- Pasek funkcji
- Menu g³ówne

Wybór katalogu

Opcja wybór katalogu, pokazuje aktualnie wybrany do analizy katalog. Poni¿ej znajduje siê okienko analizy podkatalogów, standardowo ustawione na przeszukiwanie Z podkatalogami".

Standardowe ustawienie sprawdzania jest "z podkatalogami". Klikniêcie mysz¹ w przycisk Szukaj lub (Alt+S) uruchamia wybór sprawdzania kartotek. Mamy tu mo¿liwoœæ dowolnego wyboru dysku twardego, katalogu, podkatalogów itd.

Wybór pliku

Opcja wyboru pliku umo¿liwia decyzjê, czy przeszukujemy wszystkie, czy tylko wybrane pliki. Standardowo ustawiono opcjê Pliki wybrane. Wchodzimy poprzez wybór przycisku "Wybór".

Wybór ustawienia Pliki wszystkie nie jest wskazane, poniewa¿ wirusy zara¿aj¹ tylko niektóre, programowe pliki (dokumenty, czasem Bootsektor). Analizowanie wielu plików graficznych i tekstowych bardzo spowalnia przebieg analizy, ale w szczególnych przypadkach przydaje siê.

Lepiej jest przeszukaæ tylko okreœlone pliki. W tym celu wybieramy opcjê Pliki wybrane... i klikamy w przycisk Wybór. Udajemy siê do menu rozszerzeñ.

W oknie wyboru przedstawione s¹ przyk³ady rozszerzeñ plików polecanych przez nas do analizy. Standardowo ustawiono nastêpuj¹ce rozszerzenia:

?GR; 386; BAT; BIN; COM; CPL; DLL; DRV; EXE; FO? OV?; SYS.

Mog¹ Pañstwo dowolnie zmieniaæ ustawienia wpisuj¹c w górne okienko swoj¹ propozycjê i potwierdzaj¹c j¹ poleceniem Dodaj (lub przez Alt+D). Mo¿na te¿ usuwaæ z listy wybrane propozycje zaznaczaj¹c je mysz¹ i u¿ywaj¹c polecenia Usuñ (lub Alt+U). Przez naciœniêcie polecenia Standard (lub Alt+S) powracamy do pierwotnego ustalenia

Wiersz Statusu

Pasek pokazuje z prawej strony numer wersji AVK , z któr¹ Pañstwo pracujecie. Informacja ta przydaje siê przy korzystaniu z hotline i serwisu AVK. Z drugiej strony pokazana jest œcie¿ka dostêpu analizowanego obecnie pliku analizujê Napêd:\Katalog\Plik.
Nakierowuj¹c kursor myszy na symbole paska funkcji lub funkcjê menu g³ównego, otrzymujemy w pasku statusu oznaczenie symbolu i wyjaœnienie funkcji.

Pasek funkcji

Pasek funkcji zawiera najwa¿niejsze funkcje codziennej obs³ugi AVK:

 Wydrukuj plik

 Rozpocznij analizê

 Wstrzymaj analizê

Informacje o pliku

Usuñ wirusa

 Usuñ zara¿ony plik

 Kopiuj zara¿ony plik (do analizy w G DATA)

Tekst pomocy (W³aœnie tam jesteœmy)

 Lista wirusów

Funkcje niemo¿liwe do uzyskania, s¹ pokazane w szarym kolorze.

Menu g³ówne

W menu g³ównym pod has³ami Plik, Analiza i Pomoc znajduj¹ siê wszystkie funkcje paska funkcji oraz kilka dodatkowych poleceñ:

Plik - Drukuj...
Drukuje wynik analizy (protokó³)

Plik - Ustawienie drukarki...
Dopasowuje typ drukarki

Plik - Koniec
Koñczy AVK

Analizuj - Uruchom...
Rozpoczyna analizê

Analizuj - Zatrzymaj...
Przerywa analizê

Analizuj - Uka¿ informacje
Pokazuje informacje na temat jednego pliku

Analizuj - Usuñ wirusa
Usuwa wirusa z zara¿onego pliku

Analizuj - Usuñ plik
Usuwa zara¿ony plik

Analizuj - Kopiuj plik
Kopiuje zara¿ony plik

Analizuj - Opcje
Otwiera menu opcji analizy, gdzie dokonujemy ustawieñ dotycz¹cych analizy

Pomoc - Spis treœci
Otwiera spis treœci tekstu pomocy AVK

Pomoc - Lista wirusów
Otwiera katalog wirusów

Pomoc - Informacje o programie...
Informacje o AVK

Sterowanie programem

Wszystkie funkcje obs³ugujemy za pomoc¹ klawiatury lub myszki. Kod klawiatury odpowiada kodowi systemu DOS, do którego jesteœcie Pañstwo przyzwyczajeni. Poszczególne opcje w menu g³ównym mo¿na uruchomiæ za pomoc¹ kombinacji Alt+litera podkreœlona w nazwie ¿¹danej opcji. Oprócz tego wiele poleceñ przypisano klawiszom funkcyjnym. Opis znajduje siê w oknach menu. Po piktogramach (ikonach) menu poruszamy siê pionowo za pomoc¹ kursorów , w poziomie poprzez TAB oraz Shift+TAB. Polecenia, uruchamia przycisk Enter.

Wybrane elementy podkreœlone s¹ ¿ó³tym kolorem, pozosta³e bia³¹ czcionk¹. Informacje o obs³udze DOS za pomoc¹ myszki znajd¹ Pañstwo w podrêczniku obs³ugi DOS i w tekstach DOS.

Przygotowanie analizy

Program jest tak pomyœlany, aby jak najszybciej przygotowaæ analizê. Rozpocznijmy od uruchomienia AVK. Po automatycznym teœcie pamiêci wybieramy ró¿ne ustawienia.

a) Wybieramy katalog do analizy.

b) Wybieramy typy plików do analizy.

c) Ustawiamy odpowiednie opcje analizy. W tym celu w menu g³ównym pod has³em Analizuj punkt Opcje.

Wybieramy odpowiedni¹ reakcjê na wykrycie wirusa: Tylko protokó³, Zatrzymaj analizê, Usuñ wirusa, Usuñ plik lub Przesuñ plik.

WSKAZÓWKA: Polecamy opcjê Tylko protokó³. Mo¿emy potem w spokoju zdecydowaæ co zrobimy ze znalezion¹ zmian¹ (ewentualn¹ mutacj¹).

Przy opcji Zatrzymaj analizê poszukiwanie zostanie wstrzymane. Mog¹ Pañstwo podj¹æ bezpoœrednio dzia³anie.

Ustawienie Usuñ wirusa nie zawsze osi¹ga skutek. Niektóre wirusy nie mog¹ byæ oddzielone" od zaatakowanego pliku. Bywa tak w przypadku kiedy wirus zniszczy³ powa¿nie strukturê pliku, lub zasz³a nietypowa mutacja.

Opcja Usuñ plik nie zawsze jest najlepszym rozwi¹zaniem, gdy¿ AVK potrafi ocaliæ" zainfekowany plik.

Przesuñ plik, ta opcja kopiuje plik wraz z wirusem do wskazanego katalogu. Po usuniêciu wirusa plik nale¿y przekopiowaæ ponownie do poprzedniego katalogu.

UWAGA: Prosimy zabezpieczyæ katalog z wirusami przed osobami nieupowa¿nionymi!

Teraz ustalmy reakcjê na zmianê referencji: Tylko protokó³, Zatrzymaj analizê, Z akceptacj¹ lub Przesuñ plik.

WSKAZÓWKA: Polecamy tak¿e opcjê Tylko protokó³.

Pozosta³e opcje - patrz wy¿ej.

Decydujemy tu, czy AVK ma przeprowadziæ dodatkowo test referencyjny plików. Sprawdzaj¹c referencje, program rejestruje sumy kontrolne poszczególnych plików i porównuje je z wynikami kolejnych analiz. W ten sposób AVK rozpoznaje zmiany systemowe, bêd¹ce czêsto sygna³em wyst¹pienia nieznanego wirusa.

WA¯NE: Prosimy przeprowadzaæ czêsto analizê referencyjn¹! Dziêki niej program potrafi wykrywaæ nieznane wirusy, co zwiêksza pewnoœæ ochrony.

UWAGA: Nie zmieniajmy katalogu rejestru sum kontrolnych. Program nie potrafi wtedy porównaæ ich z wynikami poprzednich analiz i test referencyjny traci swój sens, w danym momencie!

☞UWAGA: Nie jest wskazane polecenie Z akceptacj¹. Stwarza zagro¿enie pominiêcia nieznanego wirusa. Musimy zawsze poznaæ przyczynê zmiany!

Na specjalne ¿yczenie, AVK sporz¹dza protokó³ mo¿liwy do wydrukowania lub wgl¹du przez edytor. Wystarcza tu opcja Protokó³ ogólny". Ze wzglêdu na oszczêdnoœæ miejsca, radzimy usuwaæ uprzednio sporz¹dzone protoko³y (chyba ¿e chc¹ Pañstwo dokonaæ porównania dokumentów).

Mo¿emy przyst¹piæ do analizy.

Test pamiêci

Po wywo³aniu AVK program testuje najpierw pamiêæ. Przy przeprowadzaniu instalacji ka¿dej aktualizacji AVK, radzimy przeprowadziæ dodatkowo analizê podstawow¹.

Przeprowadzenie analizy

Po przygotowaniu analizy przejdŸmy do dzia³ania. Rozpoczynamy poleceniem paska funkcji: 
lub w menu uruchamiamy pod has³em Analizuj opcjê "Uruchom analizê".

Rozpoczêcie przebiegu analizy mo¿na rozpoznaæ, po rotacji (ruchu obrotowym) symbolu wirusa w oknie g³ównym.

Poza tym, pasek statusu pokazuje œcie¿kê dostêpu analizowanego pliku. Analizê mo¿emy w ka¿dej chwili przerwaæ poleceniem Przerwij": 

Po przeprowadzeniu analizy AVK pokazuje Wynik analizy.

Wynik analizy

Pokazanie wyniku

Po analizie, program pokazuje automatycznie raport zebranych informacji w trakcie analizy.

Okno informuje o iloœci sprawdzonych katalogów i plików, iloœci znalezionych wirusów i zmian referencyjnych oraz o liczbie usuniêtych wirusów i przesuniêtych plikach. W dolnej czêœci pojawi siê wynik analizy BOOT-sektora.

Wydruk wyniku

Wydrukowaæ raport wyników analizy, mo¿na przez u¿ycie funkcji Drukuj protokó³" w menu Plik", w menu g³ównym, lub te¿ poleceniem z paska funkcji: 
Po przejrzeniu raportu mo¿emy rozpocz¹æ usuwanie wirusów z plików jeœli wybraliœmy opcjê Tylko protokó³ lub Przesuñ plik.

Zadania pliku referencyjnego

W przypadku wybrania opcji Tylko protokó³", mo¿emy przyst¹piæ do usuwania znalezionych wirusów (lub zmian referencyjnych).

Je¿eli wybralicemy opcjê Zatrzymaæ analizê udajemy siê do menu:

- Informacje o jednym pliku
- Usuñ wirusa z wybranego pliku
- Usuñ wybrany plik
- Skopiuj wybrany plik (do analizy w G DATA)

Informacje o okreœlonym pliku

Szczegó³owe informacje dotycz¹ce pliku otrzymujemy:

· Przez zaznaczenie znalezionej zmiany i wybranie funkcji Uka¿ informacje" pod has³em Analizuj" w menu g³ównym.

· Podwójne klikniêcie mysz¹ w nazwê zmiany (wirusa)

· Za pomoc¹ opcji Informacje o pliku":

Na górze znajduje siê nazwa pliku, katalogu i rodzaj zmiany referencyjnej. Je¿eli jest to wirus, program informuje o jego stanie. Zazwyczaj mo¿na go usun¹æ z zara¿onego pliku. W przypadku mutacji wirusa (wirusy poliformiczne, które potrafi¹ zmieniaæ swój kod), któr¹ AVK rozpoznaje, ale nie jest w stanie usun¹æ nie niszcz¹c pliku, prosimy o przes³anie nam kopii tego pliku. W ten sposób mo¿emy dokonaæ dok³adnej analizy i zapobiec dalszemu rozprzestrzenianiu siê wirusa.
W oknie atrybutów mamy rozmiar, datê utworzenia, sumê kontroln¹ i nazwê znalezionego wirusa.

Okno zmian, informuje o rodzaju zaistnia³ej zmiany, na przyk³ad o zara¿eniu wirusem i mo¿liwoœciach usuniêcia go lub o zmianie referencyjnej. Poni¿ej znajduj¹ siê ikony pliku referencyjnego.
Wszystkie nieosi¹galne opcje, zaznaczone s¹ jasnoszar¹ czcionk¹ (opcje w tym momencie s¹ nie aktywne).

☞ WSKAZÓWKA: Skutki tych poleceñ, patrz¹c od lewej do prawej, s¹ coraz bardziej niebezpieczne, dlatego proponujemy u¿ywanie ich zawsze w standardowej kolejnoœci (np. w przypadku powy¿szym sensowniej jest usun¹æ wirusa ni¿ ca³y plik.

Usuniêcie wirusów z wybranych plików

... jest mo¿liwe, je¿eli nic nie stoi na przeszkodzie ingerencji programu we wskazany plik. Program usuwa wirus znany, u którego analiza nie wykaza³a mo¿liwoœci póŸniejszych komplikacji. Dziœ na szczêœcie jest tak w wiêkszoœci przypadków. Program bardzo skutecznie rozpoznaje, czy wirus nadaje siê do usuniêcia. Mo¿emy to sprawdziæ poprzez zaznaczenie zara¿onego pliku mysz¹ i:

- Wybranie funkcji Usuñ wirusa w menu g³ównym Analizuj lub
- Naciœniêcie w pasku funkcji: lub
- Podwójne klikniêcie mysz¹ w nazwê pliku i wybranie opcji Usuñ wirusa" w oknie informacji o pliku.

W przypadku wirusa nieznanego lub takiego, który nieodwracalnie uszkodzi³ pliki oryginalne, zaleca siê wys³anie kopii zainfekowanych plików do G DATA, w celu g³êbszej analizy. Zadanie to u³atwi nam wbudowana funkcja.

Kopiowanie wybranych plików (do analizy w G DATA)

W przypadku wirusa nieznanego lub takiego, który nieodwracalnie uszkodzi³ pliki oryginalne, zaleca siê wys³anie kopii zainfekowanych plików do G DATA, w celu g³êbszej analizy. Zadanie to u³atwi nam wbudowana funkcja. Wystarczy w³o¿yæ dyskietkê do stacji i wybraæ plik. Nastêpnie:

- w menu g³ównym wybieramy pod has³em Analizuj" funkcjê Kopiuj plik" lub
- w pasku funkcji wybieramy:  albo

po klikniêciu mysz¹, naciskamy ikonê Usuñ plik" w oknie informacji o pliku.

Wybieramy odpowiedni napêd w oknie wyboru pliku. Nie zmieniajcie Pañstwo lepiej, nazwy pliku. Dyskietki prosimy przesy³aæ pod adres:

G DATA Software Sp. z o.o.
Analiza Wirusów
ul. 28 Lutego 34

78-400 Szczecinek

Usuwanie wybranych plików

Wybrany plik zostanie usuniêty (pojawi siê wczeœniej okno potwierdzenia polecenia), a dane nale¿y ponownie zainstalowaæ. Przewa¿nie nie jest to konieczne i tylko w odosobnionych przypadkach wymagana jest interwencja firmy (produkcja œrodka zaradczego). Adres firmy jak wy¿ej.

UWAGA: W przypadku nieznanego lub zmutowanego wirusa wa¿ne jest wys³anie kopii zara¿onego programu do analizy w G DATA. Do kopiowania plików s³u¿y wbudowana funkcja.

Zainfekowany plik usuwamy zaznaczaj¹c mysz¹ jego nazwê, po czym

- w menu g³ównym pod has³em Analizuj wybieraj¹c funkcjê Usuñ plik" lub
- w pasku funkcji naciskamy na: lub
- klikamy mysz¹ w nazwê pliku i wybieramy opcjê Usuñ plik" w oknie informacji o pliku.

Wyœwietlenie listy wirusów

Znajduj¹ siê tu informacje o najwa¿niejszych wirusach, powoduj¹cych ponad 85% infekcji, dotycz¹ce dróg zara¿ania, rozmiarów, rodzaju i wiele innych.

UWAGA: Lista wirusów, które umieœciliœmy, to tylko spis wa¿niejszych wirusów wybranych przez nas jako przyk³ady. AVK rozpoznaje ich oczywiœcie o wiele wiêcej! Obecnie ponad 8 500.

Zaznaczaj¹c zainfekowany plik, mo¿emy dowiedzieæ siê o rodzaju wirusa wybieraj¹c pod has³em Pomoc" menu g³ównego funkcjê Lista wirusów" lub naciœniêcie w pasku funkcji:

Katalog wirusów

Wirusy od A do F

Wirusy od G do R

Wirusy od S do Z

100 Years
10K
17. November
1701
1704
1704-C
18. September
1808(EXE)
1813(COM)
1-in-8
3551
3555
4096
4711
5120
648
69
765
A-204
Advent
Alabama
Alabama B
Ambulance
Ambulance Car
Anarkia
Anarkia B
Angelina
Anticad
AntiCMOS
Antiexe
Anti-Tel
Apocalypse
Arab Star
Austrian
Azusa
Azusa 2
B1
Basic Virus
Beijing
Black Avenger
Black Box
Black Monday
Black Windows
Blackjack
Bloody!
Bloomington

BNY
Bouncing Ball
Bouncing Ball Boot
Bouncing Dot
Brain Slayer
Bulgarian Horse
Burger
Captain Trips
Captain Trips 2
Cascade
Cascade-B
CD
Century
Chemnitz
Creeping death (CD)
CSSR
Dark Avenger
Dark Avenger 1801
Dark Avenger B
DC10
DC11
DC12
Delwin
Devil´s Dance
Diana
DIR-2
Disk Killer
DJIDDA
Donald Duck
Donnerstag der 12.
DOS-62
DOS-68
Eddie
EXEBug
FAT
Five o´clock virus
Flip
Flip B
Form
Form Boot
FORM-Virus
Freitag, der 13.
French
Friday 13th
Frodo

Wirusy od G do R

- Wirusy od A do F
- Wirusy od S do Z

Generic 1
Generic 2
Generic 3
Generic B
Generic P
Generic virus
Generic F
G-Virus
Hacker
Hafen/NoRedX
Hafen/RedXHafenstraße
Hallo
Hallöchen
Halloween
Happy
Happy Birthday Joshi
Hasita
Hawaii
Hebrew University
Hong Kong
HongKong 1099
Horror
Horse Boot
Horse-Familie
Hungarian
Israeli
Italian
Italian-A
J&M
Jackripper
Jerusalem
Jerusalem-B
Jerusalem-C
Jerusalem-D
Jerusalem-DC
Jerusalem-USA
Joker
Joshi
Jumper
Junkie
Keypress
Killer
LastDirSect
Lenart
Liberty

Macho-A
Maltese Amoeba
Mange tout
Manitoba
Manta
Marijuana
Mendoza
Michelangelo
Monkey
Moonlight
Music Boot
Music Bug
MusicBug
Mystic
New Zealand
NewBug
Noint
Ocker Boot
Off Stealth
Gore
Omega
Mikron
One hal
Parity Boot
Park ESS
Peking
Perfume
Phenomene
Ping Pong
Ping Pong-B
Plastic Bomb
PLASTIQUE
PLASTIQUE 1
PLASTIQUE 2
PLASTIQUE 3012
PLASTIQUE 5.21
PLASTIQUE-B
PLO
possible virus found
Post
Puerto
Quox
Rabid Avenger
Raubkopie
RedX
Reset
Rostov
Russian

Wirusy od S do Z

- Wirusy od A do F
- Wirusy od G do R

Sampo
San Diego
Seventh Son
Sex Revolution
Shirley
Shirley/Vivaldi
Skism-1
Slayer
Slayer A
Slayer B
Slayer C
Slayer D
Slayer E
Slayer-Familie
Smithsonian
Spanish JB
Spanish Telecom
Spanish Telecom 2
Stardot
Stealth
Stealth Virus
Stoned
Stoned II
Storm
SVC V4.00
Swedish Disaster
Swiss 1813
Syslock
Taiwan
Tatou
Telecom
Telecom Boot
Telecom File
Telefonica
Tequila
Timemark
Timemark A
Timemark 1
Toothless Virus
TP04VIR
TP05VIR
TP06VIR
TP16VIR
TP23VIR
TP24VIR
TP25VIR

TP33VIR
TP34VIR
TP38VIR
TP41VIR
TP42VIR
TP44VIR
TP45VIR
TP46VIR
Turku
Twins
Unesco
USSR
USSR 1689
Vacsina
VAN SOFT
Vbasic
VCS-Familie
VDV
VDV2
Vera Cruz
Vien6
Vienna
Vienna 822
Vienna B
Vienna W13
Vienna-B 645
Violetta
VirCheck
Virdem
Virdem 792
Virdem 824
Vivaldi
W13
W13-A
W13-Familie
Wien
Yankee Doodle
Yankee Family

5120

ALIAS: Vbasic, Basic Virus
Wielkoœæ: 5120
TYP: nierezydentny
atakuje pliki COM/EXE
zara¿a COMMAND.COM

OBJAWY: Zara¿one pliki COM rozrastaj¹ siê o 5120 B; Zara¿one pliki EXE rozrastaj¹ siê o 5120 - 5135 B; wystêpuj¹ pozornie nieuzasadnione dostêpy do twardego dysku; przy próbach zara¿enia wirusem, zabezpieczonych przed zapisem plików, wystêpuj¹ od DOS'a komunikaty o b³êdach.

Dzia³anie: 5120 zara¿a dowolne pliki COM i EXE. Uruchomienie zara¿onego programu prowadzi do tego, ¿e w aktualnym katalogu na aktualnej stacji dysku, dalsze pliki COM i EXE zostan¹ zara¿one; poza tym wybrany wg. algorytmu liczb losowych nastêpny plik COM/EXE zostanie zara¿ony w ka¿dym katalogu stacji dysku C:.

W nastêpstwie tego zara¿enia, mog¹ ulec zmianie dane, a pliki systemowe DOS'u mog¹ ulec uszkodzeniu przez b³êdne przyporz¹dkowanie sektorów.

Poza tym: ten wirus powsta³ w skomplikowanym BASICu i dlatego, na koñcu ka¿dego, zara¿onego programu znajduj¹ siê takie s³owa jak: ´BASRUN´, ´BRUN ´, ´IBMBIO.COM´, ´IBMDOS.COM´, ´COMMAND.COM´ lub ´Access denied´. Jednak¿e istnieje odmiana tego wirusa bez wy¿ej wymienionych s³ów.

Anti-Tel

ALIAS: Telecom Boot, Spanish Telecom
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
zara¿a sektor startowy na dyskietkach (Bootsektor)
zara¿a tabelê partycji twardego dysku

OBJAWY: Ca³kowita i dostêpna pamiêæ operacyjna zostanie zredukowana; System-Performance zmniejsza siê; fa³szowanie danych na twardym dysku.

Dzia³anie: Gdy system startuje z dyskietki, która zara¿ona jest wirusem ANTI-TEL, to wirus instaluje siê rezydentnie w górnym koñcu pamiêci operacyjnej, ale zawsze poni¿ej granicy 640KB; program DOS (CHKDSK.COM) pokazuje o 1KB pamiêci mniej ni¿ siê oczekuje. Wirus ANTI-Tel zara¿a bezpoœrednio z pamiêci wszystkie twarde dyski i dyskietki, w których pliki by³y u¿ywane.

Na dyskietkach HD, oryginalny Boot-sektor, przesuniêty zostanie do 28 sektora; wirus kopiuje pierwsz¹ czêœæ swojego kodu programowego do sektora 0, a resztê do sektora 27. Poniewa¿ sektory 27 i 28 nale¿¹ do g³ównego katalogu, wszystkie pliki, które posiadaj¹ odnoœniki do tych sektorów zostan¹ zniszczone.

Na dyskietkach 360KB, oryginalny Boot-sektor, przesuniêty zostanie do 12 sektora; wirus kopiuje pierwsz¹ czêœæ swojego kodu programowego do sektora 0 i resztê do sektora 10. Poniewa¿ sektory 10 i 11 nale¿¹ do g³ównego katalogu, wszystkie pliki, które posiadaj¹ odnoœniki do tych sektorów zostan¹ zniszczone.

Na twardym dysku wirus kopiuje swój kod programowy do tabeli partycji i do sektora 6, na stronê 0, do cylindra 0; tabela partycji zostaje przesuniêta do 7-go sektora. Poniewa¿ DOS normalnie tych sektorów nie u¿ywa, dane zmagazynowane w tym miejscu przez specjalne oprogramowanie, te¿ ulegn¹ zniszczeniu.

ANTI-TEL nale¿y do grupy zamaskowanych wirusów, które u¿ywaj¹ aktywnych œrodków, aby ich odkrycie przez programy szukaj¹ce nie da³o pozytywnego rezultatu; œrodki kamufla¿u wirusa ANTI-TEL nie s¹ programowane czysto i dlatego kamufla¿ nie jest skuteczny dla dyskietek. Skuteczny jest jednak, jeœli chodzi o twardy dysk.

ANTI-TEL uaktywnia siê po 400 ³adowaniach systemu i jest nies³ychanie destrukcyjny. Ukazuje siê wiadomoœæ:

´VIRUS ANTITELEFONICA (BARCELONA)´

i dwa pierwsze dyski twarde zostan¹ zapisane œmieciami.

WARIANTY: **Telecom Boot:** Ten wirus wystêpuje przy zara¿eniach tabeli partycji wirusem TELECOM. Bardzo przypomina on wirus ANTI-TEL, jednak¿e nie zara¿a dyskietek.

Azusa

ALIAS: Hong Kong
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe
atakuje tabelê partycji twardego dysku

OBJAWY: Zmniejszenie ca³kowitego i bêd¹cego do dyspozycji obszaru pamiêci o 1KB; po³¹czenia COM 1 i LPT 1 bêd¹ sparali¿owane po ka¿dym trzydziestym drugim startowaniu systemu.

Dzia³anie: Jak tylko zostanie za³adowany system z zara¿onej dyskietki startowej, wirus AZUSA instaluje siê rezydentnie i kopiuje siê do tabeli partycji, niszcz¹c znajduj¹ce siê tam dane. Przed wirusem nie uratuje siê tabeli partycji. Jeœli wirus jest aktywny, to ka¿de otwarcie pliku do zapisania na w³o¿onej dyskietce lub ka¿de startowanie systemu z dyskietki powoduje, ¿e sektor ³adowania zostanie skopiowany na 40 œcie¿kê w sektorze 8. Na miejsce sektora ³adowania wpisuje siê kopia wirusa. Prowadzi to do tego, ¿e dla dyskietek o pojemnoœci wiêkszej ni¿ 360KB, kopie sektora ³adowania przepisane bêd¹ w œrodek dyskietki i zapisane tam ewentualnie pliki ulegn¹ zniszczeniu. Przy ka¿dym ³adowaniu systemu bêdzie zwiêksza³ siê wewnêtrzny licznik wirusa; gdy licznik osi¹gnie wartoœæ 32, bêdzie ponownie ustawiony na zero i wtedy po³¹czenia COM 1 i LPT 1 bêd¹ sparali¿owane. Dla wartoœci licznika od 1 do 31 po³¹czenia COM 1 i LPT 1 pracuj¹ poprawnie.

WARIANTY: **Azusa 2:** Wielkoœæ 2048B, podobieñstwo objawów jak przy AZUSA, poza tym mo¿liwoœæ z³ego dzia³ania kombinacji klawiszy (Ctrl+C) i zawieszanie siê systemu w trakcie ³adowania go z zainfekowanej dyskietki.

Bloody!

ALIAS: Beijing, Peking
Wielkoœæ: [-]
TYP: rezyduj¹cy w pamiêci
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: Wyd³u¿ony czas startowania systemu, zmniejsza ca³kowity i dostêpny obszar pamiêci. Zg³asza komunikaty na ekranie monitora podczas ³adowania systemu, zmienia zawartoœæ sektora ³adowania i tabeli partycji twardego dysku.

Dzia³anie: BLOODY! atakuje sektory ³adowania na dyskietkach i tabele partycji na twardych dyskach. Gdy uruchamiamy system przy pomocy zara¿onej dyskietki, wirus instaluje siê w pamiêci rezydentnej pod koniec górnego obszaru pamiêci zajmowanej przez DOS, jednak zawsze poni¿ej granicy 640KB i zmniejsza ca³kowity, dostêpny obszar pamiêci o 2KB. Proces ³adowania systemu trwa znacznie d³u¿ej ni¿ normalnie. Gdy system nie jest ³adowany z twardego dysku, natychmiast zostan¹ zara¿one wirusem tabele partycji. Poza tym, przy ka¿dym ³adowaniu systemu zwiêksza siê wewnêtrzny licznik wirusa. Gdy licznik ten osi¹gnie wartoœæ 128, to podczas ³adowania systemu uka¿e siê komunikat:

´Bloody! Jun. 4, 1989´

Ta szczególna data nawi¹zuje do krwawych zamieszek w Pekinie miêdzy chiñskimi studentami, a oddzia³ami wojskowymi.

Ta wiadomoœæ bêdzie ukazywaæ siê przy ka¿dym, dalszym 6-tym procesie ³adowania systemu. Tekst ten, jest zakodowany w wirusie, a wiêc przy ogl¹daniu tabeli partycji jest on niewidoczny. Wirus rezyduj¹cy w pamiêci próbuje zaatakowaæ ka¿dy dysk / dyskietkê, jeœli dokonuje siê dowolnej operacji na znajduj¹cym siê tu pliku lub programie; rozkaz **DIR** nie prowadzi jednak do zara¿enia (nie wzbudza wirusa).

' Uratowany sektor ³aduj¹cy zara¿onej dyskietki 360KB, zostanie zapisany w 11 sektorze, który jest czêœci¹ obszaru katalogu g³ównego; gdy obszar ten by³ u¿ywany, to nale¿¹ce do niego pliki przepadaj¹.
Inne typy dyskietek, mog¹ poprzez kopiê sektora ³adowania, staæ siê nieu¿yteczne lub bêd¹ posiadaæ zniszczone pliki.

Na twardym dysku sektor ³adowania bêdzie kopiowany (przez wirus) na stronê 0, do cylindra 0, do sektora 6.

Cascade, Cascade-B

ALIAS: Blackjack, 1704, 1704-B, 1701 Family
Wielkoœæ: 1704
TYP: rezyduje w pamiêci
atakuje pliki COM
wirus ³¹cz¹cy siê

OBJAWY: Zainfekowane pliki COM powiêkszaj¹ siê o 1704B; nieregularne restartowanie systemu.

Dzia³anie: **Cascade**, **Cascade-B** lub **1701**, **1704** nale¿¹ do najbardziej znanych i rozpowszechnionych wirusów. Wirus **Cascade** znany jest ze specjalnych efektów: spadaj¹cych liter z ekranu monitora. Jest to pierwszy wirus, który potrafi sam siê modyfikowaæ (samokodowanie). **Cascade-B** przypomina wirusa **Cascade**, jednak¿e tu, olbrzymi algorytm liter zosta³ zast¹piony przez proces restartu (gor¹cy start), który jest aktywny, co pewien przypadkowy czas.

WARIANTY: **1704-C:** Dzia³a jak 1704-B, jednak¿e tylko w miesi¹cu grudniu ka¿dego roku.

Dark Avenger

ALIAS: Black Avenger, Eddie, Diana, Rabid Avenger,
VAN SOFT, Dark Avenger 1801
Wielkoœæ: 1800
TYP: rezyduj¹cy w pamiêci
atakuje pliki COM, EXE i OVL

OBJAWY: Pliki COM i EXE zostan¹ powiêkszone; niszczy pliki i dysk twardy

Dzia³anie: **DARK AVENGER** instaluje siê rezydentnie i jest wyj¹tkowo "p³odny", przy atakowaniu plików programowych, które z jakichkolwiek powodów s¹ otwierane. Przy kopiowaniu poleceniem DOS'a COPY lub XCOPY, oryginalne pliki i powsta³e kopie s¹ przez wirus zaatakowane. Zaatakowane pliki powiêkszaj¹ siê o 1800B.

DARK AVENGER jest bardzo podstêpny. Wirus wprowadza licznik do sektora ³adowania. Po ka¿dym 16-tym zaatakowaniu jakiegoœ programu, zostaje wybrany ca³kiem przypadkowy sektor na dysku twardym, do którego zapisze siê czêœæ wirusa. Oryginalna zawartoœæ sektora zostaje zniszczona, programy i pliki nale¿¹ce do tego sektora s¹ nie do uratowania.

Wirus zawiera ³añcuchy znakowe:

´The dark Avenger, copyright 1988, 1989´, ´This program was written in the city of Sofia. Eddie lives... somewhere in time!´

Chocia¿ ten wirus jest prawie tak du¿y jak wirus **JERUSALEM**, nie wykazuje jednak ¿adnych podobieñstw.

WARIANTY: **Dark Avenger-B:** Jest bardzo podobny do **Dark Avenger**. Ró¿nica polega na tym, ¿e pliki COM bêd¹ powtórnie zaatakowane. Wirus ten, inaczej ni¿ orygina³, rezyduje w wy¿szym obszarze pamiêci. Zawarte ³añcuchy znakowe zosta³y lekko zmienione:

´Eddie lives... somewhere in time!´, ´Diana P.´, ´This program was written in the city of Sofia´, ´(C) 1988-1989 Dark Avenger´

Dark Avenger: 1801: Jest o jeden bajt d³u¿szy ni¿ orygina³, rezyduje równie¿ w wy¿szym obszarze pamiêci, jednak nie atakuje powtórnie zara¿onego ju¿ pliku COM.

Rabid Avenger: Bazuje na **Dark Avenger-B**, zajmuje 3696B w górnym obszarze pamiêci DOS, jednak zawsze poni¿ej granicy 640KB; zaatakowane pliki bêd¹ zwiêkszone o 1806-1823B; poza tym, wariant ten zosta³ tak zmieniony, ¿e nie zostaje rozpoznawany przez znawców wirusów jako wariant **Black Avenger**. £añcuchy znakowe w wirusie:

´<- Thanks to Dark Avenger ->´, ´Eat us!´, ´(C) 1991 RABID International

Development Corp!´, ´Scan String Killer Test´

Van Soft: Odró¿nia siê od orygina³u g³ównie poprzez teksty, które maj¹ postaæ (dla drukarki s¹ to znaki niewidoczne):

´V.A.N. Soft & MMMM PRESENT :SOFIA´, ´VAN&MMMM´

Zainfekowane programy COM zostan¹ zwiêkszone o 1800B, pliki EXE ulegn¹ zwiêkszeniu o 1806-1824B; wirus dopisuje siê do koñca pliku.

Flip

ALIAS: Omicron
Wielkoœæ: 2343 lub 2153
TYP: rezyduje w pamiêci
atakuje pliki COM, EXE i OVL
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: Pliki COM i EXE zostan¹ powiêkszone; zmniejsza siê ca³kowity i dostêpny obszar pamiêci; pojawiaj¹ siê b³êdy przyporz¹dkowania plików; sektor ³adowania i tabele partycji bêd¹ zmienione.

Dzia³anie: Startuj¹cy plik (zaatakowany) *.EXE przez wirus **FLIP**, wpisuje wirus w górnym obszarze pamiêci. Ca³kowity i bêd¹cy do dyspozycji obszar pamiêci (wg. programu DOS'a CHKDSK.COM) zmniejsza siê o 3064B. Poza tym, C:\COMMAND.COM, o ile wystêpuje, bêdzie zaatakowany; tak d³ugo jak ten wirus jest aktywny w pamiêci, zmiany wielkoœci s¹ niezauwa¿alne. Poza tym dokonuj¹ siê zmiany w sektorze ³adowania w tabeli partycji. Na dyskietkach zmiany wielkoœci danej COMMAND.COM s¹ dostrzegalne.

Ka¿dy wykonywany program wraz z plikiem nak³adkowym (Overlay), bêdzie zaatakowany.

Zazwyczaj wystêpuj¹ b³êdy przyporz¹dkowania plików, które mog¹ zniszczyæ pliki dane.

Ka¿dego dnia miesi¹ca, miêdzy godzin¹ 16:00 i 16:59, mog¹ wyst¹piæ na ekranie monitora strony pozamieniane w poziomie, w systemie, który zosta³ wystartowany z zara¿onego wirusem twardego dysku i który zarz¹dzany jest przez adapter EGA lub VGA.

Wirus nie atakuje ¿adnych dalszych plików, jeœli zosta³ wystartowany z pliku COM lub z sektora ³adowania; dalsze przenoszenie wirusa jest mo¿liwe tylko poprzez pliki EXE.

WARIANTY: **Flip-B:** jest trochê mniejszy (2153B) ni¿ orygina³; te warianty rozprzestrzeniaj¹ siê nie tylko przez pliki EXE, lecz tak¿e przez tabele partycji twardego dysku.

FORM-Virus

ALIAS: Form, Form Boot
Wielkoœæ: [-]
TYP: rezyduj¹cy w pamiêci
atakuje sektory startowe dyskietek

OBJAWY: Odg³osy klikania w g³oœniku komputera.

Dzia³anie: Jeœli system po raz pierwszy uruchamiany jest z dyskietki startowej zara¿onej wirusem **FORM**, to wirus instaluje siê w pamiêci i równie¿ atakuje sektor startowy na twardym dysku. Proces startowania systemu z zara¿onej dyskietki mo¿e siê nie udaæ, poniewa¿ system siê zawiesza. W wirusie mo¿e siê znajdowaæ taki tekst:

´The Form-Virus sends greetings to everyone who´s reading this text. FORM doesn´t destroy data! Don´t panic. Fuckings go to Corinne.´

W zaatakowanym systemie, pocz¹wszy od 24-dnia ka¿dego miesi¹ca, mo¿na us³yszeæ odg³osy klikania w g³oœniku komputera.

Tê formê wirusa mo¿na w prosty sposób przy pomocy rozkazu DOS'a SYS.COM usun¹æ (SYS A: C:).

Hallöchen

ALIAS: [-]
Wielkoœæ: 2011
TYP: rezyduje w pamiêci
wirus ³¹cz¹cy siê
atakuje pliki COM i EXE

OBJAWY: Zaatakowane pliki COM zwiêkszaj¹ siê o 2011-2026B, zaatakowane pliki EXE zwiêkszaj¹ siê o 2011-2026B; wprowadzone dane z klawiatury bêdê fa³szowane (nie do rozpoznania).

Dzia³anie: **HALLÖCHEN** instaluje siê rezydentnie w pamiêci, jak tylko uruchomi siê zainfekowany program, chyba, ¿e wielkoœæ zaatakowanego programu przekracza 64KB lub program ten utworzony bêdzie z dat¹ miesi¹ca i roku zgodnego z danymi systemu. Wirus powiêksza zara¿ony program do najbli¿szej ca³kowitej wielokrotnoœci liczby 16, zanim dopisze on swoj¹ kopiê o d³ugoœci 2011B do zainfekowanego programu. Jeœli wirus bêdzie aktywny, to wprowadzone dane z klawiatury s¹ nie do rozpoznania.

Jerusalem

ALIAS: PLO, Israeli, Friday 13th, Russian, 1813(COM), 1808(EXE)
Wielkoœæ: 1813 do 1808
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE bêd¹ powiêkszone; efektywnoœæ systemu (System performance) zmniejszy siê; pliki bêd¹ kasowane w ka¿dy pi¹tek 13-tego w miesi¹cu; pojawi siê czarne okno na ekranie monitora.

Dzia³anie: **JERUSALEM** odwraca przerwanie nr 8; w 30 minut po wywo³aniu zara¿onego programu, jego efektywnoœæ systemowa wynosi 10% pocz¹tkowej prêdkoœci programu. Niektóre odmiany pokazuj¹ na dole, z lewej strony ekranu czarne okno, które przy korzystaniu z funkcji przewijania ekranu (Skrolowanie) wêdruje do góry ekranu.

13 (trzynastego) wypadaj¹cego w pi¹tek, bêd¹ kasowane wszystkie u¿ywane programy zara¿onego systemu.

W niektórych wariantach, znajduje siê ³añcuch tekstowy ´sUMsDos´, jednak¿e nowsze warianty nie posiadaj¹ tego tekstu.

Jerusalem-B

ALIAS: Arab Star, Black Box, Black Window, Hebrew University
Wielkoœæ: 1813
TYP: rezyduje w pamiêci
atakuje pliki EXE, OVL, COM i SYS.

OBJAWY: Pliki COM i EXE bêd¹ powiêkszone; efektywnoœæ systemu zmaleje; pliki bêd¹ kasowane ka¿dego trzynastego w pi¹tek w miesi¹cu; czarne okno na ekranie monitora.

Dzia³anie: Wirus **JERUSALEM-B** jest praktycznie identyczny jak **JERUSALEM**, poza tym, ¿e nie wystêpuje wielokrotne zara¿enie plików EXE.

JERUSALEM-B jest jednym z najbardziej rozpowszechnionych wirusów.

Nie wszystkie warianty zmieniaj¹ efektywnoœæ systemu. Wirus staje siê aktywny, jeœli o danej dacie, poprzez start zara¿onego programu dociera do pamiêci. Znajduj¹c siê w pamiêci, gdy data siê zmieni³a, nie jest aktywny.

WARIANTY: **A-204:** Tekst ´sUMsDOs´ zosta³ zmieniony na ´*A-204´, kodowanie zosta³o zmienione, aby zapobiec rozpoznawaniu przez detektywa wirusów (Skaner wirusów). Ten wariant zmniejsza prêdkoœæ systemu i wyœwietla na ekranie monitora czarne okno.

Anarkia: Podobnie, jak orygina³, jednak¿e prêdkoœæ systemu bêdzie bardziej zmniejszona, przy czym czas trwania zmniejszonej prêdkoœci systemu jest znacznie d³u¿szy. Nie wyœwietla siê ¿adne czarne okno; tekst ´sUMsDOs´ bêdzie zast¹piony przez ´Anarkia´. Ten wariant wirusa staje siê aktywny ka¿dego trzynastego wtorku, jeœli wypada on w danym miesi¹cu.

Anarkia-B: Dzia³a podobnie jak **Anarkia**, jednak¿e wirus staje siê aktywny zawsze dwunastego paŸdziernika.

Apocalypse: Ten wariant atakuje programy podczas ich pracy. Pliki COM rosn¹ o 1808-1822 B przy pierwszej infekcji, przy nastêpnych o 1808 B . Tekst ´MsDos´ bêdzie zast¹piony przez ´C.J**´. Po 30 minutach w zaatakowanym systemie, ukazuje siê charakterystyczne czarne okno. Ten wirus nie kasuje plików.

Captain Trips: Nazwa pochodzi od wystêpuj¹cego tu ³añcucha znakowego 'Capitan Trips'. W tym wariancie nie wyœwietla siê ¿adne czarne okno na ekranie, nie zmniejsza siê prêdkoœæ systemu i programy nie s¹ kasowane w pi¹tek trzynastego. Pliki COM rozrastaj¹ siê o 1813B. Pliki EXE rozrastaj¹ siê o 1808-1822B przy pierwszej infekcji, przy nastêpnej infekcji rozrastaj¹ siê o 1808B.

Captain Trips 2: Jest to wariant wersji 'Capitan Trips'**,** która zosta³a zmieniona po to, aby nie byæ rozpoznawaln¹ przez programy wyszukuj¹ce wirusy. Pliki EXE rozrastaj¹ siê o 1808B.

Jerusalem-C: Podobny do **Jerusalem-B**, jednak z normalnym czasem zmniejszania prêdkoœci systemu.

Jerusalem-D: Wariant **Jerusalem-C**, który w ka¿dy pi¹tek trzynastego po 1990 roku, niszczy obydwie kopie FAT.

Jerusalem-DC: Podobny do **Jerusalem-B**; tekst ´sUMsDOs´ wyspacjowany; po 30 minutach zmniejsza siê efektywnoœæ systemu o 30% i wyœwietla siê czarne okno. Ten wariant nie ma ¿adnej daty pobudzaj¹cej go do aktywnoœci.

Jerusalem-E: Wariant **Jerusalem-D**, który w ka¿dy pi¹tek trzynastego, po 1992 roku niszczy obie kopie FAT.

Jerusalem USA: Jak **Jerusalem-C**, kasuje tak¿e w pi¹tek, wg. generatora liczb losowych przypadkowe pliki i FAT.

Mendoza: Jak **Jerusalem-B** ale nie atakuje plików EXE. Jest aktywny w miesi¹cach od lipca do grudnia. Ka¿dego dnia istnieje 10% szans zniszczenia wszystkich aktywnych programów.

Park ESS: Zwalnia system o 20%, czarne okno ukazuje siê po 30-tu minutach.

Phenomene: Podobny do wirusa Apocalypse, atakuje tak¿e plik COMMAND.COM. Wirus zawiera tekst ´Phenomene.COM´.

Puerto: Podobny do wirusa Mendoza; reinfekuje pliki EXE.

Skism-1: Du¿e podobieñstwo do innych wariantów i orygina³u. Jest aktywny od roku 1991-go w ka¿dy pi¹tek, po 15-tym. W tych dniach rozmiary wszystkich aktywnych plików bêd¹ skrócone do zera. Rozmiary plików typu COM rosn¹ o 1808, a plików EXE o 1808-1822 bajtów. Wprowadza czarne okno i hamuje pracê systemu.

Spanish JB: Nazywany tak¿e ´Jerusalem-F´ lub ´Jerusalem-E2´; nie wprowadza czarnego okna, reinfekuje pliki EXE.

Swiss 1813: Brak czarnego okna, nie usuwa plików, nie zwalnia pracy systemu.

Joshi

ALIAS: Happy Birthday Joshi, Stealth Virus
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: System zawiesza siê; komunikat na ekranie monitora

Dzia³anie: Po za³adowaniu systemu z dyskietki startowej zara¿onej wirusem **JOSHI**. Wirus instaluje siê rezydentnie w pamiêci i zajmuje oko³o 6KB; podobnie wygl¹da komunikat rozkazu CHKDSK.COM.

JOSHI wykazuje podobieñstwo do dwóch wirusów:
- podobnie, jak wirus **Stoned**, atakuje tabele partycji dysku twardego,
- podobnie, jak wirus **Brain**, pokazuje przy próbie czytania sektora zawieraj¹cego tabelê partycji, kopiê tego sektora.

5 stycznia ka¿dego roku system nie chce siê za³adowaæ, towarzyszy temu nastêpuj¹cy komunikat na ekranie:

´type Happy Birthday Joshi´

Jeœli u¿ytkownik wprowadzi z klawiatury wy¿ej wymieniony tekst: ´**Happy Birthday Joshi**´, mo¿e dalej korzystaæ z systemu.

Jeœli dwa pierwsze bajty sektora startowego dyskietki maj¹ wartoœæ 'EB' i '1F', to znaczy, ¿e dyskietka jest zara¿ona przez wirus **JOSHI**. Faktyczny kod programowy wirusa znajduje siê na 41 œcie¿ce 360KB dyskietce lub na 81 œcie¿ce dyskietki 1.2MB.

Te dwie wartoœci 'EB' i '1F' znajduj¹ siê te¿ w sektorze, w którym normalnie zawarta jest tabela partycji twardego dysku. Kopia tabeli partycji znajduje siê na œcie¿ce 0 w 9-tym sektorze.

Michelangelo

ALIAS: [-]
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

Dzia³anie: **MICHELANGELO** instaluje siê rezydentnie w pamiêci, jeœli system po raz pierwszy ³adowany jest z zara¿onej dyskietki, a tak¿e wtedy, gdy ³adowanie systemu koñczy siê niepomyœlnie. Ca³kowity i bêd¹cy do dyspozycji obszar pamiêci zmniejsza siê o 2KB, które wirus zajmuje w górnym obszarze pamiêci, ale zawsze poni¿ej granicy 640KB. Wirus broni siê przed nowym zapisem przez inne programy. Atakuje niezainfekowane dyskietki, gdy tylko ma do nich dostêp; bêd¹ zaatakowane tabele partycji na twardym dysku, je¿eli wykonamy dowolne operacje na plikach znajduj¹cych siê na twardym dysku.

Na 360KB dyskietkach, oryginalny sektor startowy systemu zostanie przeniesiony przez wirus do sektora 11 (ostatni sektor g³ównego katalogu), a przy dyskietkach 1,2MB na 28 sektor (równie¿ do sektora g³ównego drzewa).Je¿eli sektor ten by³ przez katalogi wykorzystywany, to zapisane pliki ulegn¹ zniszczeniu.

Sektor z tabel¹ partycji zostanie przepisany przez wirus do sektora 7, na œcie¿kê 0, do cylindra 0.

Wirus przystêpuje do ataku 6-go marca, gdzie ca³y dysk twardy zostanie zapisany przez zawartoœæ pamiêci operacyjnej.

W swojej konstrukcji, wirus ten, jest podobny do wirusa Stoned.

MusicBug

ALIAS: Music Boot, Music Bug
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: Zmniejszenie ca³kowitego i dostêpnego obszaru pamiêci; odg³osy klikania; zniszczone obszary na dysku twardym; muzyka w dowolnych momentach.

Dzia³anie: **MUSIC BUG** instaluje siê rezydentnie w pamiêci, gdy system ³aduje siê pierwszy raz, z zara¿onej dyskietki startowej. Ca³kowity i bêd¹cy do dyspozycji obszar pamiêci zmniejsza siê o 2KB, które wirus zajmuje w górnym obszarze pamiêci, ale zawsze poni¿ej granicy 640KB. Wirus broni siê przed nowym zapisem przez inne programy. Podczas ³adowania systemu z zara¿onej dyskietki / dysku twardego, mog¹ wyst¹piæ odg³osy klikania w g³oœniku komputera, jednak¿e czêœciej mog¹ to byæ krótkie kawa³ki melodii.

Jeœli wirus zainstalowa³ siê rezydentnie w pamiêci, to przy ka¿dym korzystaniu z dyskietki / dysku twardego us³yszymy dalsze czêœci melodii. Poza tym, ka¿da dyskietka / dysk twardy zostanie zaatakowany, je¿eli bêdzie u¿yty. Na dysku twardym bêdzie zara¿ony sektor startowy i tabela partycji. Poza tym program DOS'a CHKDSK, wykazuje 4096B w straconych obszarach, które zawieraj¹ wirusa i kopiê oryginalnego sektora ³adowania; w tych 4096B znajduje siê miêdzy innymi nastêpuj¹cy tekst:

´MusicBug v1.06. Macrosoft Corp.´, ´Made in Taiwan´

NoInt

ALIAS: Bloomington, LastDirSect
Wielkoœæ: [-]
TYP: rezyduje w pamiêci, ukryty
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: Ca³kowity i dostêpny obszar pamiêci bêdzie zredukowany; katalogi bêd¹ zniszczone.

Dzia³anie: **NOINT** ³aduje siê rezydentnie do pamiêci, gdy system jest startowany po raz pierwszy z zainfekowanej dyskietki. Ca³kowita i dostêpna pamiêæ zostanie o 2KB zmniejszona, któr¹ wirus zajmuje dla siebie pod koniec górnego obszaru pamiêci, jednak¿e zawsze poni¿ej granicy 640KB. Po tym czasie tabela partycji bêdzie ju¿ zaatakowana.

Sektor tabeli partycji zostanie przepisany do sektora 7, na stronê 0, do cylindra 0.

Dla dyskietek 360KB, bêdzie przez wirus przepisany oryginalny sektor ³adowania do sektora 11 (ostatni sektor g³ównego katalogu), a dla dyskietek 1.2MB na sektor 17 (równie¿ do g³ównego katalogu). Je¿eli by³y te sektory, rzeczywiœcie przez katalogi wykorzystywane, to odpowiednie pliki ulegn¹ zniszczeniu. Wirus **NOINT** nie daje ¿adnych komunikatów przy uruchamianiu systemu; dostêp do systemu /dysku twardego oraz proces startowania systemu trwa znacznie d³u¿ej, ni¿ przy nie zainfekowanym systemie. £adowanie systemu z nie zara¿onej dyskietki startowej 1.2MB, czêsto bywa przerywane z powodu b³êdu ³adowania systemu..

Perfume

ALIAS: 765, 4711, G-Virus
Wielkoœæ: 765
TYP: atakuje pliki COM

OBJAWY: Pliki COM rozrastaj¹ siê, a na ekranie monitora pojawia siê komunikat.

Dzia³anie: **PERFUME** atakuje tylko pliki COM, a szczególnie szuka COMMAND.COM. Wirus czasami zadaje pytanie w czasie uruchamiania zainfekowanego programu i startuje ten program, jeœli na to pytanie otrzyma odpowiedŸ '4711'. Istnieje szeroko rozpowszechniona wersja tego wirusa, gdzie pytania zosta³y zapisane przez zupe³nie przypadkowe liczby.

Ping Pong

ALIAS: Bouncing Ball, Bouncing Dot, Italian, Vera Cruz
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

Dzia³anie: Jeœli **PING PONG** uaktywnia siê (wg. algorytmu liczb losowych), wyœwietla siê na ekranie monitora pi³ka podskakuj¹ca w ko³o, która mo¿e byæ usuniêta tylko przez nowe za³adowanie systemu. Inne szkody nie s¹ znane.

Oryginalny wirus atakuje tylko dyskietki.
.

Ping Pong-B

ALIAS: Bouncing Ball Boot, Italian-A
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

Dzia³anie: **PING PONG-B** jest odmian¹ wirusa **PING PONG**; g³ówna ró¿nica polega na tym, ¿e **PING PONG-B** atakuje tak¿e twardy dysk. Wirus ten, podobnie jak wirus FROM mo¿e zostaæ usuniêty rozkazem DOS'a SYS (równie¿ PING PONG-C).

WARIANTY: **Ping Pong-C:** podobny do Ping Pong-B, jednak¿e bez grafiki.

PLASTIQUE

ALIAS: Plastic Bomb, Plastique 3012, Plastique 1, Anticad
Wielkoœæ: 3012
TYP: rezyduje w pamiêci
Wirus ³¹czy siê
atakuje sektory startowe dyskietek
atakuje pliki COM i EXE
nie atakuje COMMAND.COM

OBJAWY: Dzia³anie wirusa jest zale¿ne od daty systemu; zainfekowane pliki COM i EXE zwiêkszaj¹ siê o 3012-3020B; nie infekuje sektorów startowych dyskietek; odg³osy eksplozji w g³oœniku komputera; efektywnoœæ systemu pozornie maleje.

Dzia³anie: Przy pierwszym starcie zainfekowanego programu, instaluje siê PLASTIQUE rezydentnie w pamiêci i zajmuje przy tym 3264B, w dolnym obszarze pamiêci. Wirus próbuje zaraziæ ka¿dy plik COM/EXE, który jest u¿ywany lub tylko otwierany; zainfekowane pliki COM rozrastaj¹ siê o 3012B, pliki EXE o 3020B.

Je¿eli data systemu jest wiêksza od 20 wrzeœnia danego roku, wtedy wirus jest z³oœliwy i wytwarza odg³osy eksplozji w g³oœniku lub wci¹¿ siê domaga wiêkszej pojemnoœci procesora, tak, ¿e normalna praca komputera zostanie sparali¿owana.

WARIANTY: **HM2:** Wirus nie powiela siê. U¿ycie zara¿onego pliku powoduje zawieszenie siê systemu.

Plastique 4.21: Wyró¿nia siê tylko mo¿liwoœci¹ samodzielnego kodowania.

Plastique COBOL: Zawiera s³owo ´COBOL´; pliki COM rozrastaj¹ siê o 3004B; pliki EXE o 3004-3019B; wirus staje siê z³oœliwy, je¿eli data systemu le¿y miêdzy 1.01 a 21.09; system zmniejsza swoj¹ prêdkoœæ obliczeniow¹ i po 20 minutach, mo¿liwoœci systemu wynosz¹ 50%, a po 30 minutach klawiatura bêdzie unieruchomiona, a pamiêæ konfiguracji systemu CMOS, zostaje na nowo przez wirus zapisana. Od 22.09 rozpoczyna siê stan spokoju i trwa do stycznia nastêpnego roku..

PLASTIQUE-B

ALIAS: Plastique 5.21, Plastique 2
Wielkoœæ: 4096
TYP: rezyduje w pamiêci
Wirus ³¹czy siê
atakuje sektory startowe dyskietek
atakuje pliki COM i EXE
nie atakuje COMMAND.COM

OBJAWY: Ulepszona wersja wirusa **PLASTIQUE**; dzia³a zale¿nie od daty systemu; zara¿one pliki COM i EXE rozrastaj¹ siê o dalsze 4096B.

.

Dzia³anie: Przy pierwszym starcie zara¿onego programu instaluje siê **PLASTIQUE-B** rezydentnie w pamiêci. Wirus zajmuje 5120B i zapisuje siê:
- w dolnym obszarze pamiêci, jeœli data systemu le¿y przed dniem 20.09 danego roku;
- w górnym obszarze pamiêci, jeœli data systemu le¿y po dniu 20.09 danego roku.

Ka¿dy otwarty lub zastartowany plik COM/EXE zostanie zainfekowany.

Wirus **PLASTIQUE-B** atakuje sektor startowy w³o¿onej, do stacji dysków dyskietki. Je¿eli data systemu znajduje siê po 20.09.1990 roku, wirus bêdzie z³oœliwy i wytwarza odg³osy eksplozji w g³oœniku komputera lub wci¹¿ siê domaga wiêkszej pojemnoœci procesora, tak, ¿e normalna praca komputera zostanie sparali¿owana. Poza tym, po przekroczeniu dowolnie ustalonej wartoœci licznika zainstalowanego w wirusie, do wszystkich stacji dysków zostan¹ wys³ane bezsensowne dane..

Slayer Familie

ALIAS: Brain Slayer, Slayer
Wielkoœæ: 5120
TYP: atakuje pliki COM i EXE

OBJAWY: Zawartoœæ plików COM i EXE ulegnie zwiêkszeniu; wystêpuj¹ zmiany w katalogach; nieoczekiwany dostêp do wszystkich stacji dysków; nieoczekiwanie d³ugi czas dostêpu do dysku twardego.

Dzia³anie: Gdy zosta³ uruchomiony program zainfekowany wirusem, to bêd¹ zaatakowane przez **SLAYER** wszystkie pliki COM i EXE w aktualnym katalogu. W zale¿noœci od wariantu wirusa, zostan¹ zaatakowane te¿ programy w innych stacjach dysków. Zara¿one programy rozrastaj¹ siê o dalsze 5120-5135B; wirus znajduje siê zawsze na koñcu programu. W zara¿onych katalogach data i czas nie ulega zmianie. Jednak¿e mo¿e siê zdarzyæ, ¿e w zara¿onych katalogach, na samym pocz¹tku wystêpuj¹ tylko pliki COM.

Co najmniej jeden wariant z rodziny wirusa **SLAYER**, wprowadza ze sob¹ wirusa **YANKEE-DOODLE**, który po jakimœ czasie rozprzestrzenia siê w systemie.

WARIANTY: **SLAYER-A:** Zara¿a dodatkowo pliki w aktywnym katalogu, aktywnej stacji dysku (do dziewiêciu plików w podkatalogu), ale nie w g³ównym katalogu stacji dysku C:.

SLAYER-B: Dzia³a podobnie jak **SLAYER-A**, jednak zaatakowane bêd¹ równie¿ pliki w g³ównym katalogu w C:.

SLAYER-C: Dzia³a podobnie jak **SLAYER-A**, jednak zaatakowane bêd¹ wszystkie pliki programowe w C:. Poza tym, wirus ten zawiera nastêpuj¹ce znaki:

´KEYB*.COM KEYB*.EXE BASRUN BRUN COBRUN NETDOS*.COM´
´IBMBIO.COM´, ´IBMDOS.COM COMMAND.COM *.* .. \ .. *.EXE´
´Access denied´

SLAYER-D: Dzia³a podobnie jak **SLAYER-C**, jednak ¿adne pliki w C: nie bêd¹ zara¿one, chyba, ¿e z twardego dysku startowany bêdzie zara¿ony program.

SLAYER-E: Znany jako **YANKEE-DOODLE-DROPPER**. Przy startowaniu zara¿onego programu, zostan¹ zara¿one wszystkie programy w aktualnym katalogu aktualnej stacji dysku oraz niektóre pliki w C:. Po up³ywie jakiegoœ czasu, wirus ten wpisuje wirusa **YANKEE-DOODLE** i uaktywnia go. Gdy zostanie wirus **YANKEE-DOODLE** usuniêty, to wirus **SLAYER-E** powoduje nowe infekcje poprzez wprowadzanie wirusa **YANKEE-DOODLE**.

Stoned

ALIAS: Donald Duck, Hawaii, Marijuana, New Zealand
Rostov, San Diego, Sex Revolution, Smithsonian
Stoned II, Bloody, Beijing, Swedish Desaster, NoInt
Bloomington, Angelina, Manitoba

Wielkoœæ: [-]

TYP: rezyduje w pamiêci
atakuje sektory startowe dyskietek
atakuje tabelê partycji twardego dysku

OBJAWY: Komunikaty na ekranie; zawieszaj¹ siê RRL-kontrolery.

Dzia³anie: Pierwotna wersja infekowa³a tylko dyskietki 360KB, bez wyrz¹dzania wiêkszych szkód, tego wariantu ju¿ jednak nie ma. Wszystkie teraŸniejsze warianty tego wirusa zara¿aj¹ tabelê partycji twardego dysku, gdzie g³ówny katalog i FAT bêd¹ uszkodzone. Te wirusy rozró¿niane s¹ pod wzglêdem komunikatów wysy³anych na ekran w czasie startowania systemu.

Startowanie systemu z zara¿onej dyskietki przez wirus **STONED** powoduje, ¿e wirus instaluje siê rezydentnie w g³ównym obszarze pamiêci i zajmuje przy tym ok. 2KB pamiêci. Odpowiednio wygl¹da wynik zg³oszony przez rozkaz CHKDSK.COM. Gdy tabele partycji twardego dysku do tej pory nie by³y zara¿one przez wirus, to teraz to nast¹pi.

Podczas ³adowania bêd¹ wysy³ane na ekran monitora przypadkowo wybrane komunikaty, najczêœciej:

'Your Computer is now stoned.´

Z pamiêci operacyjnej, wirus **STONED** zara¿a wszystkie dyskietki, które by³y u¿ywane. Przy tym przepisany zostaje oryginalny sektor startowy do 11 sektora, podczas gdy wirus kopiuje siê do w³aœciwego sektora startowego. Sektor 11 jest czêœci¹ g³ówn¹ katalogu; jeœli by³ on przed zainfekowaniem u¿ywany, to zawarte tam pliki ulegn¹ zniszczeniu. Dla niektórych wersji DOS'a, sektor 11 nale¿y do FAT'u, tak wiêc przez t¹ infekcjê FAT (tablica rozmieszczenia plików) bêdzie zniszczona.

Przy zara¿eniu twardego dysku, zostan¹ oryginalne tabele partycji skopiowane do sektora 7, na stronê 0, do cylindra 0, podczas, gdy wirus wpisuje siê w miejsce w³aœciwego sektora tabeli partycji. Gdy twardy dysk zosta³ przy pomocy odpowiedniego oprogramowania sformatowany, oraz bezpoœrednio za sektorem tabeli partycji znajduje siê sektor startowy i FAT lub g³ówny katalog, to w konsekwencji zara¿enia twardego dysku, mo¿e on zostaæ uszkodzony.

WARIANTY: **PS-STONED:** Bazuje na wirusie **STONED**, zosta³ jednak tak zmieniony, ¿e jego odkrycie mo¿e byæ uniemo¿liwione. Przy ³adowaniu systemu nie wysy³a ¿adnych komunikatów na ekran. Poza tym atakuje wszystkie typy dyskietek.

ROSTOV: Podobny do **STONED-B**; nie pokazuje ¿adnych informacji; zawiera nastêpuj¹cy tekst: ´Replace and strike´sowie ´Non-system disk´.

SEX REVOLUTION V1.1: Taki jak **STONED-B**; wysy³a na ekran nastêpuj¹cy tekst:

´EXPORT OF SEX REVOLUTION ver 1.1.´

SEX REVOLUTION V2.0: Taki jak **Sex Revolution v1.1**; wysy³a na ekran nastêpuj¹cy tekst:

´EXPORT OF SEX REVOLUTION ver 2.0.´

STONED-A: Taki jak orygina³, nie atakuje jednak dysków twardych. Jest to prawersja. Zawiera tekst: Ýour computer is now stoned. Legalize Marijuana´. Ukazana bêdzie tylko wiadomoœæ do ´... stoned´.

STONED-B: Taki jak orygina³. Zawiesza pracê systemów wyposa¿onych w sterowniki dysków twardych typu RLL.

STONED-C: Taki jak orygina³. Nie wysy³a jednak na ekran tekstu.

STONED-D: Taki jak orygina³; atakuje dyskietki w formacie 3.5 i dyski twarde.

STONED-E: Podobny do STONED-B; wysy³a na ekran tekst: ´LEGALIZE MARIJUANA´ poprzedzony sygna³em dŸwiêkowym. Znajduje siê w sektorze startowym i tabeli partycji.

STONED-F: Podobny do STONED-E; wysy³any na ekran tekst brzmi: ´Twój PC jest teraz be!´. ´LEGALIZE MARIJUANA´ znajduje siê w sektorze startowym i tabeli partycji.

STONED II: Podobny do STONED-B; jednak wyposa¿ony jest w mechanizm chroni¹cy go przed odkryciem; Wysy³any na ekran tekst brzmi: ´Your PC is now Stoned! Version 2´, lub tak¿e: ´Donald Duck is a lie!´.

Syslock

ALIAS: 3551, 3555
Wielkoœæ: 3551
TYP: ukryty (zakodowany)
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE bêd¹ zwiêkszone; pliki zostan¹ zmienione.

Dzia³anie: **SYSLOCK** przeszukuje aktywne drzewo katalogów twardego dysku, wyszukuje pliki COM i EXE, wybiera przypadkowo jeden z nich i zara¿a go. Plik bêdzie zwiêkszony o ok. 3551B (lub trochê wiêcej).

Pliki bêd¹ zmienione. Wirus szuka w zara¿onych plikach s³owa ´Microsoft´ (niezale¿nie, czy pisane du¿ymi, czy ma³ymi literami) i zastêpuje je s³owem ´MACROSOFT´.

Gdy w œrodowisku DOS'a (DOS-Environment) wirus znajdzie tekst: ´SYSLOCK=@´, to nie wykazuje ¿adnej aktywnoœci i od razu startuje program zarz¹dzaj¹cy systemem.

WARIANTY: **ADVENT:** Normalnie nie powielaj¹cy siê wirus. Prawdopodobnie, zwielokrotnianie siê wirusa wystêpuje wtedy, gdy zosta³ zara¿ony plik EXE; jego potomkowie atakuj¹ tylko pliki COM.

MACHO-A: Zachowuje siê tak jak **SYSLOCK**, lecz s³owo ´Microsoft´ zostaje tu zast¹pione przez ´Macrosoft´..

Telecom

ALIAS: Telefonica, Telecom File, Spanish Telecom-2
Wielkoœæ: 3700
TYP: rezyduje w pamiêci
ukryty
atakuje pliki COM

OBJAWY: Pliki COM bêd¹ zwiêkszone; ca³kowita i dostêpna pamiêæ zmniejszy siê; twardy dysk zostanie sformatowany; rozsiewa wirus **ANTI-TEL**.

Dzia³anie: Je¿eli zostanie za³adowany system z zainfekowanej dyskietki, to **TELECOM** instaluje siê rezydentnie pod koniec górnego obszaru pamiêci, ale zawsze poni¿ej granicy 640KB; program DOS'a CHKDSK.COM pokazuje o 3984B mniej pamiêci. Przerwanie nr 21 zostaje odwrócone. Rezyduj¹cy w pamiêci wirus **ANTI-TEL** atakuje twarde dyski i dyskietki, które by³y u¿ywane.

W plikach COM, rezyduj¹cych w pamiêci, przekraczaj¹cych wielkoœæ 1KB, zainfekowanych wirusem w czasie u¿ywania, nastêpuje wzrost ich wielkoœci o 3700B; to zwiêkszenie siê pliku, nie jest widoczne w katalogu, poniewa¿ wirus to uniemo¿liwia.
Data zara¿onego katalogu bêdzie o 100 lat przesuniêta do przodu, jednak jest to niewidoczne w katalogu, poniewa¿ s¹ wyœwietlane tylko dwie ostatnie cyfry roku. Na podstawie daty pliku, wirus rozpoznaje, czy dany plik jest ju¿ zara¿ony, czy te¿ nie.

Rezyduj¹cy w pamiêci **TELECOM** zara¿a tabelê partycji twardego dysku, jeœli tylko jego dowolny plik by³ u¿ywany. Zara¿ona czêœæ pliku przez **TELECOM** nie uaktywnia siê, ale po 400 procesach startowania systemu, przepisuje wirus **ANTI-TEL** na pierwsze dwa twarde dyski.

Tequila

ALIAS: Stealth
Wielkoœæ: 2468
TYP: atakuje tabelê partycji twardego dysku
atakuje pliki EXE

OBJAWY: Ca³kowity i bêd¹cy do dyspozycji obszar pamiêci zostanie zredukowany o 3072B.

Dzia³anie: Wirus sprawdza przy pierwszym starcie zara¿onego programu, czy tabele partycji twardego dysku s¹ ju¿ zara¿one, je¿eli nie, to wpisuje swoj¹ niezakodowan¹ kopiê do ostatnich szeœciu sektorów twardego dysku i zmienia tabele partycji w taki sposób, ¿e s³u¿¹ one do dalszego zara¿ania. Do tego czasu wirus nie instaluje siê rezydentnie w pamiêci i nie zara¿a dalszych plików.

Gdy system bêdzie pierwszy raz startowany z zara¿onego twardego dysku, wirus instaluje siê rezydentnie w pamiêci. Ca³kowita i dostêpna pamiêæ zredukuje siê o 3KB, które wirus zajmuje dla siebie w górnym obszarze pamiêci, ale zawsze poni¿ej granicy 640KB. Wirus zabezpiecza siê przed nowym zapisem przez inne programy.
Gdy wirus rezyduje w pamiêci, zara¿a ka¿dy wywo³any program EXE. Wirus dopisuje siê do koñca programu i zwiêksza go o 2468B, jednak to zwiêkszenie siê programu, nie jest widoczne w katalogu, poniewa¿ wirus rezyduje tylko w pamiêci.

Nastêpuj¹cy niezakodowany tekst znajduje siê w ostatnim sektorze zara¿onego twardego dysku:

´Welcome to T.TEQUILA´s latest production.
Contact T.TEQUILA /P.O.Box 543/6312 St´hausen Switzerland. Loving thought to L.I.N.D.A.
BEER and TEQUILA forever !´

Pora¿one wirusem programy zawieraj¹ tekst w zakodowanej formie.

Zaatakowane systemy, przy wywo³aniu programu DOS'a CHKDSK.COM zg³aszaj¹ komunikat 'B³¹d przyporz¹dkowania plików', gdy wirus rezyduje w pamiêci. Jeœli ten program bêdzie wywo³any z opcj¹ /f, to programy mog¹ zostaæ zniszczone.

Dok³adnie, cztery miesi¹ce po zara¿eniu tabeli partycji, w danym dniu miesi¹ca, wirus staje siê znowu aktywny, podaj¹c komunikat na ekran:

´Execute: mov ax, FE03 / int 21. Key to go on´.

Przy wywo³aniu programu, który zawiera maszynowe rozkazy, zostanie pokazany komunikat z ostatniego sektora twardego dysku.
Wirus TEQUILA, jest bardzo rozpowszechniony w Europie. Wirus ten zosta³ rozpowszechniony przez pewne szwajcarskie przedsiêbiorstwo wysy³kowe.

Autorzy pomys³u zostali aresztowani. Wirus potrafi siê ca³kowicie zakodowaæ i to w wielu dowolnych wariantach. Jest trudny do zidentyfikowania. Poprzez niektóre zrêczne mechanizmy, jest on niewidoczny dla u¿ytkownika i uwa¿any za jeden z najbardziej inteligentnych wœród wirusów.

USSR 1689

ALIAS: SVC V4.00, Off Stealth
Wielkoœæ: 1689
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Zwiêksza pliki COM i EXE; System zawiesza siê.

Dzia³anie: USSR 1689 instaluje siê przez uruchomienie pierwszego zara¿onego programu rezyduj¹cego w pamiêci, w rezydentnej czêœci interpretera rozkazów. Najbli¿szy program COM lub EXE zostanie zaatakowany, który z kolei bêdzie przyczyn¹ powiêkszania siê systemu. Zara¿one programy zwiêkszaj¹ siê o 1689B, ale ten wzrost programów, które przed zara¿eniem s¹ wiêksze ni¿ 1689B jest przez wirus skutecznie ukryty. Pliki, które by³y mniejsze ni¿ 1689B (przed zara¿eniem wirusem), bêd¹ zwiêkszone i bêdzie to zauwa¿alne w katalogu. Wirus dopisuje siê zawsze na koniec programu.

Przy ka¿dym zara¿eniu programu, wystêpuje zawieszenie siê systemu i dlatego wirus ten, tak szybko siê nie rozprzestrzenia jak inne wirusy i przez to mo¿na go wczeœniej wykryæ.

Vacsina

ALIAS: [-]
Wielkoœæ: 1206
TYP: rezyduje w pamiêci
atakuje pliki COM, EXE, SYS i BIN

OBJAWY: Pliki COM, EXE, SYS i BIN rozrastaj¹ siê; Sygna³ pisku w g³oœniku komputera.

Dzia³anie: **VACSINA** atakuje pliki COM, EXE, SYS i BIN. Pliki EXE zostan¹ zamienione na pliki COM (pierwsze 2 bajty 'ZM' lub 'MZ' pliku bêd¹ w rozkazie JMP zamienione w do³¹czonym kodzie wirusa, który zawiera w³asn¹ procedurê przesuniêæ).

Wirus ten wystêpuje w bogatej formie wariantów (co najmniej 48). Cech¹ charakterystyczn¹ zara¿onego programu jest to, ¿e przy jego wywo³aniu, s³ychaæ piski w g³oœniku komputera; poza tym ulega zmianie czas i data w katalogu, które to (czas i data) zmieniaj¹ siê na takie, jakie by³y w katalogu w momencie zaatakowania przez wirus.

WARIANTY: **TP04VIR:** Zara¿a pliki EXE i zamienia je wewnêtrznie na pliki COM. Zaatakowane programy zawieraj¹ tekst 'VACSINA', a przedostatni bajt zawiera binarn¹ czwórkê.

TP05VIR: Podobny do **TP04VIR**, jednak¿e drugi od koñca bajt zawiera binarn¹ pi¹tkê. Poza tym czasami system zawiesza siê.

TP06VIR: Podobny do **TP05VIR**, jednak¿e drugi od koñca bajt zawiera binarn¹ szóstkê.

TP16VIR: Podobny do **TP06VIR**, jednak¿e drugi od koñca bajt zawiera binarn¹ szesnastkê.

TP23VIR: Podobny do **TP16VIR**, jednak¿e drugi od koñca bajt zawiera binarne 23. Tekst 'VACSINA' nie wystêpuje.

TP24VIR: Podobny do **TP16VIR**, jednak¿e drugi od koñca bajt zawiera binarne 24.

TP25VIR: Podobny do **TP16VIR**, jednak¿e drugi od koñca bajt zawiera binarne 25.

Vienna

ALIAS: Austrian, Unesco, DOS-62, 648, DOS-68, 1-in-8
Wielkoœæ: 648
TYP: atakuje pliki COM

OBJAWY: Pliki COM rozrastaj¹ siê; System zawiesza siê w czasie jego ³adowania.

Dzia³anie: Uruchamiaj¹c program zara¿ony przez **VIENNA**, zara¿a siê nastêpny program niezainfekowany (przez ten wirus) w aktualnym katalogu. Plik zwiêksza siê o 648B, a wirus znajduje siê na koñcu pliku. W katalogu, zostan¹ wartoœci sekund ustawione na 62, dla zara¿onego programu. Na 6 zaatakowanych programów, tylko jeden program bêdzie bez wirusa, ale za to pierwszych 5 bajtów programu zamienione zostanie na skok do procedury uruchamiaj¹cej restart systemu. Po uruchomieniu program / system samoistnie ³aduje siê od nowa. Poniewa¿ wirus nie dopisuje siê do programu, jest trudny do odkrycia przez skenery szukaj¹ce. Nawet po usuniêciu wirusa, mog¹ powstaæ nie przewidziane skutki, a¿ wszystkie zmienione programy zostan¹ wymienione na niezara¿one kopie, co daje gwarancjê, ¿e system nie jest zainfekowany.

Przy niektórych zaatakowanych programach, mo¿e wyst¹piæ te¿ zawieszenie siê systemu, gdy programy te bêd¹ startowane.

Wirus **VIENNA** zosta³ zaprogramowany przez pewnego studenta, a program Ÿród³owy tego wirusa zosta³ opublikowany, dlatego jest tak du¿o odmian i wariantów tego wirusa, i dlatego te¿ mog¹ wyst¹piæ jeszcze inne symptomy tego wirusa, ni¿ te które zosta³y wymienione.

WARIANTY: **VIENNA 822:** Podobny do orygina³u, jednak ma wielkoœæ 822B. Nie kasuje plików, nie wywo³uje nieoczekiwanego ³adowania siê systemu (tzw. gor¹cego startu).

VIEN6: Podobny do orygina³u; ma tak¹ sam¹ wielkoœæ; nie wywo³uje ³adowania siê systemu (tzw. gor¹cego startu). Po zara¿eniu 7 plików w aktualnym katalogu, zostan¹ zara¿one pliki w C:.

VIENNA-B: Podobny do orygina³u, jednak zamiast modyfikacji restartu jednego z szeœciu zara¿onych plików, zostanie skasowany wywo³any aktualnie program.

VIENNA-B 645: Podobny do orygina³u, lecz bez modyfikacji restartu i bez kasowania zara¿onych plików.

WIEN: Tak, jak orygina³, jednak posiada œrodki uniemo¿liwiaj¹ce jego odkrycie..

W13

ALIAS: Toothless Virus, W13-A
Wielkoœæ: 534
TYP: atakuje pliki COM

OBJAWY: Pliki COM bêd¹ powiêkszone.

Dzia³anie: W13 poza czystym zainfekowaniem, nie wyrz¹dza ¿adnych innych szkód. Jest on spokrewniony z wirusem **VIENNA**, nie uszkadza plików i nie wykazuje ¿adnych innych efektów, jak wirus **VIENNA**. Poza tym, zawiera on w sobie parê b³êdów, które mu przeszkadzaj¹ w rozprzestrzenianiu siê.

WARIANTY: **W13-A:** Niektóre b³êdy, które uniemo¿liwia³y rozrastanie siê wirusa, zosta³y usuniête. Ten wariant wirusa ma wielkoœæ 507B.

Yankee Doodle

ALIAS: TP44VIR, Five O´Clock Virus, Yankee Family
Wielkoœæ: 2885 lub 2899
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE rozrastaj¹ siê; o godzinie 5:00 (wg. zegara systemowego), zabrzmi melodia z g³oœnika komputera.

Dzia³anie: Jeœli zostanie uruchomiony zara¿ony program, instaluje siê **YANKEE DOODLE** rezydentnie w pamiêci i zara¿a pliki COM i EXE. Gdy zegar systemowy osi¹gnie godzinê 5:00 po po³udniu, to z g³oœnika komputera rozbrzmiewa melodia Yankee-Doodle. Poza zainfekowaniem plików, nie wyrz¹dza ¿adnych innych szkód.

Wirus Yankee Family obejmuje ok. 80 ró¿nych wirusów..

WARIANTY: **TP33VIR:** Ten wariant zmienia po kryjomu przerwanie nr 1 i 3 tak, ¿e nie mo¿na wiêcej u¿yæ program Debugger do œledzenia wirusa. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 33 dziesiêtnie).

TP34VIR: Podobny do **TP33VIR**, jednak rezyduje w pamiêci i zara¿a programy, gdy s¹ one u¿ywane. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 34 dziesiêtnie).

TP38VIR: Podobny do **TP34VIR**, lecz ró¿nie traktuje pliki COM i EXE. Poza tym, wirus sam siê odka¿a, jeœli program zosta³ wystartowany przez CodeView-Debugger. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 38 dziesiêtnie).

TP41VIR: Podobny do **TP38VIR**. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 41 dziesiêtnie).

TP42VIR: Ten wariant sprawdza, czy system jest zara¿ony wirusem **PING PONG** i modyfikuje go, w tym sensie, ¿e wirus ten sam siê niszczy. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 42 dziesiêtnie).

TP44VIR: Podobny do **TP42VIR**. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 44 dziesiêtnie).

TP45VIR: Podobny do **TP44VIR**. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 45 dziesiêtnie).

TP46VIR: Ta wersja sprawdza, czy system zosta³ zaatakowany przez wirusa **CASCADA (1701)** i niszczy go. Ostatnie 2 bajty wirusa zawieraj¹ nr wersji (tu: 46 dziesiêtnie).

4096

ALIAS: Century, Frodo, 100 Years
Wielkoœæ: 4096
TYP: rezyduje w pamiêci
atakuje pliki COM, EXE i OVL
b³êdny FAT

OBJAWY: Pliki COM i EXE bêd¹ powiêkszone; System zawiesza siê; Silne zmniejszenie prêdkoœci roboczej systemu.

Dzia³anie: Gdy wirus znajduje siê w pamiêci, nie wyœwietlaj¹ siê przy pomocy polecenia DIR, zmienione wielkoœci plików. Wirus atakuje ka¿dy wykonywany (uruchamiany) plik. Niszczy FAT poprzez Crosslinking. Ka¿dego roku w dniu 22.09 system zawiesza siê.

Osobliwoœci: Prawdopodobnie, w wirusie znajduje siê b³¹d, który koñczy siê pêtl¹ programu. Bez tego b³êdu by³by zmieniany sektor ³adowania, co powinno wyœwietliæ nastêpuj¹cy komunikat:
´**FRODO lives**´

DIR-2

ALIAS: Creeping Death (CD), FAT
Wielkoœæ: [-]
TYP: inteligentny, rezyduj¹cy w pamiêci wirus Stealth
wirus sektora startowego
FAT-Crosslinking

OBJAWY: Zgubiony Cluster; przy kopiowaniu pliki zostan¹ zniszczone; jeœli system bêdzie startowany z dyskietki, to rozkaz CHKDSK zg³osi zgubione ³añcuchy (Crosslinking); CHKDSK /F niszczy pliki !!!.

!

Dzia³anie: Wirus **DIR-2** jest bardzo szybki, uaktywnia siê podczas ³adowania systemu z zara¿onej stacji dysków lub twardego dysku. Jest bardzo trudny do wykrycia, poniewa¿ nie posiada ¿adnych widocznych cech charakterystycznych. Wirus nie atakuje plików programowych, lecz zmienia FAT (tablicê przydzieleñ plików). Po zara¿eniu dyskietki, wpisuje siê on do ostatniego clustera na dyskietce.

Osobliwoœci: **DIR-2** wprowadza swój cluster (adres startowy) do FAT dla ka¿dego programu. Oryginalny cluster programów zostanie umieszczony w poszczególnym pliku. Jedyny rozpoznawalny efekt to: wszystkie pliki posiadaj¹ zagubione ³añcuchy (s¹ crosslinked) w jednym cluster, w którym znajduje siê wirus. Próba korekcji tego przy pomocy CHKDSK /f powoduje zniszczenie pliku.

WARIANTY: DC10, DC11, DC12

Parity Boot

ALIAS: [-]
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
wirus sektora ³adowania tzw. Bootsektor
Wirus Stealth

OBJAWY: Wirus sektora startowego (tzw. Bootsektor), który rezyduje w pamiêci; Zg³asza PARITY CHECK ERROR, SYSTEMSTOP

Dzia³anie: **PARITY BOOT** (b³¹d parzystoœci przy startowaniu systemu). Zalicza siê do doœæ dobrze rozpowszechnionych w ostatnim czasie wirusów, sektora startowego. Zosta³ on napisany jesieni¹ 1992 roku, prawdopodobnie w Niemczech. Od po³owy 1993 roku, wystêpuje on we wzmocnionej formie. Na podstawie jego szczególnych Stealth-w³aœciwoœci, znajduje siê on w komputerze w stanie utajonym i zara¿a ka¿d¹ dyskietkê sformatowan¹ na tym komputerze. Wirus **PARITY BOOT** zapamiêtuje orygina³ sektora ³adowania i kieruje ka¿de odpytanie sektora ³adowania do zapamiêtanego orygina³u, skutkiem tego jest to, ¿e programy antywirusowe w zara¿onym systemie z trudem mog¹ go zidentyfikowaæ..

Delwin

ALIAS: [-]
Wielkoœæ: 1759
TYP: rezyduje w pamiêci
atakuje pliki EXE i tablicê partycji (MBR)

OBJAWY: Wirus rezyduje w pamiêci i infekuje (zara¿a) Masterbootrecord. Wirus zajmuje 2KB w pamiêci. Powiêksza pliki EXE o 1759 Bajtów. Oryginaln¹ tabelê partycji przenosi i zapisuje w Sektor 0,0,2.

Dzia³anie: Wirus posiada bardzo szkodliwe funkcje! Potrafi odczytaæ datê systemow¹ i dokonaæ w niej skomplikowanych operacji (zara¿aj¹c okreœla iloœæ sekund w pliku). Powoduje np to: ¿e uruchamiamy zara¿one pliki, które pocz¹tkowe litery maj¹ np: WI, na pytanie o wersjê DOS, wirus podaje 2.10, co prowadzi do unieruchomienia wielu programów, które pracuj¹ na wersjach wy¿szych.

Junkie

ALIAS: (-)
Wielkoœæ: 1030-1024
TYP: rezyduje w pamiêci
atakuje pliki EXE, COM i tabelê partycji (MBR)

OBJAWY: Wirus powsta³ prawdopodobnie w Szwecji. Wirus rezyduje w pamiêci i tabeli partycji (MBR). Przy uruchamianiu zainfekowanych plików z rozszerzeniem COM, atakuje wirusem Junkie dwa pierwsze sektory twardego dysku. D³ugoœæ wirusa wynosi 1024 Bajty. Wirus potrafi zmieniaæ swoj¹ d³ugoœæ ale nie jest poliformiczny (samokoduj¹cy).

Dzia³anie: Wirus w swym wnêtrzu posiada tekst:
Dr. White - Schweden - 1994 Junkie Virus - written in Malmo
Powy¿szych tekstów nigdy nie wyœwietla. Program unieruchamia (wy³¹cza), rezyduj¹ce programy antywirusowe.

Sampo

ALIAS: 69, WLLOP
Wielkoœæ: (-)
TYP: rezyduje w pamiêci
atakuje tabelê partycji (MBR)

OBJAWY: Wirus powsta³ na Filipinach. Atakuje sektor startowy dyskietek (tzw. Bootsektor) i tabele partycji dysku twardego. Przy starcie komputera wirus Sampo zara¿a z g³ównej pamiêci, w której rezyduje.

Dzia³anie: Aktywny wirus wydaje komunikat:
SAMPO Projekt X Copyrigt © by the SAMO X-Team. All rights reserved.
Univerity Of The East Manila.
Nie wyrz¹dza wiêkszych szkód. Rozpowszechniony jest g³ównie w Norwegii i Anglii.

Hasita

ALIAS: J&M
Wielkoœæ: (-)
TYP: rezyduje w pamiêci
atakuje tabelê partycji (MBR)

OBJAWY Wirus zara¿a Bootsektor dyskietek i tabelê partycji dysku twardego. Wirus rozpowszechniony w Skandynawii.

Dzia³anie: Wirus posiada wbudowane, bardzo szkodliwe funkcje czasowe. Ka¿dego 15 listopada formatuje pierwsze sektory twardego dysku.

Jackripper

ALIAS: (-)
Wielkoœæ: (-)
TYP: rezyduje w pamiêci
atakuje tablicê partycji (MBR)

OBJAWY Wirus zara¿a sektory startowe dyskietek (Bootsektor) i tabelê partycji twardego dysku.

Dzia³anie: Wirus posiada bardzo szkodliwe dzia³anie. Zamienia miejscami dwa nastêpuj¹ce po sobie bajty z prawdopodobieñstwem 1/1024. Zachodzi to tylko przy zapisie na twardym dysku. Tym samym niszczy pliki. Odbudowanie ich struktur nie jest mo¿liwe. Kod ³añcuchowy zawiera tekst: FUCK EM UP!

Jumper

ALIAS: French
Wielkoœæ: [-]
TYP: rezyduje w pamiêci
atakuje tablicê partycji (MBR)

OBJAWY: Wirus atakuje Bootsektor dyskietek i tabelê partycji twardego dysku. Pierwsze wiadomoœci o wirusie pochodz¹ z 1993 roku. Prawdopodobnie pochodzi z Francji. Kod wirusa wpisuje siê w system komunikatów Bootsektor'a.

Dzia³anie: Z prawdopodobieñstwem 3% przy startowaniu systemu, pojawi¹ siê nastêpuj¹ce znaki .
Informacje bootsektora dyskietek zostan¹ przeniesione do ostatniego sektora katalogu g³ównego. W przypadku dyskietek 5. 25", s¹ przeniesione do sektora 5-ego.

One_half

ALIAS: (-)
Wielkoœæ: zmienna
TYP: rezyduje w pamiêci
atakuje pliki COM, EXE oraz tablicê partycji (MBR)

OBJAWY: Wirus atakuje sektory startowe dyskietek (tzw. Bootsektor) i tablicê partycji dysku twardego. Z tego powodu zara¿ane s¹ pliki COM i EXE. Pliki powiêksza o 3.544 Bajty. Wirus jest poliformiczny.
Rozpoznanie utrudnione z powodu w³aœciwoœci "czapki niewidki".

Dzia³anie: Wirus zamyka dwa cylindry partycji DOS. Dopóki jest aktywny, u¿ycie programu jest mo¿liwe ze wzglêdu na swoist¹ strukturê wirusa. Usuwanie poleceniem FDISK /MBR prowadzi czêsto do straty danych. Znakiem rozpoznawczym s¹ zniszczone pliki, blokada Windows lub ca³kowita blokada komputera.One_half zawiera nastêpuj¹cy kod:

Dis is one half. Ress any key to continue... Did you leave the room?

Monkey

ALIAS: (-)
Wielkoœæ: (-)
TYP: rezyduje w pamiêci
atakuje tablicê partycji (MBR)

OBJAWY Wirus atakuje sektor startowy dyskietek (tzw. Bootsektor) i tabelê partycji dysku twardego. Ma w³aœciwoœci "czapki niewidki".

Dzia³anie Atakuje tabelê partycji i zamyka j¹. Niemo¿liwe usuniêcie poleceniem FDISK /MBR. Dotychczas nie uda³o siê go usun¹æ.

Ambulance

ALIAS: RedX
Wielkoœæ: 796
TYP: rezyduje w pamiêci
atakuje pliki COM

OBJAWY Wirus Ambulance powiêksza pliki COM o 796 Bajtów. Znany jest wariant wirusa o d³ugoœci 1067 Bajtów.

Dzia³anie W momencie, kiedy wirus jest aktywny, pokazuje siê na ekranie monitora karetka. Dodatkowo s³yszalny jest jej sygna³ alarmowy.

Black Monday

ALIAS: (-)
Wielkoœæ: 1055
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY Wirus powiêksza pliki COM i EXE o 1055 Bajtów.

Dzia³anie Komunikuje siê: Black Monday 2/3/90 KV KL MAL. Nie da siê go usun¹æ ca³kowicie z plików EXE, poniewa¿ niszczy i zapisuje czêœci pliku.

Quox

ALIAS: (-)
Wielkoœæ: 1024
TYP: rezyduje w pamiêci
atakuje tablicê partycji (MBR)

OBJAWY Wirus atakuje tabelê partycji (Bootsektor) na dyskietkach i twardym dysku.

Dzia³anie Wirus wpisuje siê do pamiêci g³ównej komputera.

Seventh son

ALIAS: (-)
Wielkoœæ: 332
TYP: nie rezyduje w pamiêci

OBJAWY Wirus atakuje pliki COM

Dzia³anie Brak szerszych informacji.

Maltese Amoeba

ALIAS: (-)
Wielkoœæ: (-)
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Wirus atakuje pliki COM i EXE

Dzia³anie: Brak informacji.

Halloween

ALIAS: Hallo, Happy, 10K
Wielkoœæ: 1376, 10000
Pochodzenie: Koniec 1991
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Atakuje pliki COM/EXE. Niektóre programy wywo³uj¹ *Runtime Error*. 31.paŸdziernika (Halloween) ukazuje siê na ekranie komunikat, a pliki powiêkszaj¹ siê
10 KB.

Dzia³anie: Pliki przed³u¿one o 10 KB prowadz¹ do komunikatów RuntimeError.

Szkody:

WARIANTY:

Raubkopie

ALIAS: [-]
D³ugoœæ: 2219
Pochodzenie: Niemcy (BRD)
TYP: rezyduje w pamiêci
atakuje pliki COM

OBJAWY: Wirus atakuje pliki COM.

Dzia³anie: Nie jest znane.

WARIANTY: Znana jest wersja o d³ugoœci 1888 Bajtów

Mange-tout

ALIAS: HongKong 1099
Wielkoœæ: 1099
Pochodzenie: HongKong z VGA-Treibern
TYP: rezyduje w pamiêci
atakuje pliki COM i EXE

OBJAWY: Atakuje pliki COM/EXE. Wirus korzysta z systemów kodowania, co utrudnia proces wykrycia i usuniêcia.

Dzia³anie: Nie jest znane.

WARIANTY: Znana jest wersja o d³ugoœci 1091 Bajtów.

Boot1

ALIAS: B1, BNY
Wielkoœæ: (-)
Pochodzenie: [-]
TYP: rezyduje w pamiêci, infekuje dyskietki: Bootsektor,
twardy dysk: tabela partycji

OBJAWY: Wirus atakuje Bootsektor dyskietek wzgl. tabelê partycji dysku twardego. Zaprogramowany doœæ prosto. Zara¿a tabelê partycji, przy starcie z zara¿onej dyskietki. Zara¿a wszystkie niezabezpieczone dyskietki, kiedy jest rezydentny.

Szkody: Brak szczegó³ów. Przy zara¿eniu dyskietek, dochodzi niekiedy do utraty danych.

WARIANTY: Nie s¹ znane inne warianty wirusa.

Omega

ALIAS: Reset, Freitag der 13.
Wielkoœæ: 440
Pochodzenie: Finlandia
TYP: nie rezydentny, atakuje pliki COM

OBJAWY: Wirus atakuje pliki COM. Infekuje tabele partycji ka¿dego pi¹tku dnia 13.

Dzia³anie: Wirus zrobiony doœæ prosto. Przy wywo³aniu zara¿onego programu wirus przeszukuje katalog i zara¿a wszystkie pliki COM.

Szkody: W ka¿dy pi¹tek 13-ego wyœwietla znak i zajmuje dwa pierwsze sektory dysku twardego. Niszczy przez to tabelê partycji i pliki s¹ nieodwracalnie stracone.

WARIANTY: Nie s¹ znane inne warianty.

Alabama

ALIAS: (-)
Wielkoœæ: 1560
Pochodzenie: Izrael lub Alabama (USA)
TYP: rezydentny, atakuje pliki EXE

OBJAWY: Wirus atakuje pliki EXE. Komunikuje siê. Uruchamia niewywo³ane programy.

Dzia³anie: Zaprogramowany z fantazj¹. Przy wywo³aniu zara¿onego programu staje siê rezydentny. Przy wywo³aniu nastêpnego programu, szuka niezara¿onego pliku, zara¿a go i dopiero gdy nie znajdzie ¿adnego niezainfekowanego, infekuje plik uruchamiany.

Szkody: W trybie DOS po ok. 2 godzinach uka¿e siê komunikat: Tuscambia ALABAMA

WARIANTY: Znana jest wersja **Alabama B.** Do dnia dzisiejszego jeszcze dok³adnie nie zanalizowana.

Disk Killer

ALIAS: Ogre, Ocker Boot
Wielkoœæ: (-)
Pochodzenie: USA
TYP: rezydentny, atakuje tabelê partycji

OBJAWY: Wirus zara¿a tabele partycji (Bootsektory) u¿ywanych dyskietek i twardych dysków.

Dzia³anie: Uwa¿any jest za niebezpieczny wirus bootsektorowy. Dysponuje wszystkimi w³aœciwoœciami nowoczesnego wirusa atakuj¹cego bootsektor. Godne uwagi s¹ wyrz¹dzane przez niego szkody.

Szkody: Wirus zamyka wszystkie pliki na twardym dysku, kiedy komputer dzia³a d³u¿ej ni¿ 24 godziny. Do³¹cza komunikat: DISK KILLER Version 1.00

WARIANTY:

Stardot

ALIAS: 18. September
Wielkoœæ: pliki EXE - 600, 789 lub 801
Pochodzenie: [-]
TYP: nie rezydentny, zara¿a pliki COM i EXE, niebezpieczny

OBJAWY: Wirus atakuje pliki COM i EXE. Zapisuje twardy dysk 18 wrzeœnia o godzinie 7.

Dzia³anie: Najpierw do³¹cza do ka¿dego pliku 10-16 B, nastêpnie atakuje plik. Prowadzi to do problemów, jeœli nie usuniemy go dok³adnie.

Szkody: Jak wskazuje nazwa, wirus uaktywnia siê 18. wrzeœnia o godz. 7 i zajmuje dysk twardy.

WARIANTY: Znany jest w 3 ró¿nych wariantach d³ugoœci.

Mystic

ALIAS: Liberty
Wielkoœæ: 2857
Pochodzenie: Po³udniowo-wschodnia Azja
TYP: rezydentny, atakuje pliki EXE i COM

OBJAWY: Wirus zara¿a pliki EXE/COM. Pierwsze 120 B zajmuje tekstem: M Y S T I C Copyright 1989. Prowadzi to do problemów, kiedy u¿ywamy tego obszaru pliku albo usuniemy wirusa. Samoczynnie doczepia siê do pliku.

Dzia³anie: Dzia³anie i szkody nie s¹ jeszcze dok³adnie znane.

Szkody: [-]

WARIANTY: Znanych jest kilka wariantów ale jeszcze nie zosta³y poddane analizie.

Shirley

Alias: (-)
Wielkoœæ: 4096
Pochodzenie: prawdopodobnie z Niemiec (BRD)
Typ: rezydentny, atakuje pliki EXE

OBJAWY: Wirus zara¿a pliki EXE.

Dzia³anie: Wirus zaprogramowany w sposób skomplikowany. Zawiera wielowierszowy tekst w jêzyku niemieckim, st¹d podejrzenie o pochodzeniu. Nie zanalizowano go jeszcze dok³adnie.

Szkody: (-)

WARIANTY: Znanych jest kilka wariantów np: **Vivaldi**

Vivaldi

Alias: Shirley/Vivaldi
Wielkoœæ: [-]
Pochodzenie: [-]
Typ: rezydentny, atakuje pliki EXE

OBJAWY: Wirus zara¿a pliki EXE.

Dzia³anie: Wirus jest jeszcze dok³adnie nie zanalizowany. Jest to wersja wirusa Shirley i w kodzie zawiera tekst: VIVALDI

Szkody:

WARIANTY:

Virdem

Alias: Burger, Virdem792 ,Virdem 824, Killer
Wielkoœæ: 1336
Pochodzenie: Niemcy (BRD) 1986 rok
Typ: nie rezydentny, atakuje pliki COM

OBJAWY: Wirus zara¿a pliki COM.

Dzia³anie: Jest to jeden z najstarszych wirusów. Zosta³ zaprogramowany jako wirus demonstracyjny w roku 1986 przez R. Burgera. R. Burger u¿y³ go jako przyk³adu ostrzegawczego do swej ksi¹¿ki Computer Viruses. Wariant pierwotny meldowa³ o zara¿eniu i umo¿liwia³ naprawê. Nowe warianty posiadaj¹ komunikat o zmienionej treœci lub nie posiadaj¹ go.

Szkody: Nie czyni powa¿nych szkód.

WARIANTY: Znane s¹ ró¿norodne warianty tego wirusa.

Donnerstag der 12.

Alias: CD, VirCheck
Wielkoœæ: 2161
Pochodzenie: Niemcy (BRD)
Typ: rezydentny, atakuje pliki EXE i COM

OBJAWY: Wirus zara¿a pliki EXE i COM. W ka¿dy czwartek dnia 12, komunikat w jêzyku niemieckim.

Dzia³anie: Wirus jest bardzo dobrze zaprogramowany. Ka¿dego czwartku 12 dnia wysy³a komunikat: Morgen ist Freitag der 13 (jutro jest pi¹tek 13). Swoj¹ nazwê VirCheck zawdziêcza faktowi ¿e podszywa siê pod program antywirusowy.

Szkody:

WARIANTY:

W-13-Familie

Alias: Vienna W13, REQ/Polen, CSSR, USSR
Wielkoœæ: 507-534
Pochodzenie: Europa Wschodnia
Typ: nie rezydentny, atakuje pliki COM

OBJAWY: Wirus zara¿a pliki COM.

Dzia³anie: Ta rodzina wirusów jest prymitywnie zaprogramowana i bazuje na wirusie Vienna.

Szkody: Brak szczegó³ów.

WARIANTY: wszystkie warianty s¹ nam znane.

Horse-Familie

Alias: Bulgarian horse , Hacker
Wielkoœæ: (-)
Pochodzenie: Bu³garia
Typ: rezydentny, atakuje pliki COM i EXE

OBJAWY: Ta rodzina wirusów wydaje siê byæ seri¹ eksperymentaln¹. Jest on (jak na razie) doœæ prosto zaprogramowany, a wszystkie wersje pochodz¹ prawdopodobnie z r¹k jednego programisty. Powsta³y dot¹d dwa ró¿norodne warianty (10 ró¿nych wersji). Oprócz tego pojawi³ siê wirus bootsektorowy, Horse Boot Virus. Prawdopodobnie w przygotowaniu jest wersja multiplikuj¹ca.

Dzia³anie: Nie stwierdzono szkodliwego dzia³ania.

Szkody: (-)

WARIANTY: Znanych jest 10 wersji wirusa i jedna wersja atakuj¹ca Bootsektor (patrz Horse Boot).

Horse Boot

Alias: Bulgarian Horse
Wielkoœæ: (-)
Pochodzenie: Bu³garia
Typ: rezydentny, atakuje sektory startowe dyskietek Bootsektor, tabelê partycji twardego dysku

OBJAWY: Wirus zara¿a sektory startowe dyskietek (Bootsektor) i tabele partycji twardego dysku.

Dzia³anie: Wirus zaprogramowany doœæ prosto.

Szkody: Nie znane s¹ meldunki o powodowaniu jakichkolwiek szkód.

WARIANTY: Nale¿y prawdopodobnie do eksperymentalnej serii wirusów HORSE.

VCS Familie

Alias: (-)
Wielkoœæ: 1077 + - Tekst
Pochodzenie: Niemcy
Typ: nie rezydentny, atakuje pliki COM, lekkie szkody

OBJAWY: Wirus zara¿a pliki COM. Usuwa AUTOEXEC.BAT i CONFIG.SYS

Dzia³anie: Rodzina wirusów bazuje na programie Constuction Set.
Tworzy on wirusy wyœwietlaj¹ce ¿¹dany tekst po up³ywie dowolnego czasu. W koñcu usuwa AUTOEXEC.BAT i CONFIG.SYS.

Szkody: Po dowolnej liczbie infekcji, niszczy AUTOEXEC.BAT i CONFIG.SYS

WARIANTY: **Manta:** zawiera tekst dowcipu o kierowcach samochodu marki Opel Manta.

POST: zawiera tekst: zur Bundespost.

VDV: zawiera tekst: Verband Deutscher Vierenliebhaber.

VDV2: zawiera tekst ¿yczeñ bo¿onarodzeniowych VDV (Zwi¹zku Niemieckich Mi³oœników Wirusów)

Hafenstraße

Alias: (-)
Wielkoœæ: 809,781,1641
Pochodzenie: Niemcy
Typ: nie rezydentny, atakuje pliki EXE

OBJAWY: Wirus zara¿a pliki EXE.

Dzia³anie: Wirus prosto zaprogramowany. Przy wywo³aniu zara¿onego programu atakuje 1 kolejny plik.

Szkody: Przy wywo³aniu tworzy ukryty plik zawieraj¹cy tekst: Hafenstraße bleibt ! Prowadzi to to problemów z pamiêci¹ w katalogu g³ównym (zajmuje miejsce na twardym dysku).

WARIANTY: Hafen/RedX; Ambulance Car; Hafen/NoRedX
Interesuj¹cy wariant! Wirus Ambulance do³¹czony do Hafenstraße i zmodyfikowany.

Keypress

Alias: Turku, DJIDDA, Twins
Wielkoœæ: 1232 (EXE) lub 1472 (COM)
Pochodzenie: prawdopodobnie z Finlandii
Typ: rezydentny, atakuje pliki EXE i COM

OBJAWY: Atakuje pliki EXE/COM. Dwie ró¿ne d³ugoœci dla plików COM i EXE.

Dzia³anie: Po wywo³aniu zara¿onego programu, wirus przeszkadza w poleceniach, gdzie powtarzaj¹ siê znaki klawiatury. Czasem odzywa siê równie¿ g³oœnik, co mo¿e byæ wynikiem przepe³nienia buforu klawiatury.

Szkody:

WARIANTY: Znane s¹ ró¿ne warianty.

Violetta

Alias: (-)
Wielkoœæ: 3840
Pochodzenie: Niemcy
Typ: rezydentny, atakuje pliki COM

OBJAWY: Wirus zara¿a pliki COM.

Dzia³anie: Ten zaprawdê d³ugi wirus, zaprogramowany jest doœæ prymitywnie. Prawdopodobnie, jest to nieudoskonalona wersja próbna. W kodzie posiada tekst: Violetta.

Szkody:

WARIANTY:

Devils Dance

Alias: Joker, Moonlight
Wielkoœæ: 940-960
Pochodzenie: Europa Po³udniowa
Typ: rezydentny, atakuje pliki COM, bardzo niebezpieczny, uszkadza FAT

OBJAWY: Wirus infekuje pliki COM. Komunikat w trakcie gor¹cego startu. Pliki s¹ atakowane wielokrotnie - skutek: *Plik za du¿y dla pamiêci operacyjnej*, zapisuje czêœciowo FAT (przez co niszczy pliki na twardym dysku).

Dzia³anie: Wirus bardzo z³o¿ony. Atakuje wszystkie pliki w katalogu, z którego uruchamiamy zara¿ony plik. Wirus musi byæ zwalczany w stadium pocz¹tkowym.

Szkody: Wirus liczy polecenia zadane z klawiatury.
Przy ok. 2000-3000 poleceniach zmienia kolory na ekranie.
Od ok. 3000 i po gor¹cym starcie (CTRL+ALT+DEL) ostrzega komunikatem:
Did you ever dance with the devil in the weak moonlight?
Pray for your Diks!
The Joker
Po oko³o 5000 poleceñ, zapisuje twardy dysk niszcz¹c FAT, co prowadzi do ca³kowitej utraty danych.

WARIANTY:

Chemnitz

Alias: (-)
Wielkoœæ: 765-848
Pochodzenie: Niemcy
Typ: rezydentny, atakuje pliki COM i EXE

OBJAWY: Wirus zara¿a pliki COM i EXE.

Dzia³anie: Nie stwierdzono szczególnego dzia³ania.

WARIANTY:

Taiwan

Alias: (-)
Wielkoœæ: 677, 708, 743, 752
Pochodzenie: Tajwan 1990 rok
Typ: nie rezydentny, atakuje pliki COM,
bardzo niebezpieczny

OBJAWY: Wirus zara¿a pliki COM. Zainfekowane pliki maj¹ przypisane 62 sekundy.

Dzia³anie: Po wywo³aniu zara¿onego pliku, wirus dostaje siê do pamiêci i zara¿a dalsze pliki. Mo¿e dojœæ do bardzo d³ugich poszukiwañ.

Szkody: Ósmego ka¿dego miesi¹ca zapisuje FAT i g³ówne katalogi C: i D:. Ca³kowita utrata danych.

WARIANTY: Znane s¹ 4 warianty wirusa

Boojum

Alias: (-)
Wielkoœæ: 334-350
Pochodzenie: Maj 1992
Typ: rezydentny, atakuje pliki EXE

OBJAWY: Wirus zara¿a pliki EXE.

Dzia³anie: Nie wydaje siê mieæ ¿adnych szkodliwych w³aœciwoœci.

Szkody:

WARIANTY:

Hungarian

Alias: (-)
Wielkoœæ: 482
Pochodzenie: Wêgry
Typ: rezydentny, atakuje pliki COM

OBJAWY: Wirus zara¿a pliki COM.

Dzia³anie: Wirus, nie zosta³ jeszcze dok³adnie zanalizowany.

Szkody: W miesi¹cu czerwcu i listopadzie formatuje twardy dysk.

WARIANTY:

Horror

Alias: (-)
Wielkoœæ: 1112, 1137, 1182
Pochodzenie: czerwiec 1992 roku
Typ: nie rezydentny, atakuje pliki COM i EXE

OBJAWY: Wirus zara¿a pliki COM i EXE.

Dzia³anie: Brak doniesieñ o szkodliwym dzia³aniu.

Szkody:

WARIANTY:

AntiCMOS

Alias: Lenart
Wielkoœæ: (-)
Pochodzenie: Hong Kong 1994 rok
Typ: rezydentny, atakuje sektory startowe dyskietek Bootsektor, tablicê partycji twardego dysku

OBJAWY: Wirus infekuje Bootsektor dyskietek i tabelê partycji twardego dysku. Zmienia ustawienia CMOS.

Dzia³anie: Wirus usuwa ustawienia CMOS, aby wystartowaæ z dyskietki nale¿y przywróciæ dawne ustawienia.

Szkody:

WARIANTY:

Timemark

Alias: (-)
Wielkoœæ: 1062-1076
Pochodzenie: Polska, sierpieñ 1992 rok
Typ: rezydentny, atakuje pliki EXE

OBJAWY: Wirus zara¿a pliki EXE. Nie zmienia daty plików.

Dzia³anie: Nie dzia³a szkodliwie.

Szkody: nie znane

WARIANTY: **Timemark 1**, 1062-1076 Bajtów - d³ugoœæ.

Timemark A: 1083-1097 Bajtów - d³ugoœæ, zmienia datê plików i infekuje pliki podwójnie.

17. November

Alias: (-)
Wielkoœæ: 768, 855, 880
Pochodzenie: W³ochy 1991 rok
Typ: rezydentny, atakuje pliki COM i EXE

OBJAWY: Wirus zara¿a pliki COM i EXE. Zapisuje twardy dysk ka¿dego 17 listopada.

Dzia³anie: Do dnia dzisiejszego znana jest rodzina 4 wirusów.
W zale¿noœci od rodzaju maj¹ ró¿ne dzia³anie.

Szkody: 768 zapisuje dysk 17.paŸdziernika
880 zapisuje dysk miêdzy 17.11. a 31.12.

Storm

Alias: Tatou
Wielkoœæ: 1153-1163
Pochodzenie: lato 1993 rok
Typ: rezydentny, atakuje pliki COM

OBJAWY: Wirus zara¿a pliki COM. Do zainfekowanych plików dopisuje 62 sekundy.

Dzia³anie: Nie stwierdzono szkodliwego dzia³ania.

Szkody:

WARIANTY:

generic (123PBF) virus

T³umaczenie: ogólny

Informacja: W³aœciwie to nie jest wirus. Niektóre programy antywirusowe, melduj¹ grupy wirusów i podejrzenie o zara¿eniu, dzia³a tylko w ten sposób, przy czym:
generic 1 lub P oznacza tabelê partycji PT-Virus
generic 2 lub B wirus bootsektorowy
generic 3 lub F zwyk³y file virus

Taki komunikat innego programu, powinno siê traktowaæ powa¿nie. Mo¿e to oznaczaæ wykrycie wirusa.
Prosimy powiadomiæ nas przez HOTLINE.

possible virus found

informacja: To na pewno nie jest wirus! (possible ang. -> mo¿liwe). Przewa¿nie chodzi o zapis na zabezpieczonym w CMOS bootsektorze twardego dysku.

NewBug

Alias: Antiexe, EXEbug
Wielkoœæ: 1026
Pochodzenie: (-)
Typ: rezydentny, atakuje sektory startowe dyskietek Bootsektor, tabelê partycji twardego dysku

OBJAWY: Wirus zara¿a Bootsektor dyskietek i tabele partycji u¿ywanych dysków.

Dzia³anie: Interesuj¹cy jest fakt, ¿e wirus zmienia MZ-Flag w plikach EXE. Komputer widzi je jako plik COM i czêsto nie potrafi uruchomiæ. Przy ponownej próbie uruchomienia przywraca MZ-Flag i uruchamia plik.

Szkody:

WARIANTY: