Fguard pro Windows

Fguard pro Windows je jeden z antivirových programù firmy ALWIL Software, který je urèen pro hlídání systému Windows 3.1 a novìjší v reálném èase.

Program øeší jeden z nejkritiètìjších problémù Windows, tzn. ochranu systému proti neoèekávaným nebo neoprávnìným projevùm èinnosti virù nebo uživatele. Jedná se o jedineèný program, který je schopen øešit i takové problémy, jako je ochrana proti systému pøi pokusu o formátování disku, pokusy o ètení tabulky rozdìlení pevných diskù a mnohé jiné kritické èinnosti, které jiné antivirové systémy v oblasti Windows neberou v úvahu.

Základní informace

- Instalace programu
- Princip práce
- Parametry programu
- Ovládání programu

Historie

- Verze 7.70
- Verze 7.50
- Verze 7.0
- Zmìny proti starším verzím
- Pùvod programu

Pøílohy

- Likvidace virù
- Požadavky pro práci
- Chyby a fatální chyby

Instalace programu

Program se instaluje v prùbìhu instalace systému AVAST!. Jeho samostatná instalace není možná z dùvodù komprimace jednotlivých souborù na distribuèních disketách.

Instalace samotná probíhá ve dvou krocích. První z nich je program pracující v DOSu, který instaluje programy pracující v systému DOS. Po kladné odpovìdi na dotaz, zda chcete instalovat i programy pro Windows, se instalují i soubory, které jsou nutné pro dokonèení instalace v systému Windows.

Vlastní instalace v systému Windows spoèívá ve spuštìní instalaèního programu SETUP.EXE, který je standardní souèástí dodávky a je pøipraven po instalaci systému AVAST! pro DOS.

V této èásti instalace bude program Fguard pro Windows zaøazen do skupiny AVAST!, která je automaticky vytvoøena, a do startovací skupiny Windows.

Princip práce

Program Fguard pro Windows z uživatelského hlediska pracuje stejnì, jako program Fguard pro DOS. Jeho interní èinnost je však od programu pro DOS úplnì odlišná.

Fguard pro Windows není ve skuteènosti pouze jeden program. Je to oznaèení pro nìkolik souborù a èástí kódu, které spolu komunikují a jsou na sobì plnì závislé.

Na straní operaèního systému DOS jsou to programy Fguard a Rguard, které obsahují nìkteré èásti kódu nutné pro správnou inicializaci a vzájemnou komunikaci obou systémù. Støední èlánek tvoøí soubor AVAST.386, 32 bitový program, který plní funkce spojení mezi operaèními systémy a v nìkterých pøípadech vypisuje hlášení o provádìné operaci. Poslední èástí je program FGW.EXE, 16-ti bitový program pro systém Windows, který má na starosti komunikaci s uživatelem prostøednictvím standardního rozhraní systému. Svou roli hraje i dynamická knihovna FGWLIB.DLL, která obsahuje správu nìkterých pøerušení a rutiny, které musejí být neustále v pamìti.

Fguard pro Windows pro svou práci vyžaduje pøítomnost rezidentních programù v pamìti pøed spuštìním systému Windows. Podle toho, co chcete v systému chránit, to musí být Fguard nebo Rguard nebo oba spoleènì.

Veškerou ochranu v systému Windows 3.x mají na starosti programy pracující v DOSu. Tato skuteènost vyplývá ze skuteènosti, že Windows 3.x prakticky úplnì závisí na systému souborù DOSu. Všechny ostatní uvedené programy slouží pro rychlé a bezpeèné pøenesení informace do Windows, zobrazené zprávy a odeslání odpovìdi nazpátek programu v DOSu.

- Spouštìní programu
- Spouštìní systému Windows
- Ukonèení programu
- Spolupráce se systémem DOS

Spouštìní programu

Fguard pro Windows je standardní program systému Windows, který je možné spustit jako každý jiný program urèený pro toto prostøedí. Pokud se ho pokusíte spustit z DOSu, program vypíše hlavièku a informuje Vás o této skuteènosti.

Pøi spuštìní programu byste mìl mít v DOSu instalovaný program Fguard pro DOS, Rguard pro DOS nebo oba spoleènì, jinak Fguard pro Windows vypíše chybové hlášení a ukonèí svou práci. Všechny tyto programy musí mít stejné èíslo verze, jinak se program neodstartuje.

Pokud chcete používat tuto nápovìdu, musíte mít pøíslušný soubor nápovìdy (FGW.HLP) umístìn ve stejném adresáøi jako vlastní program. Pokud používáte instalaèní program, nemusíte se o tuto podmínku starat, všechny soubory se nainstalují do jednoho adresáøe.

Program Fguard pro Windows Vám doporuèujeme spouštìt automaticky se startem systému Windows, což zaruèí správnou funkci programu Fguard a Rguard i se systémem Windows a znemožní zablokování systému a z toho vyplývající ztrátu dat.

Spouštìní systému Windows

Soubory programu Fguard pro Windows nijak neovlivòují spuštìní systému Windows ve standardním a reálném režimu práce a není je možné v tìchto režimech vùbec použít. Soubor AVAST.386 není vùbec systémem rozeznáván jako souèást Windows a program FGW.EXE pøi startu testuje konfiguraci systému a v tìchto režimech odmítne pracovat.

Pro rozšíøený režim je nutné dodržet nìkolik podmínek. Pokud máte v pamìti DOSu instalován program Fguard, Rguard nebo oba spoleènì je nutné je mít ve stejném adresáøi a v nìm mít taky soubor AVAST.386. Pokud tomu tak není, jeden z programu vypíše varovné hlášení a Windows nebudou v rozšíøeném režimu spuštìny. Program Fguard pro Windows je možné umístit do libovolného adresáøe. Je ho možné spustit jenom za pøedpokladu, že Windows pracují v rozšíøeném režimu a pøi startu Windows byl úspìšnì instalován program AVAST.386.

Ukonèení programu

Fguard pro Windows mùžete ukonèit jako každý jiný program v systému Windows. Jelokož se tento program skládá ze dvou èástí a dùležitìjší z nich, soubor AVAST.386, zùstává v pamìti po celou dobu práce systému je po ukonèení programu Váš poèítaè stále stoprocentnì chránìn. Není-li však systém instalován kompletnì, ztrácíte:

- Možnost interaktivní zmìny konfigurace ochrany poèítaèe,
- Grafický režim zobrazování varovných hlášení. Veškerá varování budou zobrazována v textovém režimu (stejný režim používají kritická varovaní systému Windows, napøíklad pro varování pøed resetováním poèítaèe z klávesnice),
- Možnost testování spouštìných programù na pøítomnost virù.

Všechny ostatní parametry ochrany zùstávají zachovány. Pro správnou funkci programu Vám doporuèujeme nechat program pracovat po celou dobu práce Windows.

Spolupráce se systémem DOS

Antivirová ochrana zajiš□ovaná programem Fguard pro Windows používá pro svou práci stejná data jako systém DOS. Toto øešení má své výhody i nevýhody. Výhodou je, že v každém okamžiku jsou konfiguraèní data jednoznaènì urèená a systém není v žádném okamžiku zbaven kontroly. Uživatel rovnìž ví, že se zmìnou operaèního systému zùstávají všechny parametry ochrany nezmìnìny.

Na tyto skuteènosti se však mùžeme podívat i z opaèného hlediska. Nìkdy mùže být výhodné mít jinou konfiguraci pro DOS a jinou pro Windows. Tato koncepce však se sebou nese vysoký stupeò nekonzistence. Pokud pøi práci ve Windows nepoèítáme se spouštìním aplikací DOSu, je øešení velice jednoduché. Staèí pøi spuštìni Windows nahradit konfiguraèní data DOSu daty pro systém Windows a problém by byl vyøešen. Co však dìlat, pokud chceme spustit jednu aplikaci DOSu? Musíme zajistit, aby jeden program, který je instalován pøed spuštìním Windows, mìl zároveò k dispozici dvì sady konfiguraèních dat a zároveò v reálném èase zjiš□ovat, která data mají být použita bez jakékoli znalosti pøíèiny (Windows nebo DOS), která reakci programu vyvolala a to všechno ještì napøíklad v pøerušení BIOSu pøi pokusu o formátování disku. Øešení není triviální a situace není ještì stále tak jednoduchá. Aplikací DOSu mùže být spuštìno více a každá z nich mùže mìnit konfiguraci rezidentních programù podle své libovùle (pøesnìji dle libovùle uživatele).

Z tìchto dùvodù jsme si vybrali první øešení a všechny aplikace (Fguard, Rguard, FGW i AVAST.386) pracují se stejnými daty. Každá zmìna konfiguraèních dat se promítá do obou prostøedí. Vlastní zmìna konfiguraèních dat je okamžitá, bez ohledu na to, ze kterého prostøedí ji uskuteèníme. Na druhou stranu mùže nìjakou dobu trvat, než se zmìna dat uskuteènìná v DOSu "vizuálnì" promítne do systému Windows. Tato prodleva je zpùsobena charakterem systému Windows, který je víceúlohový a není možné zaruèit okamžik zpracování zprávy ze systému DOS do systému Windows (obecnì vzato žádné zprávy). Zmìna se "vizuálnì" projeví za nìkolik okamžikù i když vlastní zmìna dat a tím pádem i ochrana je provedena okamžitì pøímým zápisem do pamìti. Tuto vlastnost systému mùžeme nejlépe dokumentovat na použití "horké" klávesy v DOSu pro program Fguard. Pokud si spustíte DOS v oknì Windows a máte instalovaný program FGW.EXE, pak po stlaèení klávesy CTRL-5 (pøesný význam naleznete v popisu programu Fguard) uslyšíte zvukové znamení pøepnutí aktivity programu a po kratším nebo delším èasovém okamžiku (dle využívání systému a poètu spuštìných programù) uvidíte, že ikona programu FGW nebo obsah rozvinutého okna se automaticky zmìní. Tato zmìna však není z výše uvedených dùvodù okamžitá.

Verze 7.70

Program ve své verzi 7.70 obsahuje pouze minimální zmìny proti verzi 7.50.

Verze 7.50

Program ve své verzi 7.50 obsahuje pouze minimální zmìny proti verzi 7.0.

Verze 7.0

Program ve své verzi 7.0 je již trvalou souèástí antivirového systému AVAST!. Verze 7.0 pøináší mírné rozšíøení uživatelského rozhraní a nìkolik interních zmìn, které zlepšují stabilitu programu v mezních podmínkách.

Zmìny proti starším verzím.

Zmìny verze 7.0 proti verzi 6.2
Ve verzi 7.0 byla instalována schopnost ukrýt ikonu programu tak, že nemusí být po dobu èinnosti systému Windows viditelná.

Všechny ostatní zmìny programu se týkají pouze interních èástí, které nejsou viditelné pro uživatele.

Zmìny verze 6.2 proti verzi 6.0.
Ve verzi 6.2 byla plnì implementována spolupráce programu Fguard pro Windows s programem Rguard pro DOS - implementace testování spouštìných programù na pøítomnost virù. V návaznosti na tuto zmìnu program rozeznává dva parametry pøíkazové øádky:

/SB	Program 'zasekne' poèítaè v pøípadì zjištìní BOOT viru na disketì.
/SE	Program 'zasekne' poèítaè v pøípadì zjištìní viru ve spouštìném programu.

Nová verze má nepatrnì zmìnìno uživatelské rozhraní a pøi zobrazování varování upozoròuje na skuteènost, že odpovìï je nevyhnutelné zadat z klávesnice.

Zmìny verze 6.0 proti verzi 5.1.
Ve verzi 6.0 byla zmìnìna práce s jazykovou mutací èeštiny. Program je schopen automaticky nastavovat potøebnou jazykovou mutaci. Toto zjiš□ování spoèívá v testování promìnné **sCountry** z oblasti **[intl]** souboru WIN.INI. Pokud promìnná obsahuje øetìzec 'CZECH' nebo 'Èesk' psaný libovolnou kombinací velkých a malých písmen, program používá kódovou stránku 1250. Pokud promìnná tento øetìzec neobsahuje, program automaticky konvertuje všechny potøebná data z kódové stránky 1250 do èeštiny bez diakritiky. Pro tuto konverzi se používá dynamická knihovna AWLANG.DLL, která je souèástí dodávky systému AVAST! pro èeské zákazníky.

Byl zmìnìn tvar okna pro varování, které již neobsahuje tlaèítka. Tato zmìna byla provedena, protože program není schopen z principiálních dùvodù konstrukce systému Windows používat myš na odpovìï ve varovném oknì.

Hlášené REPORT není nadále vypisováno pøímo do plochy hlavního okna, ale do samostatného okna, které již nadále nepøepisuje obsah obrazovky. Toto okno je umístìno v pravém horním rohu vždy nad všemi aktivníma aplikacemi.

Program FGW.EXE rozeznává jeden parametr pøíkazové øádky, který mùže být psán libovolnou kombinací velkých a malých písmen. Parametr musí být uveden znakem '/' nebo '-'. Rozeznávaný parametr je:

/SB	Program 'zasekne' poèítaè v pøípadì zjištìní BOOT viru na disketì.

Zmìny verze 5.1 proti verzi 5.0.
Ve verzi 5.1 je program urèen jenom pro práci v tzv. rozšíøeném režimu práce Windows. Toto omezení však není tak svazující, jak se mùže na první pohled zdát. Systém Windows lze sice používat i na poèítaèích s procesorem 80286 a pamìtí 1 MB, ale vlastní práce s

podobným hardwarem pøipomíná spíše pomalou demonstraci než cokoli jiného. Druhým dùvodem omezení je to, že systém Windows pracující ve standardním režimu není schopen komunikace s DOSem a naopak. Tento režim pøipomíná (a ve své podstatì je) pouhý pøepínaè mezi DOSem a systémem Windows. Toto tvrzeni samozøejmì neplatí o provozování úloh Windows, ale pouze o spolupráci úloh DOSu a Windows. V rozšíøeném režimu práce je již možné zajistit plnohodnotnou a spolehlivou ochranu systému pøed napadením nebo vlastní nepozorností uživatele bez ohledu na poèet a typ úloh, které jsou právì zpracovávány.

Program FGW se ve verzi 5.10 skládá ze dvou hlavních èástí, souborù AVAST.386 a FGW.EXE. První z nich, tzv. virtuální driver, je 32 bitová knihovna, která obsahuje kritické èásti programu nutné pro spolupráci systému DOS a Windows. Tvoøí spojovací èlánek mezi rezidentními programy Fguard a Rguard z DOSu a programem FGW.

Druhý ze souborù je program FGW.EXE, což je standardní aplikace pro systém Windows, která obsluhuje komunikaci programu s uživatelem. Má za úkol zobrazovat aktuální nastavení ochrany a vypisovat varovná hlášení ve tvaru, který je pro Windows standardem.

Pùvod programu

Program Fguard pro Windows je souèástí systému AVAST! již od verze 5.0. S vývojem antivirového systému se také vyvíjel a nyní již poskytuje stabilní ochranu systému pøed viry i uživatelem.

Program se vyvinul z programù Fguard a Rguard pro DOS, které prozatím stále pro svou práci potøebuje.

Parametry programu

Program Fguard pro Windows rozeznává dva parametry pøíkazové øádky, parametry uvedené v konfiguraèním souboru AVAST!.INI a parametry, které si pøeète z rezidentních programù v DOSu.

Jednotlivé parametry:

- Parametry pøíkazové øádky
- Parametry konfiguraèního souboru
- Parametry rezidentních programù

Parametry pøíkazové øádky

Program Fguard pro Windows rozeznává dva parametry, které mohou být udávány na pøíkazové øádce. Parametry mohou být uvedeny znaky '**/**' nebo '**-**' a mohou být uvedeny velkými nebo malými písmeny.

Jednotlivé parametry jsou:

/SB Program 'zasekne' poèítaè v pøípadì zjištìní BOOT viru na disketì.
/SE Program 'zasekne' poèítaè v pøípadì zjištìní viru ve spouštìném programu.

Zaseknutí spoèívá v zablokování jakékoli další práce systému, ale obrazovka Windows zùstane nezmìnìna, takže správce systému se mùže pokusit identifikovat nakažený program nebo disketu. Pokraèování v práci je možné až po RESETu poèítaèe.

Parametry konfiguraèního souboru

Program Fguard pro Windows pro ukládání parametrù v dobì mezi jednotlivými spuštìními programu používá soubor AVAST!.INI, který je umístìn v adresáøi, odkud byl program spuštìn.

Všechny parametry programu Fguard pro Windows jsou uloženy v skupinì [FGUARD]. Soubor AVAST!.INI používají i další programy systému AVAST.

Promìnná TEMP
Promìnná TEMP slouží pro úèely komunikace jednotlivých instancí programu Fguard pro Windows. Její hodnota se mezi jednotlivými bìhy programu mìní. Je dùležité, aby se obsah promìnné bìhem práce programu Fguard pro Windows nezmìnil jiným programem, jinak mùže dojít k zablokování poèítaèe.

Promìnná HideIcon
Promìnná HideIcon obsahuje logickou hodnotu 0 nebo 1. V pøípadì, že promìnná obsahuje hodnotu 1, bude ikona programu po dobu jeho bìhu skrytá a program nebude zobrazován ani v seznamu pracujících úloh (standardním Seznamu úloh).

Parametry rezidentních programù

Program Fguard pro Windows pøi svém startu zjiš□uje pøítomnost a nastavení programù Fguard pro DOS a Rguard pro DOS. Jejich nastavení si èete pøímo z jejich interních dat, kam zapisuje také veškeré zmìny.

V pøípadì, že nìkterý program není zaveden do pamìti, jsou pøíslušné ovládací prvky nepøístupné. Popis jednotlivých parametrù mùžete najít v pøíslušných kapitolách.

Ovládání programu

Z hlediska ovládání má program dvì zcela samostatné èásti. Konfiguraèní okno programu, ve kterém je možné nastavovat konfiguraci a okno varování, které se zobrazí v závislosti na provádìných operacích a nastavené konfiguraci.

Program je možno ovládat pomocí klávesnice nebo pomocí myši stejným zpùsobem, jako všechny ostatní programy systému Windows. V programu je pouze jedna výjimka a tou je okno varování, které není možno ovládat myší.

Ovládání jednotlivých èástí programu

- Konfiguraèní okno
- Okno varování
- Report okno

Konfiguraèní okno

Konfiguraèní okno programu Fguard pro Windows je hlavní a jediné okno, které pracuje standardním zpùsobem oken systému Windows. Je to dialogové okno, které obsahuje nìkolik skupin ovládacích prvkù rùzných typù a rùzného urèení. Ovládací prvky jsou od rozdìleny do tøí skupin podle svého urèení tøírozmìrným efektem. Vrchní èást je urèena pro obsluhu programu Rguard a spodní pro obsluhu programu Fguard. Na kraji okna je umístìna skupina tlaèítek pro spoleèné použití. Podle konfigurace Vašeho systému, nemusí být všechny ovládací prvky aktivní.

Jednotlivé ovládací prvky:

- Ovládání programu Rguard
- Ovládání programu Fguard
- Spoleèné ovládací prvky

Okno varování

Okno varování má pro každé varování rozdílný obsah, který dostateènì výstižnì vyjadøuje pøíèinu jeho zobrazení i zpùsob odpovìdi nebo jiné reakce. Jeho ovládání je velice jednoduché. Je možné použít jenom kláves, které jsou v oknì uvedeny nebo klávesy Enter (Return), která má stejný úèinek jako první ze zobrazených voleb.

Report okno

Report okno je velice jednoduché okno, které se zobrazuje na dobu asi 10 vteøin v pravém horním rohu obrazovky. Okno zobrazuje krátký text, který vyjadøuje pøíèinu jeho zobrazení. Okno je naprosto samostatné a nemá žádný vliv na ostatní okna Windows. Ono je zobrazeno nad všemi ostatními okny a není s ním možno pohybovat.

Ovládání programu Rguard

Práce programu Rguard je ovlivòována dvìma parametry v horní èásti konfiguraèního okna.

Testuj BOOT sektor disket
Parametr urèuje, zda bude BOOT sektor každé diskety otestován na viry pøi pøístupu na disketu. V pøípadì, že BOOT sektor diskety obsahuje virus, je zobrazeno varování a v práci je možné pokraèovat nebo pøístup na disketu nepovolit.

Testuj spouštìné programy
Parametr urèuje, zda budou všechny spouštìné programy testovány na pøítomnost virù. Pokud je vzorek viru ve spouštìném programu nalezen, je možné zakázat spuštìní programu. Spouštìné programy jsou testovány jako jeden celek ve tvaru, v jakém se nacházejí na disku. Z toho vyplývá, že test mùže nìjakou dobu trvat, zvláštì pøi programech s délkou nad 1 MB (QPro 5.0, MS Word, ...) na poèítaèích s malou vyrovnávací pamìtí procesoru a nízkou frekvencí. Dle velikosti programu je nutné poèítat až s prodlevou 30 vteøin.

Ovládání programu Fguard

Práce programu Fguard je ovlivòována parametry uvedenými ve spodní èásti konfiguraèního okna.

Pokud je nìkterý parametr oznaèen šedivým ètvercem, program sleduje pokusy uvedenou èinnost, ale uživatele o jejím prùbìhu pouze informuje pomocí REPORT okna.

Program je aktivní
Parametr urèuje, zda budou nebo nebudou sledovány všechny èinnosti programu Fguard. Pokud není parametr oznaèen, program Fguard je vypnut.

Pokus o formátování stopy
Parametr urèuje, zda program sleduje nebo nesleduje pokusy o formátování nìkterého z pøístupných diskù nebo disket.

Manipulace se soubory
Parametr urèuje, zda program sleduje nebo nesleduje pokusy o otevírání souborù, jejich mazání a další podobné èinnosti s celými soubory.

Pøímý zápis pomocí DOSu
Parametr urèuje, zda program sleduje nebo nesleduje pokusy o pøímý zápis na pevné disky nebo diskety DOSem (pøerušení 25h), který obchází standardní metody ukládání dat.

Pøímý zápis pomocí BIOSu
Parametr urèuje, zda program sleduje nebo nesleduje pokusy o pøímý zápis na pevné disky nebo diskety BIOSem (pøerušení 13h), který obchází standardní metody ukládání dat. Protože i legální zápisy jsou ve své koneèné podobì transformovány na zápis pomocí BIOSu, použití tohoto pøepínaèe mùže vést k záplavì varovných hlášení. Doporuèujeme Vám tento pøepínaè aktivovat až v pøípadì podezøení na nákazu virem.

Zmìna obsahu CMOS pamìti
Parametr urèuje, zda program periodicky sleduje nebo nesleduje zmìny obsahu konfiguraèní pamìti CMOS. Nìkteré programy nebo systémy pravidelnì mìní její obsah. V tìchto pøípadech je sledování zmìn prakticky neproveditelné. Tìchto programù nebo systémù je však minimum.

Zmìna vektorù pøerušení
Parametr urèuje, zda program periodicky sleduje nebo nesleduje pokusy o zmìny vybraných vektorù pøerušení, což je jedna ze standardních èinností mnoha virù, ale i mnoha programù. Tomuto hlášení je vhodné vìnovat zvýšenou pozornost.

Krokování pøerušení
Parametr urèuje, zda program sleduje nebo nesleduje pokusy o krokování (tunelování) pøerušení, což je jedna ze obvyklých èinností moderních virù. Pravdìpodobnost, že by normální program vykonával tuto èinnost je velice malá a proto hlášení o pokusu o krokování pøerušení vìnujte maximální pozornost.

Editaèní okna
Editaèní okna obsahují až 10 rùzných typù souborù, které mùže program Fguard pro Windows sledovat. Pokud potøebujete pracovat s více typy souborù mùžete použít standardních znakù systému DOS pro urèení více typù jedním øetìzcem (tzv. wildchars). Typ

souboru je urèen øetìzcem maximálnì tøí znakù.

Spoleèné ovládací prvky

Spoleèné ovládací prvky slouží pro práci se samotným programem Fguard pro Windows. Tyto prvky nejsou uzavøeny v žádném grafickém prvku.

Skrýt ikonu programu
Parametr urèuje, zda bude ikona programu viditelná nebo ne.

OK
Tlaèítko OK slouží pro uložení zmìnìných informací do pamìti rezidentních programù instalovaných v systému DOS a jejich okamžitou aktivaci. Po jeho stisku se okno programu zmenší do tvaru ikony.

Zruš
Tlaèítko Zruš slouží pro zrušení zmìn všech parametrù zmìnìných od posledního stisku tlaèítka OK. Po jeho stisku se okno programu zmenší do tvaru ikony.

Nápovìda
Tlaèítko Nápovìda slouží pro vyvolání této nápovìdy na stránce Konfiguraèní okno.

Report
Tlaèítko Report slouží pro pøepnutí všech parametrù do režimu REPORT a zpìt. Obìma smìry jsou pøepnuta všechna tlaèítka, která mají tøi stavy.

Likvidace virù

Podle mnoha prùzkumù se již milióny uživatelù výpoèetní techniky po celém svìtì setkali s viry, a tak je bohužel vysoká pravdìpodobnost, že pøes veškerá preventivní opatøení se to mùže jednou pøihodit i Vám.

Nejdùležitìjší v takovém okamžiku je nepropadnout panice a zachovat klid. Jelikož jste jistì uživatel, který nerad riskuje, máte jistì všechna dùležitá data a programy zálohovány, takže ani kompletní znièení obsahu Vašeho disku by Vás jistì pøíliš nezaskoèilo. Navíc jste jistì uživatel pozorný a peèlivý, takže pøítomnost viru jste odhalil pomìrnì vèas, tedy døíve, než mohl napáchat velké škody. Odhalit virus mùžete napøíklad pozorováním neobvyklého chování systému (grafické a zvukové efekty, neobvyklé chybové hlášení, neznámá aktivita disku, chyby dosud bezvadnì fungujících programù apod.) nebo pomocí pravidelného a peèlivého používání antivirového systému AVAST!.

Pokud tedy zjistíte nesrovnalosti, které nelze nìjakým racionálním zpùsobem vysvìtlit (zmìna délky nebo obsahu souboru, nepovolená manipulace se soubory, podivné diskové operace, zmìny v operaèní pamìti atd.), je tøeba nejprve pomocí programu Lguard a Vguard zjistit, zda v systému není pøítomen nìkterý ze známých virù, které umí tyto programy odhalit. Program Lguard by si mìl poradit s naprostou vìtšinou dnešních virù. Pokud ani jeden z tìchto programù virus nenalezne, použijte program Aguard, který je schopen zachytit všechny zmìny, ke kterým na disku došlo od jeho posledního spuštìní. Program Aguard obsahuje i možnost otestovat zmìnìné soubory na pøítomnost virù a pøípadnì tyto viry ze souborù odstranit. Pøi jejich odstraòování nepotøebuje žádné informace o typu virù a tak je velice úèinný i proti novým nebo neznámým typùm.

Pøi likvidaci napadení vložte do disketové jednotky poèítaèe pracovní disketu, vytvoøenou pøi instalaci systému AVAST!, která by mìla být chránìna proti zápisu a spus□te program Lguard, napøíklad:

A:
LGUARD C:

Program Lguard nejdøíve prohledává operaèní pamì□, zda v ní nenajde aktivní virus. Pokud je nìjaký virus nalezen, je potøeba ho v pamìti eliminovat, aby pøestal být funkèní. Poté co byl z pamìti virus odstranìn, nehrozí nebezpeèí jeho další aktivity. Dále program testuje systémovou oblast disku a následuje testování souborù. Na závìr program vypíše pøehlednou tabulku s výsledky své èinnosti.

Pro odstranìní neznámého typu viru je potøeba nahrát systém z **èisté** systémové diskety (nejlépe z té, která byla vytvoøena pøi instalaci programového vybavení AVAST!). Programem Aguard snadno odhalíte všechny soubory, které byly virem nelegálnì modifikovány. Jejich seznam lze vytisknout na tiskárnì pøíkazem Print Screen nebo vytvoøit na disku pomocí parametru "**/O**".

Programy antivirového souboru AVAST! obsahují vlastní mechanismus, který umožòuje zjistit jejich pøípadnou modifikaci virem. Pøi svém spuštìní nejdøíve testují, zda nebyly samy zmìnìny, a pokud ano, ohlásí tuto skuteènost uživateli, napø.:

VGUARD.EXE
WARNING: This program was modified (maybe by some virus ??) !!

Press any key to continue...

Toto hlášení slouží jako upozornìní, že program byl modifikován. Jeho hlavní význam tkví v tom, ze uživatel je vèas varován. Po stisknuti kterékoli klávesy program pokraèuje ve své normální èinnosti, je však pravdìpodobné, že v tomto okamžiku byl již virus aktivován.

Pøi napadení systémových oblastí pevných diskù je možné v pøípadì používání operaèního systému MS-DOS 5.0 a vyšších použít systémový program FDISK s parametrem "**/MBR**", který obnoví standardní stav systémových oblastí bez vlivu na data, která mohou být na disku uložena. Nevyhnutelnou podmínkou pro použití je nastartování poèítaèe z èisté systémové diskety, jinak je léèba neúèinná.

Pro ochranu BOOT sektoru je možné výhodnì použít program Bguard, kterým je možno obnovit stav BOOT sektorù pevných diskù.

Pøejeme Vám, aby se Vám poèítaèové viry zdaleka vyhnuly. A pokud se pøece jen objeví, aby Vám naše programové vybavení pomohlo pøekonat všechny problémy, které Vám poèítaèové viry zpùsobily.

Pokud si nejste jisti, svìøte odstranìní virù odborníkùm !!

Požadavky pro práci

Program Fguard pro Windows potøebuje pro svou práci:

- Windows 3.1 nebo novìjší 16-ti bitový systém (Windows 3.11, Windows for Workgroups 3.1, 3.11) pracující v rozšíøeném režimu.
- VGA video adaptér nebo lepší.
- Disketová jednotka pro instalaci systému.
- Pevný disk pro uložení programù.

Chyby a fatální chyby

Program Fguard pro Windows je schopen zobrazit nìkolik rùzných druhù varování a chybových hlášení, která zobrazuje v rùzné formì. Jejich seznam a bližší informace o možných variantách jsou uvedeny níže.

- Nekompatibilita verzí.
- Program není instalován.
- Interní chyba DPMI.
- Interní chyba pøi zmìnì dat.
- Chyba inicializace programu.
- Chyba pøi vytváøení REPORT okna.
- Chyba alokace pamìti.
- Spouštìné programy nebudou testovány.
-
- Chyba detekce rozšíøeného módu.

Nekompatibilita verzí. Program není schopen pracovat z dùvodu nekompatibility s podpùrnou knihovnou (AVAST.386).
Soubor FGW.EXE a AVAST.386 musí mít stejnou verzi. Tyto dva soubory spolu velice úzce spolupracují proto není možné použít rùzné kombinace pro práci.

Program není instalován. V pamìti poèítaèe není FGUARD nebo RGUARD pro DOS nebo programy FGUARD nebo RGUARD a FGW nejsou vzájemnì kompatibilní.
Program Fguard pro Windows nevykonává žádné sledování èinnosti programù nebo uživatele ve své vlastní režii. V souèasné verzi pouze zobrazuje informace pøedané rezidentními programy z DOSu. V pøípadì, že tyto programy nejsou instalovány nebo nemají stejnou verzi, nemùže Fguard pro Windows pracovat.

Interní chyba DPMI. Nemohu alokovat struktury nutné pro pøístup k datùm. Program není schopen pracovat. Doporuèuji ukonèit práci ve Windows.
Program Fguard pro Windows používá k nìkterým operacím prostøedkù DPMI. Pokud dojde k chybì pøi práci s tímto rozhraním, jde s nejvìtší pravdìpodobností o vážnou chybu.

Interní chyba pøi zmìnì dat. Zobrazovaná data neodpovídají datùm, které jsou brány do úvahy pøi chránìní systému.
Program zjistil chybu pøi ukládání zmìnìných konfiguraèních dat do datových oblastí rezidentních programù. Pøi této chybì mùže dojít k pøepsání èásti pamìti a èinnost systému mùže být nestabilní.

Chyba inicializace programu. Není volný žádný èasovaè, který je nutný pro práci. Ukonèete nìkterý program a zkuste znova.
Program Fguard pro Windows potøebuje pro svou práci jeden kanál pro získávaní informací o zmìnì èasu. Protože jde o zdroj, který je v 16-ti bitových Windows limitován, nemusí být pokaždé k dispozici.

Chyba pøi vytváøení REPORT okna. Hlášení nebude zobrazeno.
Pøi vytváøení REPORT okna došlo k jakékoli chybì. Protože REPORT okno slouží jenom pro informaci uživatele, tato chyba není pøíliš závažná.

Chyba alokace pamìti. Nemohu alokovat pamì DOSu. Sledování spuštìných programù je vypnuto.
Sledování spouštìných programù vyžaduje pamì umístìnou na adrese pod 1 MB (tzv. pamì DOSu). Tato pamì je v 16-ti bitových Windows velice intenzívnì používaná a její množství je limitováno, takže nemusí být pokaždé k dispozici.

Spouštìné programy nebudou testovány. Knihovna pro jejich testování (AWANTI.386) není instalována.
Knihovna AWANTI.386 implementuje vlastní podprogramy pro testování dat. Její instalace probíhá pøi zavádìní systému Windows a nemusí pokaždé probìhnout. Napøíklad v pøípadì nedostatku pamìti nebude tato knihovna instalována.

Chyba detekce rozšíøeného módu. Program není schopen pracovat v jiném módu. Ukonèete Windows a použijte pøíkaz 'WIN /3'.
Program Fguard pro Windows pracuje pouze v rozšíøeném režimu systému Windows.

Konfiguraèní soubor je soubor, ve kterém se uchovávají parametry programu v dobì, kdy je poèítaè vypnut nebo kdy program nepracuje. Konfiguraèní soubor pro programy systému AVAST! se nazývá AVAST!.INI a mùžete ho najít v adresáøi, odkud byl program spuštìn. Je to standardní typ konfiguraèního souboru pro programy urèené do systému Windows. Pøed manuálními zmìnami obsahu tohoto souboru doporuèujeme poøídit si jeho zálohu, protože nesprávnì provedené zmìny mohou zpùsobit nefunkènost antivirového systému AVAST! nebo zablokování systému.

FGUARD je rezidentní antivirový program pro DOS, který v reálném èase hlídá všechny pokusy o modifikaci sledovaných souborù (smazání, otevøení pro zápis, zápis, pøejmenování, zrušení pøíznaku "pouze ètení"). Kromì toho je program schopen sledovat i pøípadnou destruktivní èinnost viru. Umožòuje hlídat pokusy o formátování, pøímí zápis na disk pomocí DOSu èi BIOSu, zmìnu obsahu konfiguraèní pamìti CMOS, krokování pøerušení a zmìny vybraných vektorù pøerušení.

Firma ALWIL Software a její programové produkty nejsou na trhu žádným nováèkem. Firma samotná byla založena až v dubnu 1991 oddìlením od družstva ALWIL, ale kolektiv jejich pracovníkù je pospolu již od roku 1988, kdy vznikla první verze souboru antivirových programù AVAST! a Správce uživatelských programù SUP. V tomtéž roce byla na trh uvedena implementace národního prostøedí nejen pro osobní poèítaèe kompatibilní s IBM PC a jeho obvyklé periférie, ale i pro laserové tiskárny.

Zùstáváme i nadále vìrni své specializaci v oblasti systémových programù, ochrany dat a implementaci národního prostøedí pro laserové tiskárny. Poslední novinky z naší produkce jsou napøíklad šifrování obsahu pevných diskù v reálném èase nebo program Lguard pro Windows.

ALWIL Software
Prùbežná 76, 100 31 Praha 10
telefon (+422)782 20 50

fax (+42 2)782 25 53
BBS (+42 2)782 25 50
BBS (+42 2)782 20 50 (18:00 - 7:00)
cc:Mail (+42 2)782 2549

RGUARD je jeden z rezidentních antivirových programù pro DOS, který zajiš uje antivirové testování spouštìných programù a testování pøítomnosti BOOT virù na disketách v prostøedí DOSu.