



Spis treści AntiVirenKit 6



- ▣ Część ogólna
- ▣ Przygotowanie
- ▣ Praca z AVK 6 dla Windows 3.X
- ▣ Tajniki i sztuczki
- ▣ Informacje o wirusach



Część ogólna

- ▣ Wstęp
- ▣ Serwis G DATA
- ▣ G DATA-Hotline
- ▣ Numer rejestracyjny
- ▣ Numer wersji
- ▣ Zapasowa dyskietka
- ▣ Porady - serwis wirusowy
- ▣ Aktualizacja programu
- ▣ Serwis dyskietek AVK
- ▣ Z³amanie warunków serwisu
- ▣ Przesy³anie dyskietek
- ▣ Plik tekstowy (AVK.TXT)



Przygotowanie

▣ Analiza wirusów



Praca z AVK 6 dla Windows 3.X

- ▣ Wymogi sprzętu i oprogramowania
- ▣ Okno g³ówne
- ▣ Przygotowanie analizy
- ▣ Przebieg analizy
- ▣ Wynik analizy
- ▣ Zadania pliku referencyjnego
- ▣ Wyœwietl listê wirusów



Tajniki i sztuczki

- ▣ Sporządzenie dyskietki startowej
- ▣ Ogólne oerodki ochrony
- ▣ Użycie AVK



Informacje o wirusach

▣ [Katalog wirusów](#)

Wstêp

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

Dla ka¿dego œatwy w obs³udze i jednocześnie odpowiadaj¹cy najwy¿szym wymogom bezpieczeñstwa - to odwieczne cele pracy G DATA Software, nad ulepszeniem AVK.

Poni¿sza wersja œ¹czy je, na dotychczas nie osi¹gniêtym poziomie. Aby Państwo 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 Państwo, jedn¹ z najlepszych mo¿liwoœci programowej ochrony antywirusowej. W po³¹czeniu z Serwisem Profesjonalnym, maj¹ Państwo 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 najważniejsze:

Prosimy o przesłanie nam karty serwisowej!

Znajdź Państwo w opakowaniu oprogramowania. Otrzymaj Państwo od nas kolorową dyskietkę serwisową z upoważnieniem do udzielania kolejnych aktualizacji programu. Tylko w ten sposób mogą Państwo korzystać z następujących udogodnień:

SERWIS PRYWATNY

SERWIS PROFESJONALNY


Bezpłatny Hotline

Serwis wirusów

Informacje dla Państwa o zmianach i nowościach.

Karta serwisowa zawiera z prawej strony pole, w którym deklarujemy chęć uzyskania SERWISU PROFESJONALNEGO. Jeżeli nie przekonuj Państwa zalety SERWISU PROFESJONALNEGO, prosimy przesłać nam kartę bez deklaracji.

SERWIS PROFESJONALNY, można wykupić w dowolnym, późniejszym terminie.

 **UWAGA:** Już kilkumiesięczna wersja nie gwarantuje pełnej ochrony przed wirusami! Każdy użytkownik otrzyma od nas bezpłatnie po wysłaniu, kolorową dyskietkę serwisową z najnowszą wersją AVK. W ten sposób czas skądowania programu u dystrybutora czy sprzedawcy nie działa na Państwa niekorzyść.

Jakość naszych usług zależy w dużej mierze od tego, czy Państwo będą przestrzegać określonych warunków. W ten sposób możemy gwarantować swobodny rozwój naszych usług 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 znaleŹæ w tekstach pomocy i podrêcznikach. Prosimy spróbowaæ najpierw tej drogi rozwi¹zania problemu.

No.: XY **Numer wersji AVK**

Numer wersji pomaga ustalić aktualność Państwa programu, a w razie problemu odpowiednio zareagować. Numer wersji znaleźć można pod opcją¹ Info... lub na etykiecie (Label) kolorowej dyskietki serwisowej.

No.: XY **Numer rejestracyjny**

W opakowaniu AVK znajduje się karta rejestracji. Prosimy wypełnić i odesłać do nas. Tylko tak możemy Państwa zarejestrować i pomóc w przypadku wyjaśnienia wątpliwości. Serwis pyta o numer rejestracji sprawdzając tożsamość. Numer można znaleźć na pierwszej stronie podręcznika. Prosimy podać numer rejestracyjny także przy zamawianiu SERWISU PROFESJONALNEGO.



Zapasowa dyskietka

W każdej chwili mogli Państwo odesłać nam uszkodzone lub niesfunkcjonujące dyskietki G DATA. Prosimy zamieścić zaadresowaną, ofrankowaną kopertę zwrotną. Otrzymają Państwo zapasową dyskietkę.



Porady wirusowe


W przypadku zauważenia nowego wirusa lub dziwnego zachowania komputera, prosimy o przesłanie nam dyskietki z kopią podejrzanego programu. Przeanalizujemy dyskietkę i dostarczymy Państwu jak najszybciej pomysły na rozwiązanie problemu. Prosimy przesyłać dyskietki w sytuacjach proponowanych przez AVK. Oczywiście gwarantujemy pełną dyskrecję co do przesłanych nam Państwa danych.



Aktualizacja programu

... podstawowa czynnoœæ przy obs³udze ka¿dego programu antywirusowego.. ³aden 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.

 **WA³NE:** 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 się w pakiecie AVK!

Otrzymuj¹ j¹ Państwo po wys³aniu karty serwisowej AVK (znajduje się 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 Państwo podrêcznika ani opakowania).

SERWIS PROFESJONALNY

W ramach serwisu profesjonalnego otrzymuj¹ Państwo 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 ŒNE: 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

Pominięcie aktualizacji, może spowodować poważne szkody. Aby temu zaradzić oferujemy Państwu pakiet **Serwis Profesjonalny**), umożliwiającym automatyczne przesłanie nowo powstałej wersji programu. Pakiet Serwis Profesjonalny, można uzyskać przy pomocy karty serwisowej. Serwis Profesjonalny wymaga odnowienia po upływie roku. Poinformujemy Państwa o upływie terminu ważności pakietu.

Umowa obowiązuje tylko rok:. Decyduje Państwo sami czy ją przedłużyć. Pakiet Serwisu Profesjonalnego można zamówić listownie lub telefonicznie (Faksem) niezależnie od daty zakupu. Polecamy go nie tylko profesjonalistom i Firmom ale także wszystkim użytkownikom AVK. Serwis jest szczególnie przydatny, kiedy używamy komputera do pracy zawodowej, gdzie ochrona plików z danymi ma duże znaczenie. Koszty zakupu pakietu, nie przewyższają kosztów przesłania dyskietek i wkładu 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 Państwo,

Chciałbym za cenę 122,- Z³

zamówić

przedsięwzięcie (zakreślamy wybraną pozycję).

na okres jednego roku SERWIS PROFESJONALNY AVK

Otrzymam przy jego pomocy każdą nowopowstającą aktualizację AVK. Po upływie roku umowa wygasa i zdecyduję czy chcę ją przedsięwziąć.

Proszę przesłać aktualizację i rachunek pod adres:

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

Nazwisko : _____

Ulica: _____

kod, miejscowość: _____, _____

Mój numer rejestracji: _____

W razie pytań jestem uchwytany pod numerem tel.: _____ / _____.

Data, podpis: _____



Pismo VIREN-NEWS

VIREN-NEWS to czasopismo fachowe wydawane przez G DATA w Bochum. VIREN-NEWS można otrzymać w ramach serwisu profesjonalnego. Każdy użytkownik serwisu, otrzyma wraz z aktualizacją¹ najnowsze wydanie czasopisma.

W piśmie VIREN-NEWS poruszona jest tematyka ochrony danych przed wirusami. Informuje ono o wydarzeniach i trendach na scenie wirusowej, a także zawiera wskazówki G DATA w temacie wirusów itp.

X Zmianie warunków serwisu

Możemy skutecznie nasze usługi tak długo, jak tylko Państwo trzymają się "regu gry". Zmianie warunków umowy wliczamy w Państwa koszty. Zaległe aktualizacje prześlemy dopiero po uregulowaniu rachunków.

Prosimy o zrozumienie środków ostrożności, podjętych z wymienionych powodów. Ma to na celu utrzymanie porządku w strukturze serwisu.

Przesyłanie dyskietek

Przesyłając nam dyskietki z podejrzeniem infekcji lub nieznanymi zmianami, prosimy pamiętać:

- o napisaniu na dyskietce nazwiska i adresu
- o nieprzesyłaniu oryginalnych dyskietek AVK
- o załączeniu numeru wersji AVK,

Prosimy przestrzegać także następujących wskazówek:

- Wysyłanie listów poleconych itp., z reguły nie ma sensu i jest nie wskazane.
- Dyskietki z opisami muszą być wysłane jako listy.
- Do przesyłek można używać zamiast normalnych kopert torebek powietrznych, które możemy odesłać z powrotem. W tym przypadku nie muszą Państwo wysłać koperty zwrotnej.



Plik tekstowy (AVK.TXT)

Z powodu dokonywania zmian i poprawek, nie jest możliwe wydrukowanie podręcznika zawierającego dokładny opis. W celu umieszczenia wznowień i nowych informacji nie zawartych w podręczniku utworzyliśmy plik AVK.TXT, informujący o aktualnym stanie produktu. Prosimy przejrzeć ten plik przed uruchomieniem AVK 6!

Pliki AVK.TXT można wyświetlić następującymi poleceniami DOS:

na ekranie:

```
TYPE A: AVK.TXT
```

lub wydrukować:

```
TYPE A: AVK.TXT >PRN
```

W wersji Windows można to robić w³asnymi edytorami.



UWAGA: Staraliśmy się uniknąć sprzeczności tekstów podręcznika i pliku, w przypadku ich wystąpienia prosimy pamiętać: teksty w pliku mają pierwszeństwo przed podręcznikiem pomocy!



Analiza podstawowa

Przed instalacją...

W żadnym przypadku nie można instalować AVK 6 (ani innego programu) kiedy analiza wstępna wykazała obecność wirusa na dysku lub w pamięci. Przekonajmy się, czy nie zamelduje ona o wykryciu wirusów, a w przypadku ich wykrycia, czy usunie je dokładnie. Sposób przeprowadzenia analizy:

ANALIZA PODSTAWOWA (skrót)

1. Wyłączmy komputer na ok. pięć sekund.
2. Wystartujemy z zabezpieczonej dyskietki.
3. Przeprowadzimy analizę twardego dysku.

Polecenie DOS: **AVK [napęd]:** (przeważnie: **AVK C:**)

Po zakończeniu analizy możemy zainstalować AVK 6.



Sporządzenie dyskietki startowej

Bardzo często pytają Państwo, co robić w przypadku zarażenia bootsektora. Także dyskietki są wtedy zarażone. Aby zanalizować komputer konieczna jest wolna od wirusów dyskietka startowa.

Jest ona także niezbędna przy instalacji nowej aktualizacji programu. Tylko przy starcie z takiej dyskietki można mieć pewność, że w pamięci nie ma wirusów. Dopóki w pamięci rezyduje wirus, analiza i usunięcie go nie jest możliwe. Wirusy typu Stealth, mogą doprowadzić do niezauważenia wirusa w systemie. Z tej przyczyny radzimy sporządzić dyskietkę startową, zanim dojdzie do infekcji.


Sposób jej sporządzenia znajdzie Państwo w podręczniku obsługi Windows.



Użycie AVK 6

Do czego s³uży AVK?

Zapoznali siê Państwo z problematyk¹ wirusów komputerowych i postanowili chronić 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 Państwo do zakupionej wersji pakiet serwisowy, który m.in. umo¿liwia nowelizacjê programu. Tylko w ten sposób mo¿emy gwarantowaæ Państwu pewn¹ i dobr¹ ochronê.

Jak czêsto uaktualniaæ program?

G DATA wydaje 6-10 nowelizacji rocznie. OdpowiedŹ 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 Państwo 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 Państwa 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 Państwo pod¹¿aæ œladem 64% u¿ytkowników i sprawdzaæ dane przynajmniej raz w tygodniu i przy ka¿dej operacji instalacyjnej.



Ogólne oerodki ochrony

Chcielibyœmy, Ÿeby Państwo poprzez uŸycie AVK 6.0, przyzwyczaili siê do niektórych waŸnych czynnoœci zapobiegawczych. Prosimy, trzymaœ siê w miarê moŸliwoœci wszystkich zaleceñ, dziêki czemu zmniejszy siê ryzyko infekcji wirusowej.


Oryginalne oprogramowanie

- UŸywajcie Państwo tylko oryginalnego oprogramowania.
- NaleŸy pamiêtaæ o zabezpieczeniu oryginalnych dyskietek przed zapisem (otwory po obu stronach u góry).
- Prosimy sporz¹dziæ kopiê oryginalnego oprogramowania do uŸytku codziennego.
- Przechowywaæ orygina³ oprogramowania w pewnym miejscu.

Prosimy sporz¹dziæ zapasow¹, nie zakaŸon¹ wirusem dyskietkê systemow¹.

Kontrola stacji dysków

- Przed kaŸdym uruchomieniem komputera naleŸy sprawdziæ, czy w stacji dysków, nie ma dyskietki (zagroŸenie zainfekowania BOOT sektora!), takŸe przy dyskietkach bez systemu.

 **Wskazówka:** Wielu problemów moŸna unikn¹æ poprzez ustawienie sekwencji bootowania (startowania systemu) C:,A:. MoŸna tego dokonaæ w menu CMOS-Setup (klawisz DEL w czasie bootowania).

UWAGA: Przy analizie podstawowej naleŸy przywróciæ sekwencjê A:, C:.

Backup

- NaleŸy regularnie sporz¹dzaæ wersjê Backup Państwa danych (kopie zapasowe)

W Firmach

- Prosimy unikaæ wprowadzania prywatnych programów i gier.
- KaŸd¹ obc¹ dyskietkê naleŸy sprawdziæ.
- Analiza referencyjna powinna byæ przeprowadzana regularnie.
- Reagujmy na kaŸde nietypowe zachowanie komputera lub oprogramowania.

W wypadku infekcji wirusem

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

ZauwaŸyli Państwo coœ nietypowego?

Na pytanie, czy to jest objaw zakaŸenia wirusem, naleŸy odpowiedzieæ "**TAK**" i przeprowadziæ analizê AVK 6.0 !

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

nieoczekiwane zmiany napędów)?

- Czy dane z powodu rozmiarów nie mieszczą się na dysku?
- Czy zmienia się obraz (kolor, ramki, rzadkie znaki i komunikaty)?
- Litery spadają z ekranu, zmiana znaków na klawiaturze?
- Głośnik wydaje dziwne dźwięki, piski, melodie?
- Pamięć dysku twardego zabezpiecza się w niewytłumaczalny sposób?
- Czy po poleceniu CHKDSK C: uzyskujemy komunikat o uszkodzeniu dysku (spróbujemy uruchomić komputer z innej dyskietki i ponownie użyć CHKDSK C:)?

Wymogi sprzętu i oprogramowania

AVK pracuje w trzech wersjach systemowych: DOS, Windows 3.x i Windows'95. W każdym przypadku wymagane jest przynajmniej 640 KB pamięci operacyjnej. Przy użyciu graficznej wersji DOS, w pamięci nie mogą rezydować żadne inne programy. Narzędzia rezydencyjne można umieścić w pamięci 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 więcej.



Okno g³ówne

Okno g³ówne dla wersji Windows 3.X AVK 6, sk³ada siê z nastêpuj¹cych element³ów:

- ▣ Sterowanie programem
- ▣ Wyb³r pliku
- ▣ Wiersz statusu z numerem wersji
- ▣ Pasek funkcji
- ▣ Menu g³ówne

Wybór katalogu

Opcja wybór katalogu, pokazuje aktualnie wybrany do analizy katalog. Poniżej znajduje się okienko analizy podkatalogów, standardowo ustawione na przeszukiwanie "z podkatalogami".

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



Wybór pliku

Opcja wyboru pliku umożliwia decyzję, czy przeszukujemy wszystkie, czy tylko wybrane pliki. Standardowo ustawiono opcję Pliki wybrane. Wchodzimy poprzez wybór przycisku "Wybór".

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

Lepiej jest przeszukać tylko określone pliki. W tym celu wybieramy opcję Pliki wybrane... i klikamy w przycisk Wybór. Udajemy się do menu rozszerzeń.

W oknie wyboru przedstawione są przykłady rozszerzeń plików polecanych przez nas do analizy. Standardowo ustawiono następujące rozszerzenia:

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

Mogą Państwo dowolnie zmieniać ustawienia wpisując w górne okienko swoją propozycję i potwierdzając ją poleceniem Dodaj (lub przez Alt+D). Można też usuwać z listy wybrane propozycje zaznaczając je myszą i używając polecenia Usuń (lub Alt+U). Przez naciśnięcie polecenia Standard (lub Alt+S) powracamy do pierwotnego ustalenia



Wiersz Statusu


Pasek pokazuje z prawej strony numer wersji AVK, z któr¹ Państwo pracujecie. Informacja ta przydaje się przy korzystaniu z hotline i serwisu AVK. Z drugiej strony pokazana jest ościeżka dostępu analizowanego obecnie pliku analizuj² Napêd:\Katalog\Plik.

Nakierowuj³c kursor myszy na symbole paska funkcji lub funkcj⁴e menu g⁵ównego, otrzymujemy w pasku statusu oznaczenie symbolu i wyjaœnienie funkcji.

Pasek funkcji



Pasek funkcji zawiera najważniejsze funkcje codziennej obsługi AVK:


 Wydrukuj plik

 Rozpocznij analizę

 Wstrzymaj analizę

▪ Informacje o pliku

▪ Usuń wirusa

 Usuń zarażony plik

 Kopiuj zarażony plik (do analizy w G DATA)

▪ Tekst pomocy (W³aœnie tam jesteœmy)

 Lista wirusów

Funkcje niemożliwe 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 - Uka¼ informacje

Pokazuje informacje na temat jednego pliku

Analizuj - Usuñ wirusa

Usuwa wirusa z zara¼onego pliku

Analizuj - Usuñ plik

Usuwa zara¼ony plik

Analizuj - Kopiuj plik

Kopiuje zara¼ony 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 obsługujemy za pomocą klawiatury lub myszki. Kod klawiatury odpowiada kodowi systemu DOS, do którego jesteście Państwo przyzwyczajeni. Poszczególne opcje w menu głównym można uruchomić za pomocą kombinacji Alt+litera podkreślona w nazwie danej opcji. Oprócz tego wiele poleceń przypisano klawiszom funkcyjnym. Opis znajduje się w oknach menu. Po piktogramach (ikonach) menu poruszamy się pionowo za pomocą kursorów, w poziomie poprzez TAB oraz Shift+TAB. Polecenia, uruchamia przycisk Enter.

Wybrane elementy podkreślone są różnym kolorem, pozostałe białym czcionką. Informacje o obsłudze DOS za pomocą myszki znajdą Państwo w podręczniku obsługi DOS i w tekstach DOS.

Przygotowanie analizy

Program jest tak pomyślany, aby jak najszybciej przygotować analizę. Rozpocznijmy od uruchomienia AVK. Po automatycznym ładowaniu pamięci wybieramy różne ustawienia.

- a) Wybieramy katalog do analizy.
- b) Wybieramy typy plików do analizy.
- c) Ustawiamy odpowiednie opcje analizy. W tym celu w menu głównym pod hasłem Analizuj punkt Opcje.

Wybieramy odpowiednią reakcję na wykrycie wirusa: Tylko protokół³, Zatrzymaj analizę, Usuń wirusa, Usuń plik lub Przesuń plik.

 **WSKAZÓWKA:** Polecamy opcję Tylko protokół³. Możemy potem w spokoju zdecydować co zrobimy ze znalezionymi zmianami (ewentualnymi mutacjami).

Przy opcji Zatrzymaj analizę poszukiwanie zostanie wstrzymane. Mogą Państwo podjąć bezpośrednio działanie.

Ustawienie Usuń wirusa nie zawsze osiąga skutek. Niektóre wirusy nie mogą być oddzielone od zaatakowanego pliku. Bywa tak w przypadku kiedy wirus niszczy poważnie strukturę pliku, lub zaszła nietypowa mutacja.

Opcja Usuń plik nie zawsze jest najlepszym rozwiązaniem, gdyż AVK potrafi ocalić zainfekowany plik.

Przesuń plik, ta opcja kopiuje plik wraz z wirusem do wskazanego katalogu. Po usunięciu wirusa plik należy przekopiować ponownie do poprzedniego katalogu.


 **UWAGA:** Prosimy zabezpieczyć katalog z wirusami przed osobami nieupoważnionymi!


Teraz ustalmy reakcję na zmianę referencji: Tylko protokół³, Zatrzymaj analizę, Z akceptacją lub Przesuń plik.


 **WSKAZÓWKA:** Polecamy także opcję Tylko protokół³.

Pozostałe opcje - patrz wyżej.

Decydujemy tu, czy AVK ma przeprowadzić dodatkowo test referencyjny plików. Sprawdzając referencje, program rejestruje sumy kontrolne poszczególnych plików i porównuje je z wynikami kolejnych analiz. W ten sposób AVK rozpoznaje zmiany systemowe, będące często sygnałem wystąpienia nieznanego wirusa.

 **WAŻNE:** Prosimy przeprowadzać często analizę referencyjną! Dzięki niej program potrafi wykrywać nieznanne wirusy, co zwiększa pewność ochrony.

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

 **UWAGA:** Nie jest wskazane polecenie Z akceptacj¹. Stwarza zagrożenie pominięcia nieznanego wirusa. Musimy zawsze poznać przyczynę zmiany!

Na specjalne życzenie, AVK sporządza protoko³ możliwy do wydrukowania lub wgl¹du przez edytor. Wystarcza tu opcja Protoko³ ogólny". Ze względu na oszczędność miejsca, radzimy usuwać uprzednio sporządzone protoko³y (chyba że chc¹ Państwo dokonać porównania dokumentów).

Możemy przystąpić do analizy.

Test pamięci

Po wywołaniu AVK program testuje najpierw pamięć. Przy przeprowadzaniu instalacji każdej aktualizacji AVK, radzimy przeprowadzić dodatkowo analizę podstawową¹.


Przeprowadzenie analizy

Po przygotowaniu analizy przejdźmy do działania. Rozpoczynamy poleceniem paska funkcji:



lub w menu uruchamiamy pod hasłem Analizuj opcję "Uruchom analizę".

Rozpoczęcie przebiegu analizy można rozpoznać, po rotacji (ruchu obrotowym) symbolu wirusa w oknie głównym.

Poza tym, pasek statusu pokazuje odciek dostępu analizowanego pliku. Analizę możemy w każdej chwili przerwać 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 ilości sprawdzonych katalogów i plików, ilości znalezionych wirusów i zmian referencyjnych oraz o liczbie usuniętych wirusów i przesuniętych plikach. W dolnej części pojawi się wynik analizy BOOT-sektora.

Wydruk wyniku

Wydrukować raport wyników analizy, można przez użycie funkcji "Drukuj protokół" w menu "Plik", w menu głównym, lub też poleceniem z paska funkcji: 

Po przejrzaniu raportu możemy rozpocząć usuwanie wirusów z plików jeżeli wybraliśmy opcję "Tylko protokół" lub "Przesuń plik".

Zadania pliku referencyjnego

W przypadku wybrania opcji Tylko protokół³", możemy przystąpić do usuwania znalezionych wirusów (lub zmian referencyjnych).

Jeżeli wybraliśmy opcję Zatrzymać analizę udajemy się do menu:

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

Informacje o określonym pliku

Szczegółowe informacje dotyczące pliku otrzymujemy:


- Przez zaznaczenie znalezionej zmiany i wybranie funkcji "Ukaż informacje" pod hasłem "Analizuj" w menu głównym.
- Podwójne kliknięcie myszy w nazwie zmiany (wirusa)
- Za pomocą opcji "Informacje o pliku":

Na górze znajduje się nazwa pliku, katalogu i rodzaj zmiany referencyjnej. Jeżeli jest to wirus, program informuje o jego stanie. Zazwyczaj można go usunąć z zarażonego pliku. W przypadku mutacji wirusa (wirusy polifformiczne, które potrafią zmieniać swój kod), który AVK rozpoznaje, ale nie jest w stanie usunąć nie niszczyć pliku, prosimy o przesłanie nam kopii tego pliku. W ten sposób możemy dokonać dokładnej analizy i zapobiec dalszemu rozprzestrzenianiu się wirusa.

W oknie atrybutów mamy rozmiar, datę utworzenia, sumę kontrolną i nazwę znalezionej zmiany.


Okno zmian, informuje o rodzaju zaistniałej zmiany, na przykład o zarażeniu wirusem i możliwościach usunięcia go lub o zmianie referencyjnej. Poniżej znajdują się ikony pliku referencyjnego.

Wszystkie nieosiągalne opcje, zaznaczone są jasnoszarymi czcionkami (opcje w tym momencie są nie aktywne).

 **WSKAZÓWKA:** Skutki tych poleceń, patrz od lewej do prawej, są coraz bardziej niebezpieczne, dlatego proponujemy używanie ich zawsze w standardowej kolejności (np. w przypadku powyższym sensowniej jest usunąć wirusa niż cały plik).

Usunięcie wirusów z wybranych plików


... jest możliwe, jeżeli nic nie stoi na przeszkodzie ingerencji programu we wskazany plik. Program usuwa wirus znany, u którego analiza nie wykazała możliwości poważniejszych komplikacji. Dzieło na szczęście jest tak w większości przypadków. Program bardzo skutecznie rozpoznaje, czy wirus nadaje się do usunięcia. Możemy to sprawdzić poprzez zaznaczenie zarażonego pliku mysz¹ i:

- Wybranie funkcji Usun wirusa w menu głównym Analizuj lub
- Naciśnięcie w pasku funkcji:  lub
- Podwójne kliknięcie mysz¹ w nazwę pliku i wybranie opcji Usun wirusa" w oknie informacji o pliku.

W przypadku wirusa nieznanego lub takiego, który nieodwracalnie uszkodzi³ pliki oryginalne, zaleca się wysłanie kopii zainfekowanych plików do G DATA, w celu głębszej analizy. Zadanie to ułatwi nam wbudowana funkcja.

Kopiowanie wybranych plików (do analizy w G DATA)

W przypadku wirusa nieznanego lub takiego, który nieodwracalnie uszkodzi³ pliki oryginalne, zaleca się wys³anie kopii zainfekowanych plików do G DATA, w celu g³ębszej analizy. Zadanie to u³atwi nam wbudowana funkcja. Wystarczy w³o³yæ dyskietskê 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 usunięty (pojawia się wcześniej okno potwierdzenia polecenia), a dane należy ponownie zainstalować. Przeważnie nie jest to konieczne i tylko w odosobnionych przypadkach wymagana jest interwencja firmy (produkcja ośrodka zaradczego). Adres firmy jak wyżej.


 **UWAGA:** W przypadku nieznanego lub zmutowanego wirusa ważne jest wysłanie kopii zarażonego programu do analizy w G DATA. Do kopiowania plików służy wbudowana funkcja.


Zainfekowany plik usuwamy zaznaczając myszą jego nazwę, po czym

- w menu głównym pod hasłem Analizuj wybierając funkcję "Usuń plik" lub
- w pasku funkcji naciskamy na:  lub
- klikamy myszą w nazwę pliku i wybieramy opcję "Usuń plik" w oknie informacji o pliku.

Wyświetlenie listy wirusów

Znajduj¹ się tu informacje o najważniejszych wirusach, powoduj¹cych ponad 85% infekcji, dotycz¹ce dróg zarażenia, rozmiarów, rodzaju i wiele innych.

 **UWAGA:** Lista wirusów, które umieściliśmy, to tylko spis ważniejszych wirusów wybranych przez nas jako przyk³ady. AVK rozpoznaje ich oczywiście o wiele więcej! Obecnie ponad 8 500.

Zaznaczaj¹c zainfekowany plik, możemy dowiedzieć się 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



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
DJDDA
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
Vaccina
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
Wielkość: 5120
TYP: nierezydentny
atakuje pliki COM/EXE
zaraża COMMAND.COM

OBJAWY: Zarażone pliki COM rozrastają się o 5120 B; Zarażone pliki EXE rozrastają się o 5120 - 5135 B; występują pozornie nieuzasadnione dostępy do twardego dysku; przy próbach zarażenia wirusem, zabezpieczonych przed zapisem plików, występują od DOS'a komunikaty o błędach.

Działanie: 5120 zaraża dowolne pliki COM i EXE. Uruchomienie zarażonego programu prowadzi do tego, że w aktualnym katalogu na aktualnej stacji dysku, dalsze pliki COM i EXE zostaną zarażone; poza tym wybrany wg. algorytmu liczb losowych następny plik COM/EXE zostanie zarażony w każdym katalogu stacji dysku C:.

W następstwie tego zarażenia, mogą ulec zmianie dane, a pliki systemowe DOS'u mogą ulec uszkodzeniu przez błędne przyporządkowanie sektorów.

Poza tym: ten wirus powstał w skomplikowanym BASICu i dlatego, na końcu każdego zarażonego programu znajdują się takie słowa jak: 'BASRUN', 'BRUN', 'IBMBIO.COM', 'IBMDOS.COM', 'COMMAND.COM' lub 'Access denied'. Jednakże istnieje odmiana tego wirusa bez wyżej wymienionych słów.

Anti-Tel

ALIAS: [Telecom Boot, Spanish Telecom](#)
Wielkość: [-]
TYP: [rezyduje w pamięci](#)
[zaraża sektor startowy na dyskietkach \(Bootsektor\)](#)
[zaraża tabelę partycji twardego dysku](#)

OBJAWY: Całkowita i dostępna pamięć operacyjna zostanie zredukowana; System-Performance zmniejsza się; fałszowanie danych na twardego dysku.

Działanie: Gdy system startuje z dyskietki, która zarażona jest wirusem ANTI-TEL, to wirus instaluje się rezydentnie w górnym końcu pamięci operacyjnej, ale zawsze poniżej granicy 640KB; program DOS (CHKDSK.COM) pokazuje o 1KB pamięci mniej niż się oczekuje. Wirus ANTI-Tel zaraża bezpośrednio z pamięci wszystkie twarde dyski i dyskietki, w których pliki były używane.

Na dyskietkach HD, oryginalny Boot-sektor, przesunięty zostanie do 28 sektora; wirus kopiuje pierwszą część swojego kodu programowego do sektora 0, a resztę do sektora 27. Ponieważ sektory 27 i 28 należą do głównego katalogu, wszystkie pliki, które posiadają odnośniki do tych sektorów zostaną zniszczone.

Na dyskietkach 360KB, oryginalny Boot-sektor, przesunięty zostanie do 12 sektora; wirus kopiuje pierwszą część swojego kodu programowego do sektora 0 i resztę do sektora 10. Ponieważ sektory 10 i 11 należą do głównego katalogu, wszystkie pliki, które posiadają odnośniki do tych sektorów zostaną zniszczone.

Na twardego dysku wirus kopiuje swój kod programowy do tabeli partycji i do sektora 6, na stronie 0, do cylindra 0; tabela partycji zostaje przesunięta do 7-go sektora. Ponieważ DOS normalnie tych sektorów nie używa, dane zmagazynowane w tym miejscu przez specjalne oprogramowanie, też ulegną zniszczeniu.

ANTI-TEL należy do grupy zamaskowanych wirusów, które używają aktywnych środków, aby ich odkrycie przez programy szukające nie dało pozytywnego rezultatu; środki kamuflażu wirusa ANTI-TEL nie są programowane czysto i dlatego kamuflaż nie jest skuteczny dla dyskietek. Skuteczny jest jednak, jeżeli chodzi o twardego dysk.

ANTI-TEL uaktywnia się po 400 ładowaniach systemu i jest nieszkodliwym destrukcyjnym. Ukazuje się wiadomości:

‘**VIRUS ANTITELEFONICA (BARCELONA)**’

i dwa pierwsze dyski twarde zostaną zapisane śmieciami.

WARIANTY: **Telecom Boot:** Ten wirus występuje przy zarażeniach tabeli partycji wirusem TELECOM. Bardzo przypomina on wirus ANTI-TEL, jednakże nie zaraża dyskietek.

Azusa

ALIAS: Hong Kong
Wielkość: [-]
TYP: rezyduje w pamięci
atakuj sektory startowe
atakuj tabelę partycji twardego dysku

OBJAWY: Zmniejszenie całkowitego i béd¹cego do dyspozycji obszaru pamięci o 1KB; po³¹czenia COM 1 i LPT 1 béd¹ 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, niszczy¹c 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 béd¹ w œrodek dyskietki i zapisane tam ewentualnie pliki ulegn¹ zniszczeniu. Przy ka¿dym ³adowaniu systemu bédzie zwiêksza³ siê wewnêtrzny licznik wirusa; gdy licznik osi¹gnie wartoœæ 32, bédzie ponownie ustawiony na zero i wtedy po³¹czenia COM 1 i LPT 1 béd¹ 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
Wielkość: [-]
TYP: rezydujący w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Wydłużony czas startowania systemu, zmniejsza całkowity i dostępny obszar pamięci. Zgłasza komunikaty na ekranie monitora podczas ładowania systemu, zmienia zawartość sektora ładowania i tabeli partycji twardego dysku.

Działanie: BLOODY! atakuje sektory ładowania na dyskietkach i tabele partycji na twardech dyskach. Gdy uruchamiamy system przy pomocy zarządzonej dyskietki, wirus instaluje się w pamięci rezydentnej pod koniec górnego obszaru pamięci zajmowanej przez DOS, jednak zawsze poniżej granicy 640KB i zmniejsza całkowity, dostępny obszar pamięci o 2KB. Proces ładowania systemu trwa znacznie dłużej niż normalnie. Gdy system nie jest ładowany z twardego dysku, natychmiast zostaną zarządzone wirusem tabele partycji. Poza tym, przy każdym ładowaniu systemu zwiększa się wewnętrzny licznik wirusa. Gdy licznik ten osiągnie wartość 128, to podczas ładowania systemu ukazuje się komunikat:

‘Bloody! Jun. 4, 1989’

Ta szczególna data nawiązuje do krwawych zamieszek w Pekinie między chińskimi studentami, a oddziałami wojskowymi.

Ta wiadomość będzie ukazywać się przy każdym, dalszym 6-tym procesie ładowania systemu. Tekst ten, jest zakodowany w wirusie, a więc przy oglądaniu tabeli partycji jest on niewidoczny. Wirus rezydujący w pamięci próbuje zaatakować każdy dysk / dyskietkę, jeżeli dokonuje się dowolnej operacji na znajdującym się tu pliku lub programie; rozkaz **DIR** nie prowadzi jednak do zarządzenia (nie wzbudza wirusa).

Uratowany sektor ładowany zarządzonej dyskietki 360KB, zostanie zapisany w 11 sektorze, który jest częścią obszaru katalogu głównego; gdy obszar ten był używany, to należy do niego pliki przepadają. Inne typy dyskietek, mogą poprzez kopię sektora ładowania, stać się nieużyteczne lub być posiadające zniszczone pliki.

Na twardego dysku sektor ładowania będzie kopiowany (przez wirus) na stronie 0, do cylindra 0, do sektora 6.

Cascade, Cascade-B

ALIAS: [Blackjack, 1704, 1704-B, 1701 Family](#)

Wielkość: [1704](#)

TYP: [rezyduje w pamięci](#)
[atakuję pliki COM](#)
[wirus 31czy się](#)

OBJAWY: Zainfekowane pliki COM powiększają się o 1704B; nieregularne restartowanie systemu.

Działanie: **Cascade, Cascade-B** lub **1701, 1704** należą do najbardziej znanych i rozpowszechnionych wirusów. Wirus **Cascade** znany jest ze specjalnych efektów: spadających liter z ekranu monitora. Jest to pierwszy wirus, który potrafi sam się modyfikować (samokodowanie). **Cascade-B** przypomina wirusa **Cascade**, jednakże tu, olbrzymi algorytm liter został zastąpiony przez proces restartu (gorący start), który jest aktywny, co pewien przypadkowy czas.

WARIANTY: **1704-C:** Działają jak 1704-B, jednakże tylko w miesiącu grudniu każdego roku.

Dark Avenger

ALIAS: Black Avenger, Eddie, Diana, Rabid Avenger,
VAN SOFT, Dark Avenger 1801
Wielkość: 1800
TYP: rezydujący w pamięci
atakujący pliki COM, EXE i OVL

OBJAWY: Pliki COM i EXE zostaną powiększone; niszczy pliki i dysk twardy

Działanie: **DARK AVENGER** instaluje się rezydentnie i jest wyjątkowo "płodny", przy atakowaniu plików programowych, które z jakichkolwiek powodów są otwierane. Przy kopiowaniu poleceniem DOS'a COPY lub XCOPY, oryginalne pliki i powstałe kopie są przez wirus zaatakowane. Zaatakowane pliki powiększają się o 1800B.

DARK AVENGER jest bardzo podstępny. Wirus wprowadza licznik do sektora badawania. Po każdym 16-tym zaatakowaniu jakiegoś programu, zostaje wybrany przypadkowy sektor na dysku twardym, do którego zapisze się część wirusa. Oryginalna zawartość sektora zostaje zniszczona, programy i pliki należące do tego sektora są nie do uratowania.

Wirus zawiera łańcuchy znakowe:

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

Choć ten wirus jest prawie tak duży jak wirus **JERUSALEM**, nie wykazuje jednak żadnych podobieństw.

WARIANTY: **Dark Avenger-B:** Jest bardzo podobny do **Dark Avenger**. Różnica polega na tym, że pliki COM będą powtórnie zaatakowane. Wirus ten, inaczej niż oryginał, rezyduje w wyższym obszarze pamięci. Zawarte łańcuchy znakowe zostały 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 dłuższy niż oryginał, rezyduje również w wyższym obszarze pamięci, jednak nie atakuje powtórnie zarażonego już pliku COM.

Rabid Avenger: Bazuje na **Dark Avenger-B**, zajmuje 3696B w górnym obszarze pamięci DOS, jednak zawsze poniżej granicy 640KB; zaatakowane pliki będą zwiększone o 1806-1823B; poza tym, wariant ten został tak zmieniony, że nie zostaje rozpoznawany przez znawców wirusów jako wariant **Black Avenger**. Łańcuchy znakowe w wirusie:

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

Development Corp!', 'Scan String Killer Test'

Van Soft: Odróżnia 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
Wielkość: 2343 lub 2153
TYP: rezyduje w pamięci
atakuj pliki COM, EXE i OVL
atakuj sektory startowe dyskietek
atakuj tabelę partycji twardego dysku

OBJAWY: Pliki COM i EXE zostaną powiększone; zmniejszą się całkowite i dostępne obszary pamięci; pojawiają się błędy przyporządkowania plików; sektorów i tabel partycji będą zmienione.

Działanie: Startujący plik (zaatakowany) *.EXE przez wirus **FLIP**, wpisuje wirus w górnym obszarze pamięci. Całkowite i będący do dyspozycji obszary pamięci (wg. programu DOS'a CHKDSK.COM) zmniejszą się o 3064B. Poza tym, C:\COMMAND.COM, o ile występuje, będzie zaatakowany; tak drugo jak ten wirus jest aktywny w pamięci, zmiany wielkości są niezauważalne. Poza tym dokonują się zmiany w sektorze i tabel partycji. Na dyskietkach zmiany wielkości danej COMMAND.COM są dostrzegalne.

Każdy wykonywany program wraz z plikiem nakładkowym (Overlay), będzie zaatakowany.

Zwyczaj występują błędy przyporządkowania plików, które mogą zniszczyć pliki dane.

Każdego dnia miesiąca, między godzin 16:00 i 16:59, mogą wystąpić na ekranie monitora strony pozamieniane w poziomie, w systemie, który został wystartowany z zarażonego wirusem twardego dysku i który zarządzany jest przez adapter EGA lub VGA.

Wirus nie atakuje żadnych dalszych plików, jeżeli został wystartowany z pliku COM lub z sektora i tabel partycji; dalsze przenoszenie wirusa jest możliwe tylko poprzez pliki EXE.

WARIANTY: **Flip-B:** jest trochę mniejszy (2153B) niż oryginał; te warianty rozprzestrzeniają się nie tylko przez pliki EXE, lecz także przez tabelę partycji twardego dysku.

FORM-Virus

ALIAS: Form, Form Boot
Wielkość: [-]
TYP: rezydujący w pamięci
atakuje sektory startowe dyskietek

OBJAWY: Odgłosy klikania w głośniku komputera.

Działanie: Jeżeli system po raz pierwszy uruchamiany jest z dyskietki startowej zarażonej wirusem **FORM**, to wirus instaluje się w pamięci i również atakuje sektor startowy na twardym dysku. Proces startowania systemu z zarażonej dyskietki może się nie udać, ponieważ system się zawiesza. W wirusie może się znajdować 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, począwszy od 24-dnia każdego miesiąca, można usłyszeć odgłosy klikania w głośniku komputera.

Tę formę wirusa można w prosty sposób przy pomocy rozkazu
DOS'a SYS.COM usunąć (SYS A: C:).

Hallöchen

ALIAS: [-]
Wielkoœæ: 2011
TYP: rezyduje w pamieci
wirus ³cz¹cy siê
atakujê 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** instalujê siê rezydentnie w pamieci, jak tylko uruchomi siê zainfekowany program, chyba, Ÿe wielkoœæ zaatakowanego programu przekracza 64KB lub program ten utworzony bêdzie z dat¹ miesi¹ca i roku zgodnego z danymi systemu. Wirus powiêksza zaraŸony program do najbliŸszej 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)
Wielkość: 1813 do 1808
TYP: rezyduje w pamięci
atakuj e pliki COM i EXE

OBJAWY: Pliki COM i EXE b e d¹ powi e k s z o n e; efektywność systemu (System performance) zmniejsz y si e; pliki b e d¹ kasowane w ka d y pi t e k 13-tego w miesi cu; pojawi si e czarne okno na ekranie monitora.

Dzia n i e: JERUSALEM odwraca przerwanie nr 8; w 30 minut po wywo d z aniu zara z onego programu, jego efektywność systemowa wynosi 10% pocz t kowej pr e d k o o c i programu. Niekt o r e odmiany pokazuj t na dole, z lewej strony ekranu czarne okno, kt o r e przy korzystaniu z funkcji przewijania ekranu (Skrolowanie) w e d r u j e do g o r y ekranu.

13 (trzynastego) wypadaj t c e g o w pi t e k, b e d¹ kasowane wszystkie u z y w a n e programy zara z onego systemu.

W niektórych wariantach, znajduje si e t a n c u c h tekstowy 'sUMsDos', jednak z e nowsze warianty nie posiadaj t tego tekstu.

Jerusalem-B

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

OBJAWY: Pliki COM i EXE będą powiększone; efektywność systemu zmaleje; pliki będą kasowane każdego trzynastego w piątek w miesiącu; czarne okno na ekranie monitora.

Działanie: Wirus **JERUSALEM-B** jest praktycznie identyczny jak **JERUSALEM**, poza tym, że nie występuje wielokrotne zarażenie plików EXE.

JERUSALEM-B jest jednym z najbardziej rozpowszechnionych wirusów.

Nie wszystkie warianty zmieniają efektywność systemu. Wirus staje się aktywny, jeżeli o danej dacie, poprzez start zarażonego programu dociera do pamięci. Znajduje się w pamięci, gdy data się zmienia, nie jest aktywny.

WARIANTY: A-204: Tekst 'SUMSDOs' został zmieniony na '*A-204', kodowanie zostało zmienione, aby zapobiec rozpoznawaniu przez detektora wirusów (Skaner wirusów). Ten wariant zmniejsza prędkość systemu i wyświetla na ekranie monitora czarne okno.

Anarkia: Podobnie, jak oryginał, jednakże prędkość systemu będzie bardziej zmniejszona, przy czym czas trwania zmniejszonej prędkości systemu jest znacznie dłuższy. Nie wyświetla się żadne czarne okno; tekst 'SUMSDOs' będzie zastąpiony przez 'Anarkia'. Ten wariant wirusa staje się aktywny każdego trzynastego wtorku, jeżeli wypada on w danym miesiącu.

Anarkia-B: Działa podobnie jak **Anarkia**, jednakże wirus staje się aktywny zawsze dwunastego października.

Apocalypse: Ten wariant atakuje programy podczas ich pracy. Pliki COM rosną o 1808-1822 B przy pierwszej infekcji, przy następnych o 1808 B. Tekst 'MsDos' będzie zastąpiony przez 'C.J**'. Po 30 minutach w zaatakowanym systemie, ukazuje się charakterystyczne czarne okno. Ten wirus nie kasuje plików.

Captain Trips: Nazwa pochodzi od występującego tu łańcucha znakowego 'Capitan Trips'. W tym wariantcie nie wyświetla się żadne czarne okno na ekranie, nie zmniejsza się prędkość systemu i programy nie są kasowane w piątek trzynastego. Pliki COM rozrastają się o 1813B. Pliki EXE rozrastają się o 1808-1822B przy pierwszej infekcji, przy następnej infekcji rozrastają się o 1808B.

Captain Trips 2: Jest to wariant wersji 'Capitan Trips', która została zmieniona po to, aby nie był rozpoznawalny przez programy wyszukujące wirusy. Pliki EXE rozrastają się o 1808B.

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

Jerusalem-D: Wariant **Jerusalem-C**, który w każdy piątek trzynastego po 1990 roku, niszczy obydwa kopie FAT.

Jerusalem-DC: Podobny do **Jerusalem-B**; tekst 'SUMSDOs' wyspaczowany; po 30 minutach zmniejsza się efektywność systemu o 30% i wyświetla się czarne okno. Ten wariant nie ma żadnej daty pobudzającej go do aktywności.

Jerusalem-E: Wariant **Jerusalem-D**, który w każdy piątek trzynastego, po 1992 roku niszczy obie kopie FAT.

Jerusalem USA: Jak **Jerusalem-C**, kasuje także w piątek, wg. generatora liczb losowych przypadkowe pliki i FAT.

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

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

Phenomene: Podobny do wirusa Apocalypse, atakuje także plik COMMAND.COM. Wirus zawiera tekst 'Phenomene.COM'.

Puerto: Podobny do wirusa Mendoza; reinfekuje pliki EXE.

Skism-1: Duże podobieństwo do innych wariantów i oryginału. Jest aktywny od roku 1991-go w każdy piątek, po 15-tym. W tych dniach rozmiary wszystkich aktywnych plików będą skrócone do zera. Rozmiary plików typu COM rosną o 1808, a plików EXE o 1808-1822 bajtów. Wprowadza czarne okno i hamuje pracę systemu.

Spanish JB: Nazywany także '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
Wielkość: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek
atakujê tabelê partycji twardego dysku

OBJAWY: System zawiesza siê; komunikat na ekranie monitora

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

JOSHI wykazuje podobieñstwo do dwóch wirusów:
- podobnie, jak wirus **Stoned**, atakuje tabele partycji twardego, dysku
- 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 wartoœci '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 znajdujê siê na œcie¿ce 0 w 9-tym sektorze.

Michelangelo

ALIAS: [-]
Wielkość: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek
atakujê tabelê partycji twardego dysku

Dzia³anie: MICHELANGELO instaluje siê rezydentnie w pamięci, 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 pamięci zmniejsza siê o 2KB, które wirus zajmuje w górnym obszarze pamięci, 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 twardego dysku, je¿eli wykonamy dowolne operacje na plikach znajduj¹cych siê na twardego 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 twardego zostanie zapisany przez zawartoœæ pamięci operacyjnej.

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

MusicBug

ALIAS: Music Boot, Music Bug
Wielkość: [-]
TYP: rezyduje w pamięci
atakuj sektory startowe dyskietek
atakuj tabelę partycji twardego dysku

OBJAWY: Zmniejszenie całkowitego i dostępnego obszaru pamięci; odgłosy klikania; zniszczone obszary na dysku twardym; muzyka w dowolnych momentach.

Działanie: MUSIC BUG instaluje się rezydentnie w pamięci, gdy system ładuje się pierwszy raz, z zarażonej dyskietki startowej. Całkowity i dostępny do dyspozycji obszar pamięci zmniejsza się o 2KB, które wirus zajmuje w górnym obszarze pamięci, ale zawsze poniżej granicy 640KB. Wirus broni się przed nowym zapisem przez inne programy. Podczas ładowania systemu z zarażonej dyskietki / dysku twardego, mogą wystąpić odgłosy klikania w głośniku komputera, jednakże częściej mogą to być krótkie kawałki melodii.

Jeżeli wirus zainstalował się rezydentnie w pamięci, to przy każdym korzystaniu z dyskietki / dysku twardego usłyszymy dalsze części melodii. Poza tym, każda dyskietka / dysk twardy zostanie zaatakowany, jeżeli będzie użyty. Na dysku twardym będzie zarażony sektor startowy i tabela partycji. Poza tym program DOS'a CHKDSK, wykazuje 4096B w straconych obszarach, które zawierają wirusa i kopie oryginalnego sektora ładowania; w tych 4096B znajduje się między innymi następujący tekst:

‘MusicBug v1.06. Macrosoft Corp.’, ‘Made in Taiwan’

NoInt

ALIAS: [Bloomington, LastDirSect](#)
Wielkość: [-]
TYP: [rezyduje w pamięci, ukryty](#)
[atakuje sektory startowe dyskietek](#)
[atakuje tabelę partycji twardego dysku](#)

OBJAWY: Całkowity i dostępny obszar pamięci będzie zredukowany; katalogi będą zniszczone.

Działanie: **NOINT** ładuje się rezydentnie do pamięci, gdy system jest startowany po raz pierwszy z zainfekowanej dyskietki. Całkowita i dostępna pamięć zostanie o 2KB zmniejszona, którą wirus zajmuje dla siebie pod koniec górnego obszaru pamięci, jednakże zawsze poniżej granicy 640KB. Po tym czasie tabela partycji będzie już zaatakowana.

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

Dla dyskietek 360KB, będzie przez wirus przepisany oryginalny sektor ładowania do sektora 11 (ostatni sektor głównego katalogu), a dla dyskietek 1.2MB na sektor 17 (również do głównego katalogu). Jeżeli były te sektory, rzeczywiście przez katalogi wykorzystywane, to odpowiednie pliki ulegną zniszczeniu. Wirus **NOINT** nie daje żadnych komunikatów przy uruchamianiu systemu; dostęp do systemu /dysku twardego oraz proces startowania systemu trwa znacznie dłużej, niż przy nie zainfekowanym systemie. Ładowanie systemu z nie zarażonej dyskietki startowej 1.2MB, często bywa przerywane z powodu błędów ładowania 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 odpowiedŹ '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

Wielkość: [-]

TYP: rezyduje w pamięci
atakujektor sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

Dzia³anie: Jeœli **PING PONG** uaktywria 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
Wielkość: [-]
TYP: rezyduje w pamięci
atakuję sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

Dzia³anie: **PING PONG-B** jest odmian¹ wirusa **PING PONG**; g³ówna ró¿nica polega na tym, że **PING PONG-B** atakuje tak¿e twardy dysk. Wirus ten, podobnie jak wirus FROM mo¿e zostaæ usunięty 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
Wielkość: 3012
TYP: rezyduje w pamięci
Wirus ³¹czy się
atakuj sektor startow dyskietek
atakuj pliki COM i EXE
nie atakuj COMMAND.COM

OBJAWY: Działanie wirusa jest zależne od daty systemu; zainfekowane pliki COM i EXE zwiększają się o 3012-3020B; nie infekuje sektorów startowych dyskietek; odgłosy eksplozji w głośniku komputera; efektywność systemu pozornie maleje.

Działanie: Przy pierwszym starcie zainfekowanego programu, instaluje się PLASTIQUE rezydentnie w pamięci i zajmuje przy tym 3264B, w dolnym obszarze pamięci. Wirus próbuje zarazić każdy plik COM/EXE, który jest używany lub tylko otwierany; zainfekowane pliki COM rozrastają się o 3012B, pliki EXE o 3020B.

Jeżeli data systemu jest większa od 20 września danego roku, wtedy wirus jest złośliwy i wytwarza odgłosy eksplozji w głośniku lub wciśnięcie się domaga większej pojemności procesora, tak, że normalna praca komputera zostanie sparaliżowana.

WARIANTY: **HM2:** Wirus nie powiela się. Użycie zarażonego pliku powoduje zawieszenie się systemu.

Plastique 4.21: Wyróżnia się tylko możliwością ¹ samodzielnego kodowania.

Plastique COBOL: Zawiera słowo 'COBOL'; pliki COM rozrastają się o 3004B; pliki EXE o 3004-3019B; wirus staje się złośliwy, jeżeli data systemu leży między 1.01 a 21.09; system zmniejsza swoją prędkość obliczeń ¹ i po 20 minutach, możliwości systemu wynoszą ¹ 50%, a po 30 minutach klawiatura będzie unieruchomiona, a pamięć konfiguracji systemu CMOS, zostaje na nowo przez wirus zapisana. Od 22.09 rozpoczyna się stan spokoju i trwa do stycznia następnego roku..

PLASTIQUE-B

ALIAS: [Plastique 5.21, Plastique 2](#)
Wielkość: [4096](#)
TYP: [rezyduje w pamięci](#)
[Wirus](#) ³¹czy się
[atakuje sektory startowe dyskietek](#)
[atakuje pliki COM i EXE](#)
[nie atakuje COMMAND.COM](#)

OBJAWY: Ulepszona wersja wirusa **PLASTIQUE**; działa niezależnie od daty systemu; zarażone pliki COM i EXE rozrastają się o dalsze 4096B.

Działanie: Przy pierwszym starcie zarażonego programu instaluje się **PLASTIQUE-B** rezydentnie w pamięci. Wirus zajmuje 5120B i zapisuje się:
- w dolnym obszarze pamięci, jeżeli data systemu leży przed dniem 20.09 danego roku;
- w górnym obszarze pamięci, jeżeli data systemu leży po dniu 20.09 danego roku.

Każdy otwarty lub zainicjowany plik COM/EXE zostanie zainfekowany.

Wirus **PLASTIQUE-B** atakuje sektor startowy włożonej, do stacji dysków dyskietki. Jeżeli data systemu znajduje się po 20.09.1990 roku, wirus będzie złośliwy i wytwarza odgłosy eksplozji w głośniku komputera lub wciż się domaga większej pojemności procesora, tak, że normalna praca komputera zostanie sparaliżowana. Poza tym, po przekroczeniu dowolnie ustalonej wartości licznika zainstalowanego w wirusie, do wszystkich stacji dysków zostaną wysłane 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; nieoczekiwane 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, Nolnt
Bloomington, Angelina, Manitoba

Wielkoœæ: [-]

TYP: rezyduje w pamieci
atakujektor startowe dyskietek
atakujektor tabelê partycji twardego dysku

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

Dzia³anie: Pierwotna wersja infekowa³a tylko dyskietki 360KB, bez wyrz¹dzania wiêkszych szk³d, tego wariantu ju¿ jednak nie ma. Wszystkie teraŹniejsze warianty tego wirusa zara¿aj¹ tabelê partycji twardego dysku, gdzie g³ówny katalog i FAT bêd¹ uszkodzone. Te wirusy rozrózniane 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 pamieci i zajmuje przy tym ok. 2KB pamieci. 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 pamieci 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 w³œciwego 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 w³œciwego 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 niemo¿liwe. Przy ³adowaniu systemu nie wysy³a ¿adnych komunikatów na ekran. Poza tym atakuje wszystkie typy dyskietek.

ROSTOV: Podobny do **STONED-B**; nie pokazuje żadnych informacji; zawiera następujący tekst: 'Replace and strike' sowie 'Non-system disk'.

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

'EXPORT OF SEX REVOLUTION ver 1.1.'

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

'EXPORT OF SEX REVOLUTION ver 2.0.'

STONED-A: Taki jak orygina³, nie atakuje jednak dysków twardych. Jest to prawersja. Zawiera tekst: 'Your 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 dŹwiêkowym. 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 chroni³cy 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
Wielkość: 3551
TYP: ukryty (zakodowany)
atakuj¹e pliki COM i EXE

OBJAWY: Pliki COM i EXE b¹ed¹ zwi¹kszone; pliki zostan¹ zmienione.

Dzia³anie: **SYSLOCK** przeszukuj^e aktywne drzewo katalogów twardego dysku, wyszukuj^e pliki COM i EXE, wybiera przypadkowo jeden z nich i zara³ga go. Plik b¹edzie zwi¹kszony o ok. 3551B (lub troch^e wi¹cej).

Pliki b¹ed¹ zmienione. Wirus szuka w zara³zonych plikach s³owa 'Microsoft' (niezale³nie, czy pisane du³yymi, czy ma³yymi literami) i zast^epuj^e je s³owem 'MACROSOFT'.

Gdy w o^erodowisku DOS'a (DOS-Environment) wirus znajdzie tekst: 'SYSLOCK=@', to nie wykazuj^e 3adnej aktywno^eci i od razu startuj^e program zarz¹dzaj¹cy systemem.

WARIANTY: **ADVENT:** Normalnie nie powielaj¹cy si^e wirus. Prawdopodobnie, zwielokrotnianie si^e wirusa wyst^epuj^e wtedy, gdy zosta³ zara³zony plik EXE; jego potomkowie atakuj¹ tylko pliki COM.

MACHO-A: Zachowuj^e si^e tak jak **SYSLOCK**, lecz s³owo 'Microsoft' zostaj^e tu zast¹pione przez 'Macrosoft'..

Telecom

ALIAS: Telefonica, Telecom File, Spanish Telecom-2
Wielkoœæ: 3700
TYP: rezyduje w pamieci
ukryty
atakuj¹ pliki COM

OBJAWY: Pliki COM bêd¹ zwiêkszone; ca³kowita i dostêpna pamieæ 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 pamieci, ale zawsze poni¿ej granicy 640KB; program DOS'a CHKDSK.COM pokazuje o 3984B mniej pamieci. Przerwanie nr 21 zostaje odwrócone. Rezyduj¹cy w pamieci wirus **ANTI-TEL** atakuje twarde dyski i dyskietki, które by³y u¿ywane.

W plikach COM, rezyduj¹cych w pamieci, 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 pamieci **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](#)
Wielkość: [2468](#)
TYP: [atakuje tabelę partycji twardego dysku](#)
[atakuje pliki EXE](#)

OBJAWY: Całkowity i dostępny do dyspozycji obszar pamięci zostanie zredukowany o 3072B.

Działanie: Wirus sprawdza przy pierwszym starcie zarażonego programu, czy tabele partycji twardego dysku są już zarażone, jeżeli nie, to wpisuje swój niezakodowany kopię do ostatnich sześciu sektorów twardego dysku i zmienia tabele partycji w taki sposób, że są one do dalszego zarażenia. Do tego czasu wirus nie instaluje się rezydentnie w pamięci i nie zaraża dalszych plików.

Gdy system będzie pierwszy raz startowany z zarażonego twardego dysku, wirus instaluje się rezydentnie w pamięci. Całkowita i dostępna pamięć zredukuje się o 3KB, które wirus zajmuje dla siebie w górnym obszarze pamięci, ale zawsze poniżej granicy 640KB. Wirus zabezpiecza się przed nowym zapisem przez inne programy.

Gdy wirus rezyduje w pamięci, zaraża każdy wywołany program EXE. Wirus dopisuje się do końca programu i zwiększa go o 2468B, jednak to zwiększenie się programu, nie jest widoczne w katalogu, ponieważ wirus rezyduje tylko w pamięci.

Następujący niezakodowany tekst znajduje się w ostatnim sektorze zarażonego 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 !´
```

Porażone wirusem programy zawierają tekst w zakodowanej formie.

Zaatakowane systemy, przy wywołaniu programu DOS'a CHKDSK.COM zgłaszają komunikat 'Błąd przyporządkowania plików', gdy wirus rezyduje w pamięci. Jeżeli ten program będzie wywołany z opcją /f, to programy mogą zostać zniszczone.

Dokładnie, cztery miesiące po zarażeniu tabeli partycji, w danym dniu miesiąca, wirus staje się znowu aktywny, podając komunikat na ekran:

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

Przy wywołaniu programu, który zawiera maszynowe rozkazy, zostanie pokazany komunikat z ostatniego sektora twardego dysku. Wirus TEQUILA, jest bardzo rozpowszechniony w Europie. Wirus ten został rozpowszechniony przez pewne szwajcarskie przedsiębiorstwo wyspykowe.

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
Wielkość: 1689
TYP: rezyduje w pamięci
atakuj pliki COM i EXE

OBJAWY: Zwiększa pliki COM i EXE; System zawiesza się.

Działanie: USSR 1689 instaluje się przez uruchomienie pierwszego zarażonego programu rezydującego w pamięci, w rezydentnej części interpretera rozkazów. Najbliższy program COM lub EXE zostanie zaatakowany, który z kolei będzie przyczyną powiększenia się systemu. Zarażone programy zwiększają się o 1689B, ale ten wzrost programów, które przed zarażeniem są większe niż 1689B jest przez wirus skutecznie ukryty. Pliki, które byłyby mniejsze niż 1689B (przed zarażeniem wirusem), będą zwiększone i będzie to zauważalne w katalogu. Wirus dopisuje się zawsze na koniec programu.

Przy każdym zarażeniu programu, występuje zawieszenie się systemu i dlatego wirus ten, tak szybko się nie rozprzestrzenia jak inne wirusy i przez to można go wcześniej wykryć.

Vacsina

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

OBJAWY: Pliki COM, EXE, SYS i BIN rozrastają się; Sygnał pisku w głośniku komputera.

Działanie: **VACSINA** atakuje pliki COM, EXE, SYS i BIN. Pliki EXE zostaną zamienione na pliki COM (pierwsze 2 bajty 'ZM' lub 'MZ' pliku będą w rozkazie JMP zamienione w dołączonym kodzie wirusa, który zawiera własną procedurę przesunięcia).

Wirus ten występuje w bogatej formie wariantów (co najmniej 48). Cechą charakterystyczną zarażonego programu jest to, że przy jego wywołaniu, słychać piski w głośniku komputera; poza tym ulega zmianie czas i data w katalogu, które to (czas i data) zmieniają się na takie, jakie były w katalogu w momencie zaatakowania przez wirus.

WARIANTY: **TP04VIR:** Zaraża pliki EXE i zamienia je wewnętrznie na pliki COM. Zaatakowane programy zawierają tekst 'VACSINA', a przedostatni bajt zawiera binarną czwórkę.

TP05VIR: Podobny do **TP04VIR**, jednakże drugi od końca bajt zawiera binarną piątkę. Poza tym czasami system zawiesza się.

TP06VIR: Podobny do **TP05VIR**, jednakże drugi od końca bajt zawiera binarną szóstkę.

TP16VIR: Podobny do **TP06VIR**, jednakże drugi od końca bajt zawiera binarną szesnastkę.

TP23VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 23. Tekst 'VACSINA' nie występuje.

TP24VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 24.

TP25VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 25.

Vienna

ALIAS: [Austrian](#), [Unesco](#), [DOS-62](#), [648](#), [DOS-68](#), [1-in-8](#)
Wielkoœæ: [648](#)
TYP: [atakuję pliki COM](#)

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

Dzia³anie: Uruchamiaj¹c program zara¼ony przez **VIENNA**, zara¼a 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 zara¼onego 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. Poniewa¼ wirus nie dopisuje siê do programu, jest trudny do odkrycia przez skenery szukaj¹ce. Nawet po usuniêciu wirusa, mog¹ powstaæ nie przewidziane skutki, a¼ wszystkie zmienione programy zostan¹ wymienione na niezara¼one kopie, co daje gwarancjê, Ÿe system nie jest zainfekowany.

Przy niektórych zaatakowanych programach, mo¼e wyst¹piæ te¼ 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 du¼o odmian i wariantów tego wirusa, i dlatego te¼ mog¹ wyst¹piæ jeszcze inne symptomy tego wirusa, ni¼ 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 zara¼eniu 7 plików w aktualnym katalogu, zostan¹ zara¼one pliki w C:.

VIENNA-B: Podobny do orygina³u, jednak zamiast modyfikacji restartu jednego z szeœciu zara¼onych plików, zostanie skasowany wywo³any aktualnie program.

VIENNA-B 645: Podobny do orygina³u, lecz bez modyfikacji restartu i bez kasowania zara¼onych plików.

WIEN: Tak, jak orygina³, jednak posiada œrodki uniemo¼liwiaj¹ce 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
Wielkość: 2885 lub 2899
TYP: rezyduje w pamięci
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE rozrastają się; o godzinie 5:00 (wg. zegara systemowego), zabrzmie melodia z głośnika komputera.

Działanie: Jeżeli zostanie uruchomiony zarażony program, instaluje się **YANKEE DOODLE** rezydentnie w pamięci i zaraża pliki COM i EXE. Gdy zegar systemowy osiągnie godzinę 5:00 po południu, to z głośnika komputera rozbrzmiewa melodia Yankee-Doodle. Poza zainfekowaniem plików, nie wyrządza żadnych innych szkód.

Wirus Yankee Family obejmuje ok. 80 różnych wirusów..

WARIANTY: **TP33VIR:** Ten wariant zmienia po kryjomu przerwanie nr 1 i 3 tak, że nie można więcej użyć programu Debugger do odcodzenia wirusa. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 33 dziesiętnie).

TP34VIR: Podobny do **TP33VIR**, jednak rezyduje w pamięci i zaraża programy, gdy są one używane. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 34 dziesiętnie).

TP38VIR: Podobny do **TP34VIR**, lecz różnie traktuje pliki COM i EXE. Poza tym, wirus sam się odkłada, jeżeli program został wystartowany przez CodeView-Debugger. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 38 dziesiętnie).

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

TP42VIR: Ten wariant sprawdza, czy system jest zarażony wirusem **PING PONG** i modyfikuje go, w tym sensie, że wirus ten sam się niszczy. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 42 dziesiętnie).

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

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

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

4096

ALIAS: Century, Frodo, 100 Years
Wielkość: 4096
TYP: rezyduje w pamięci
atakuję pliki COM, EXE i OVL
błędny FAT

OBJAWY: Pliki COM i EXE błędnie powiększone; System zawiesza się; Silne zmniejszenie prędkości roboczej systemu.

Działanie: Gdy wirus znajduje się w pamięci, nie wyświetla się przy pomocy polecenia DIR, zmienione wielkości plików. Wirus atakuje każdy wykonywany (uruchamiany) plik. Niszczy FAT poprzez Crosslinking. Każdego roku w dniu 22.09 system zawiesza się.

Osobliwości: Prawdopodobnie, w wirusie znajduje się błąd, który kończy się pętlą programu. Bez tego błędu byłby zmieniany sektor badowania, co powinno wyświetlać następujący komunikat:
'FRODO lives'

DIR-2

ALIAS: Creeping Death (CD), FAT
Wielkość: [-]
TYP: inteligentny, rezydujący w pamięci wirus Stealth
wirus sektora startowego
FAT-Crosslinking

OBJAWY: Zgubiony Cluster; przy kopiowaniu pliki zostaną zniszczone; jeżeli system będzie startowany z dyskietki, to rozkaz CHKDSK zgłosi zgubione łańcuchy (Crosslinking); CHKDSK /F niszczy pliki !!!.

!

Działanie: Wirus **DIR-2** jest bardzo szybki, uaktywnia się podczas ładowania systemu z zarażonej stacji dysków lub twardego dysku. Jest bardzo trudny do wykrycia, ponieważ nie posiada żadnych widocznych cech charakterystycznych. Wirus nie atakuje plików programowych, lecz zmienia FAT (tablicę przydziałów plików). Po zarażeniu dyskietki, wpisuje się on do ostatniego clustera na dyskietce.

Osobliwości: **DIR-2** wprowadza swój cluster (adres startowy) do FAT dla każdego programu. Oryginalny cluster programów zostanie umieszczony w poszczególnym pliku. Jedyny rozpoznawalny efekt to: wszystkie pliki posiadają zagubione łańcuchy (są crosslinked) w jednym cluster, w którym znajduje się wirus. Próba korekcji tego przy pomocy CHKDSK /f powoduje zniszczenie pliku.

WARIANTY: DC10, DC11, DC12

Parity Boot

ALIAS: [-]
Wielkość: [-]
TYP: rezyduje w pamięci
wirus sektora ładowania tzw. Bootsektor
Wirus Stealth

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

Działanie: **PARITY BOOT** (bardzo parzyście przy startowaniu systemu). Zalicza się do
dobrze rozpowszechnionych w ostatnim czasie wirusów, sektora
startowego. Został napisany jesienią 1992 roku, prawdopodobnie w
Niemczech. Od połowy 1993 roku, występuje on we wzmożonej formie. Na
podstawie jego szczególnych Stealth-właściwości, znajduje się on w
komputerze w stanie utajonym i zarządza każdą dyskietkę sformatowaną na tym
komputerze. Wirus **PARITY BOOT** zapamiętuje oryginalny sektor ładowania i
kieruje każde odpytanie sektora ładowania do zapamiętanego oryginału,
skutkiem tego jest to, że programy antywirusowe w zarażonym systemie z
trudem mogą go zidentyfikować..

Delwin

ALIAS: [-]
Wielkość: 1759
TYP: rezyduje w pamięci
atakuje pliki EXE i tablicę partycji (MBR)

OBJAWY: Wirus rezyduje w pamięci i infekuje (zaraża) Masterbootrecord. Wirus zajmuje 2KB w pamięci. Powiększa pliki EXE o 1759 Bajtów. Oryginalną tabelę partycji przenosi i zapisuje w Sektor 0,0,2.

Działanie: Wirus posiada bardzo szkodliwe funkcje! Potrafi odczytać datę systemową i dokonać w niej skomplikowanych operacji (zarażając określa ilość sekund w pliku). Powoduje np to: że uruchamiamy zarażone pliki, które początkowe litery mają np: WI, na pytanie o wersję DOS, wirus podaje 2.10, co prowadzi do unieruchomienia wielu programów, które pracują na wersjach wyższych.

Junkie

ALIAS: (-)
Wielkość: 1030-1024
TYP: rezyduje w pamięci
atakuje pliki EXE, COM i tabelę partycji (MBR)

OBJAWY: Wirus powstał prawdopodobnie w Szwecji. Wirus rezyduje w pamięci i tabeli partycji (MBR). Przy uruchamianiu zainfekowanych plików z rozszerzeniem COM, atakuje wirusem Junkie dwa pierwsze sektory twardego dysku. Długość wirusa wynosi 1024 Bajty. Wirus potrafi zmieniać swój dźwięk ale nie jest poliformiczny (samokodujący).

Działanie: Wirus w swym wnętrzu posiada tekst:
Dr. White - Schweden - 1994 Junkie Virus - written in Malmo
Powyższych tekstów nigdy nie wyświetla. Program unieruchamia (wyłącza), rezyduje programy antywirusowe.

Sampo

ALIAS: 69, WLLOP
Wielkość: (-)
TYP: rezyduje w pamięci
atakujê tabelê partycji (MBR)

OBJAWY: Wirus powsta³ na Filipinach. Atakuje sektor startowy dyskietek (tzw. Bootsektor) i tabele partycji dysku twardego. Przy starcie komputera wirus Sampo zara³a z g³ówniej pamięci, w której rezyduje.

Dzia³anie: Aktywny wirus wydaje komunikat:
SAMPO Projekt X Copyright © 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 pamieci
atakujê tabelê partycji (MBR)

OBJAWY Wirus zaraŹa Bootsektor dyskietek i tabelê partycji dysku twardego. Wirus rozpowszechniony w Skandynawii.

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

Jackripper

ALIAS: (-)
Wielkoœæ: (-)
TYP: rezyduje w pamieci
atakujê tablicê partycji (MBR)

OBJAWY Wirus zaraŹa 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 twardego dysku. Tym samym niszczy pliki. Odbudowanie ich struktur nie jest moŹliwe. Kod ³añcuchowy zawiera tekst: FUCK EM UP!

Jumper

ALIAS: French
Wielkość: [-]
TYP: rezyduje w pamięci
atakujê 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 pamieci
atakuj¹ 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 pamieci
atakujê tablicê partycji (MBR)

OBJAWY Wirus atakuje sektor startowy dyskietek (tzw. Bootsektor) i tabelê partycji dysku twardego. Ma w³aciwoci "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 pamieci
atakuj e pliki COM

OBJAWY Wirus Ambulance powieksza 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 karetki. Dodatkowo s³yszalny jest jej sygna³ alarmowy.

Black Monday

ALIAS: (-)
Wielkość: 1055
TYP: rezyduje w pamięci
atakuję pliki COM i EXE

OBJAWY Wirus powiększa pliki COM i EXE o 1055 Bajtów.

Działanie Komunikuję się: Black Monday 2/3/90 KV KL MAL. Nie da się go usunąć całkowicie z plików EXE, ponieważ niszczy i zapisuję część pliku.

Quox

ALIAS: (-)
Wielkoœæ: 1024
TYP: rezyduje w pamieci
atakujê tablicê partycji (MBR)

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

Dzia³anie Wirus wpisuje siê do pamieci g³ównej komputera.

Seventh son

ALIAS: (-)
Wielkoœæ: 332
TYP: [nie rezyduje w pamieci](#)

OBJAWY Wirus atakuje pliki COM

Dzia³anie Brak szerszych informacji.

Maltese Amoeba

ALIAS: (-)
Wielkoœæ: (-)
TYP: rezyduje w pamieci
atakuj e 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 pamieci](#)
[atakuje pliki COM i EXE](#)

OBJAWY: Atakuje pliki COM/EXE. Niektóre programy wywo³uj¹ *Runtime Error*.
31.paŹdziernika (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 pamieci
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](#)
Wielkość: 1099
Pochodzenie: [HongKong z VGA-Treiber](#)
TYP: rezyduje w pamięci
atakuj e pliki COM i EXE

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

Dzia³anie: Nie jest znane.

WARIANTY: Znana jest wersja o d³ugoœci 1091 Bajtów.

Boot1

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

OBJAWY: Wirus atakuje Bootsektor dyskietek wzgl. tabelê partycji dysku twardego. Zaprogramowany doœæ prosto. ZaraŹa tabelê partycji, przy starcie z zaraŹonej dyskietki. ZaraŹa wszystkie niezabezpieczone dyskietki, kiedy jest rezydentny.

Szkody: Brak szczeg³ów. Przy zaraŹeniu dyskietek, dochodzi niekiedy do utraty danych.

WARIANTY: Nie s¹ znane inne warianty wirusa.

Omega

ALIAS: [Reset, Freitag der 13.](#)
Wielkość: 440
Pochodzenie: [Finlandia](#)
TYP: [nie rezydentny, atakuje pliki COM](#)

OBJAWY: Wirus atakuje pliki COM. Infekuje tabele partycji każdego piątku dnia 13.

Działanie: Wirus zrobiony dość prosto. Przy wywołaniu zarażonego programu wirus przeszukuje katalog i zaraża wszystkie pliki COM.

Szkody: W każdy piątek 13-ego wyświetla znak i zajmuje dwa pierwsze sektory dysku twardego. Niszczy przez to tabelę partycji i pliki są nieodwracalnie stracone.

WARIANTY: Nie są 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 zaraŹa tabele partycji (Bootsektory) uŹywanych dyskietek i twardych dysków.

Dzia³anie: UwaŹany jest za niebezpieczny wirus bootsektorowy. Dysponuje wszystkimi w³aœciwoœciami nowoczesnego wirusa atakuj¹cego bootsektor. Godne uwagi s¹ wyrz¹dzone przez niego szkody.

Szkody: Wirus zamyka wszystkie pliki na twardym dysku, kiedy komputer dzia³a d³uŹej niŹ 24 godziny. Do³¹cza komunikat: DISK KILLER Version 1.00

WARIANTY:

Stardot

ALIAS: 18. September
Wielkość: pliki EXE - 600, 789 lub 801
Pochodzenie: [-]
TYP: nie rezydentny, zaraża pliki COM i EXE, niebezpieczny

OBJAWY: Wirus atakuje pliki COM i EXE. Zapisuje twarde dyski 18 września o godzinie 7.

Działanie: Najpierw dołącza do każdego pliku 10-16 B, następnie atakuje plik. Prowadzi to do problemów, jeżeli nie usuniemy go dokładnie.

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

WARIANTY: Znany jest w 3 różnych wariantach długości.

Mystic

ALIAS: [Liberty](#)
Wielkość: 2857
Pochodzenie: [Południowo-wschodnia Azja](#)
TYP: [rezydentny, atakuje pliki EXE i COM](#)

OBJAWY: Wirus zaraża pliki EXE/COM. Pierwsze 120 B zajmuje tekstem: M Y S T I C Copyright 1989. Prowadzi to do problemów, kiedy używamy tego obszaru pliku albo usuniemy wirusa. Samoczynnie doczepia się do pliku.

Działanie: Działanie i szkody nie są jeszcze dokładnie znane.

Szkody: [-]

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

Shirley

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

OBJAWY: Wirus zaraŹa 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 zaraŹa 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](#)
Wielkość: [1336](#)
Pochodzenie: [Niemcy \(BRD\) 1986 rok](#)
Typ: [nie rezydentny, atakuje pliki COM](#)

OBJAWY: Wirus zaraża pliki COM.

Działanie: Jest to jeden z najstarszych wirusów. Został zaprogramowany jako wirus demonstracyjny w roku 1986 przez R. Burgera. R. Burger użył go jako przykładu ostrzegawczego do swej książki Computer Viruses. Wariant pierwotny meldował o zarażeniu i umożliwia naprawę. Nowe warianty posiadają komunikat o zmienionej treści lub nie posiadają go.

Szkody: Nie czyni poważnych szkód.

WARIANTY: Znane są różnorodne warianty tego wirusa.

Donnerstag der 12.

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

OBJAWY: Wirus zaraŹa pliki EXE i COM. W kaŹdy czwartek dnia 12, komunikat w jêzyku niemieckim.

Dzia³anie: Wirus jest bardzo dobrze zaprogramowany. KaŹdego czwartku 12 dnia wysy³a komunikat: Morgen ist Freitag der 13 (jutro jest pi¹tek 13). Swoj¹ nazwê VirCheck zawdziêcza faktowi Źe 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 zaraŹa pliki COM.

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

Szkody: Brak szczeg³ów.

WARIANTY: wszystkie warianty s¹ nam znane.

Horse-Familie

Alias: [Bulgarian horse , Hacker](#)
Wielkość: (-)
Pochodzenie: [Bułgaria](#)
Typ: [rezydentny, atakuje pliki COM i EXE](#)

OBJAWY: Ta rodzina wirusów wydaje się być serią eksperymentalną. Jest on (jak na razie) dość prosto zaprogramowany, a wszystkie wersje pochodzą prawdopodobnie z ręki jednego programisty. Powstały dotychczas dwa różnorodne warianty (10 różnych wersji). Oprócz tego pojawił się wirus bootsektorowy, Horse Boot Virus. Prawdopodobnie w przygotowaniu jest wersja replikująca.

Działanie: Nie stwierdzono szkodliwego działania.

Szkody: (-)

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

Horse Boot

Alias: [Bulgarian Horse](#)
Wielkość: (-)
Pochodzenie: [Bułgaria](#)
Typ: [rezydentny, atakuje sektory startowe dyskietek Bootsektor, tabelę partycji twardego dysku](#)

OBJAWY: Wirus zaraża sektory startowe dyskietek (Bootsektor) i tabele partycji twardego dysku.

Działanie: Wirus zaprogramowany do działania prosto.

Szkody: Nie znane są meldunki o powodowaniu jakichkolwiek szkód.

WARIANTY: Należy prawdopodobnie do eksperymentalnej serii wirusów HORSE.

VCS Familie

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

OBJAWY: Wirus zaraża pliki COM. Usuwa AUTOEXEC.BAT i CONFIG.SYS

Działanie: Rodzina wirusów bazuje na programie Constuction Set. Tworzy on wirusy wyświetlające dany tekst po upływie dowolnego czasu. W końcu 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 życzeń bożonarodzeniowych VDV (Związku Niemieckich Miłośników Wirusów)

Hafenstraße

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

OBJAWY: Wirus zaraża pliki EXE.

Działanie: Wirus prosto zaprogramowany. Przy wywołaniu zarażonego programu atakuje 1 kolejny plik.

Szkody: Przy wywołaniu tworzy ukryty plik zawierający tekst: Hafenstraße bleibt !
Prowadzi to do problemów z pamięcią w katalogu głównym (zajmuje miejsce na twardym dysku).

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

Keypress

Alias: [Turku, DJIDDA, Twins](#)
Wielkość: [1232 \(EXE\) lub 1472 \(COM\)](#)
Pochodzenie: [prawdopodobnie z Finlandii](#)
Typ: [rezydentny, atakuje pliki EXE i COM](#)

OBJAWY: Atakuje pliki EXE/COM. Dwie różne długości dla plików COM i EXE.

Działanie: Po wywołaniu zarażonego programu, wirus przeszkadza w poleceniach, gdzie powtarzają się znaki klawiatury. Czasem odzywa się również głosnik, co może być wynikiem przepełnienia buforu klawiatury.

Szkody:

WARIANTY: Znane są różne warianty.

Violetta

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

OBJAWY: Wirus zaraża pliki COM.

Dzia³anie: Ten zaprawdê d³ugi wirus, zaprogramowany jest doœæ prymitywnie. Prawdopodobnie, jest to nieudoscionalna 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 pamieci 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 niszczyc FAT, co prowadzi do ca³kowitej utraty danych.

WARIANTY:

Chemnitz

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

OBJAWY: Wirus zaraŹa 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 zaraŹa pliki COM. Zainfekowane pliki maj¹ przypisane 62 sekundy.

Dzia³anie: Po wywo³aniu zaraŹonego pliku, wirus dostaje siê do pamieci i zaraŹa dalsze pliki. MoŹe dojœæ do bardzo d³ugich poszukiwañ.

Szkody: Ósmego kaŹdego 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 zaraŹa pliki EXE.

Dzia³anie: Nie wydaje siê mieæ Źadnych szkodliwych w³aœciwoœci.

Szkody:

WARIANTY:

Hungarian

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

OBJAWY: Wirus zaraŹa 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 zaraŹa 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 zaraŹa 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 zaraŹa pliki COM i EXE. Zapisuje twardy dysk kaŹdego 17 listopada.

Dzia³anie: Do dnia dzisiejszego znana jest rodzina 4 wirusów.
W zaleŹnoœci od rodzaju maj¹ r³õne dzia³anie.

Szkody: 768 zapisuje dysk 17.paŹdziernika
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 zaraŹa pliki COM. Do zainfekowanych plików dopisuje 62 sekundy.

Dzia³anie: Nie stwierdzono szkodliwego dzia³ania.

Szkody:

WARIANTY:

generic (123PBF) virus

Tłumaczenie: ogólny

Informacja: Właściwie to nie jest wirus. Niektóre programy antywirusowe, meldują grupy wirusów i podejrzenie o zarażeniu, działa tylko w ten sposób, przy czym:
generic 1 lub P oznacza tabelę partycji PT-Virus
generic 2 lub B wirus bootsektorowy
generic 3 lub F zwykły file virus

Taki komunikat innego programu, powinno się traktować poważnie. Może to oznaczać wykrycie wirusa.

Prosimy powiadomić nas przez HOTLINE.

possible virus found

informacja: To na pewno nie jest wirus! (possible ang. -> możliwe). Przeważnie 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 zaraża Bootsektor dyskietek i tabele partycji u¿ywanych dysków.

Dzia³anie: Interesuj¹cy jest fakt, Ÿe 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:

