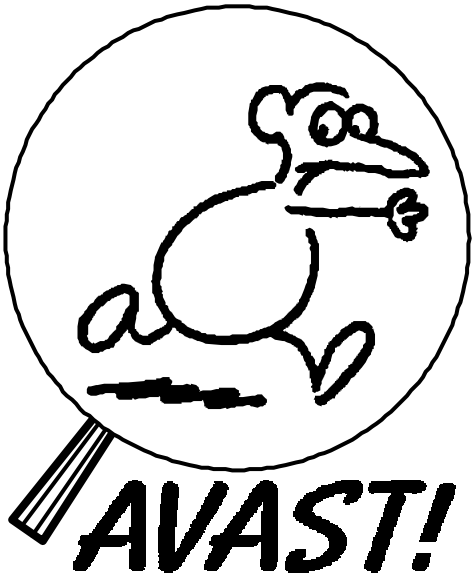
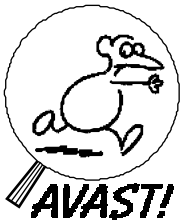


Soubor antivirových programů pro MS–DOS a Windows 3.x verze 7.7

ALWIL SOFTWARE

Grafická úprava a sazba Eda Kučera, ALWIL Software
Dokumentace byla zpracována program Adobe PageMaker 6
Elektronická forma zpracována programy Adobe Acrobat Distiller a Exchange
Osvit: ...ARA
Tisk: Tiskárna Hugo

Obsah



Úvod

Blahopřejeme vám k zakoupení souboru antivirových programů AVAST!. Dostává se vám do rukou nová verze tohoto populárního programového vybavení, verze 7.7. V úvodu této dokumentace jsou popsány základní vlastnosti programového vybavení a konvence použité v této uživatelské příručce.

V dalších kapitolách budete seznámeni s instalací, funkcí a ovládáním jednotlivých programů a s vlastnostmi některých virů, se kterými se mohou uživatelé v České republice i na Slovensku nejčastěji setkat. Dozvíte se i to, jak se zachovat v případě, že zjistíte přítomnost počítačového viru ve vašem systému.

Přestože soubor antivirových programů AVAST! je důkladnou ochranou počítačového systému proti virům, přejeme vám, abyste se s žádným virem nesetkali. Pokud se tak stane, a naše programy si s daným konkrétním virem nebudou vědět rady, budeme vám vděčni za rychlou telefonickou nebo písemnou informaci. Díky vaší spolupráci můžeme kvalitu našeho programového vybavení dále zvyšovat.

Protože oblast počítačových virů je dnes nejdynamičtějším odvětvím ve světě počítačů vůbec, je důležité používat opravdu poslední verze antivirových produktů. Pro uživatele to znamená, že se musí často a sami o aktualizaci starat. Abychom našim zákazníkům tuto činnost usnadnili, již delší dobu jim poskytujeme antivirovou službu AVS. V rámci této služby dostávají po dobu jednoho roku automaticky nejnovější verze souboru AVAST!, mají zajištěnu technickou a poradenskou službu. Pro aktualizaci je možno využít i naši BBS. Tato služba je výhodná i po finanční stránce. Další informace o službě AVS vám na vyžádání rádi poskytneme.

Změny v AVAST! verze 7.7

Nejdůležitějšími změnami, které jsou obsaženy v nové verzi je detekce makrovirů založená na analýze OLE2 souborů, doplnění charakteristiky viru o příznak ITW, možnost

ovládání programu BGUARD z příkazové řádky a zpracování data a času v programu CHKAVAST. Samozřejmě jsme věnovali pozornost i detekci nových virů a odstranění drobných chyb, které se v poslední době vyskytly u uživatelů.

Po dlouhém váhání jsme opustili program VGUARD, který umožňoval přesně vyhledat a odstranit okolo dvaceti virů. Slovo přesně znamenalo, že v programu byla uložena o viru rozsáhlá informace a teprve na základě této přesné identifikace byl vir odstraněn. Tato koncepce je v současné době pro velikost potřebných souborů (existují tisíce různých virů) neudržovatelná, a proto také VGUARD nebyl v podstatě v poslední době aktualizován. Na druhou stranu mohlo uživatele mást, že AVAST obsahoval dvojici programů pro hledání známých virů, z nichž každý poskytoval jiné výsledky. Pro odstraňování virů lze použít obecnou obnovu souborů nabízenou programem pro kontrolu integrity dat AGUARD a pro odstranění makrovirů nových schopností programu LGUARD.

Změny programu LGUARD

- **Změnila se struktura datového souboru LGUARD.VPS, takže ten není kompatibilní s předchozí verzí.**
- Do vyhledávacích programů byla přidána korektní detekce makro virů včetně správné analýzy OLE2 souborů. Pro detekci makrovirů již není potřeba prohledávat celý soubor, program jej sám analyzuje, vyhledá makra, pokud jsou přítomna, a detekuje makroviry. Ty jsou detekovány dvojím způsobem – jednak přesnou identifikací konkrétního makroviru, založenou na kontrolním součtu maker viru, jednak pomocí vyhledávacích řetězců, které umožňují zjistit přítomnost i nových virů z dané rodiny makrovirů. DOSový program LGUARD umožňuje dokonce odstranění makro virů z dokumentu, které může být velmi užitečné, protože po odstranění maker je možno dokument bez problémů použít. Pro smazání maker je možno použít stejný parametr, jako pro smazání souborů napadených klasickým virem. Pokud je zjištěn makrovirus, program se ptá, zda se mají odstranit pouze makra daného viru (pouze při přesné identifikaci), všechna makra, či má li být smazán celý dokument. Podobný požadavek je možno specifikovat i na příkazovém řádku, pokud je za /Z

uvedeno M (jen Makra viru), V (Všechna makra) nebo S (celý Soubor). Program se pak zeptá pouze na to, zda má dané odstranění provést (Ano či Ne). To je možno využít i s parametrem /P pro plynulé odstranění. Pokud program pracuje plynule a je uvedeno pouze /Z, předpokládá se /ZM pro přesně identifikované viry a /ZV pro rodiny virů.
Pokud není žádný virus nalezen, zobrazuje program LGUARD informaci o tom, zda soubor obsahuje nějaká makra, zda je šablonou či dokumentem Word či zda se jedná o soubor OLE2.

- Program LGUARD má nyní rychlejší algoritmus pro testování virů.
- Program LGUARD zobrazuje při verifikaci a načítání databáze virů po vteřině údaj o množství již zpracovaných v procentech (je to zřejmé a užitečné zejména při spuštění programu z diskety).
- Program LGUARD umožňuje při výpisu jemu známých jmen virů (parametr /V) interakčně zadat více znaků ze jména viru. Přitom se posunuje v seznamu tak, že první virus podle abecedy, který zadaným znakům odpovídá, je na právě zobrazené straně. Zadávání je možno zrušit pomocí klávesy Escape.
- Program LGUARD nyní rozeznává zvláštní kategorii virů, které se volně šíří mezi uživateli (tj. jsou In the Wild, zkratka ITW). Údaj o tom, že virus je ITW se zobrazuje jak v seznamu virů (znakem W), tak i v případě nalezení viru speciálním upozorněním v popisu viru (klávesa F1). Ve výpisu virů jsou makroviry označeny písmenem M.
- Program LGUARD v celkovém souhrnu po výpisu virů zobrazuje dvě nové zvláštní kategorie: počet makrovirů a počet ITW virů.
- Program LGUARD umí rozpoznat v uživatelské definici virů makroviry (M) a viry, které jsou ITW (W).
- Program LGUARD pří výpisu seznamu známých druhů virů zvýrazňuje duplicitní jména virů, zadaných uživatelem (červeně a zvukem) a uživatelem zadané řetězce (žlutě)
- Program LGUARD má nyní vícestránkovou nápovědu (help).

Změny programu AGUARD

- Program AGUARD má při zobrazení zjištěných změn definovánu novou klávesu Ctrl–E pro vyhledání následujícího adresáře, který obsahuje nějaké změny. Popis všech definovaných kláves je možno zobrazit pomocí F1 v daném okně.
- Program AGUARD má nový parametr /X pro netestování systémové oblasti disku. To může být užitečné zejména pro testování integrity přenesených souborů elektronickou cestou na různých počítačích (typicky desktop a notebook).
- Program AGUARD má nyní vícestránkovou nápovědu (help).

Změny programu RGUARD

- Program RGUARD zobrazuje při výpisu boot virů W pro viry, které jsou ITW.
- Program RGUARD implicitně testuje přítomnost diskety v jednotce A, pokud je stisknuto Ctrl–Alt–Del a nepovolí restart počítače, pokud není disketa odstraněna. Tato funkce se dá vypnout pomocí parametru /R (je možno použít na počítačích bez disket, nebo pokud je zakázáno zavádění systému z diskety v setupu počítače.
- Pro test boot sektorů disket vyžaduje paměť XMS.

Změny programu BGUARD

Program BGUARD lze nyní ovládat i parametry příkazové řádky a o dalším postupu v dávce rozhodnout na základě návratového kódu. Parametry musí být zadány malými písmeny a používány velmi opatrně!!

BGUARD clean <disketa> <size>

BGUARD vytvoří nový boot sektor diskety. Parametr disketa může být A nebo B, parametr size určuje kapacitu diskety a může nabývat hodnot 360, 720, 1.2, 1.44, 2.88. Použití nesprávné velikosti bude mít za následek ztrátu dat!!!

BGUARD save <disketa> “popis”

Uloží systémové oblasti pevných disků na disketu. Popis může obsahovat údaje o daném počítači. Musí být v uvozovkách!

BGUARD restore <disketa>

Obnoví systémové oblasti pevných disků z údajů uložených na disketě.

BGUARD compare <disketa>

Porovná systémové oblasti pevných disků se stavem uloženým na disketě

Pokud jsou tyto parametry použity, není na obrazovce nic zobrazeno a veškerý výstup je realizován pouze pomocí návratového kódu. Definované hodnoty návratového kódu jsou:

1 data obnovena,
2 data uložena,
3 nic neprovedeno,
4 chyba při práci s disketou,
5 chyba při práci s pevným diskem,
6 porovnání je v pořádku,
7 porovnání není v pořádku,
99 zobrazena nápověda

Změny programu CHKAVAST

Program CHKAVAST má řadu nových parametrů pro zpracování informace o času a datu.

CHKAVAST ISTIME hh:mm

Slouží pro zjišťování času; vrací návratový kód 1, pokud je systémový čas vyšší než čas zadaný a 0, pokud je nižší nebo stejný.

CHKAVAST ISDAY [NEW] [OLD] [<den>] [<datum>]

Slouží ke zjištění údajů o nastaveném systémovém datu a dnu a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný den, parametr OLD má opačný význam.

Kromě těchto parametrů je možno použít i anglickou zkratku dne v týdnu a nebo datum, zadané pomocí dvou dvouciferných čísel, udávajících den a měsíc. Pokud je některé

z těchto čísel nulové, jedná se o libovolnou hodnotu (00–08 znamená celý srpen, 15–00 je patnáctého v libovolném měsíci). Pro zadání data se bere v úvahu nastavení kódu země (tj. buď evropská nebo americká konvence zadání).

Jednotlivé parametry je možno kombinovat (například pro pátek třináctého), výsledek je správně pouze tehdy, jestliže jsou splněny všechny dílčí podmínky.

Příklad:

```
chkavast isday mon new
if errorlevel 1 goto label1
echo Na začátku týdne provedeme důkladné testy!!
lguard c:\*.* /s /e*
:label1
...
isday 13-00 fri
if errorlevel 1 goto label2
pause Dnes je pátek 13. Přeji vám hodně štěstí...
:label2
```

CHKAVAST ISMONTH [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém měsíci a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný měsíc, parametr OLD má opačný význam.

Příklad:

```
chkavast ismonth new
if errorlevel 1 goto label1
echo Dnes je třeba udělat záložní kopie!!
:label1
...
```

CHKAVAST ISWEEK [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém týdnu a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na

nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný týden, parametr OLD má opačný význam.

Příklad (stejná činnost jako u ISDAY ale spolehlivější, protože funguje i v případě svátků či pokud je počítač zapnut například až v úterý):

```
chkavast isweek new
if errorlevel 1 goto label1
echo Na začátku týdne provedeme důkladné testy!!
lguard c:\*.* /s /e*
:label1
...
```

CHKAVAST ISYEAR [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém roce a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný rok, parametr OLD má opačný význam.

Příklad:

```
isyear new
if errorlevel 1 goto label1
echo Hodně štěstí v novém roce!!
:label1
...
```

CHKAVAST pro svoji činnost používá soubor AVAST.DAT ve stejném adresáři pro ukládání dat, pokud je použit příkaz NEW či OLD. Parametry ISDAY, ISWEEK, ISMONTH a ISYEAR jsou na sobě nezávislé, tj. pokud například zapnete počítač v pondělí ráno, podmínky ISDAY NEW a ISWEEK new ve dvou po sobě následujících příkazech jsou obě splněny.

Typografická konvence

V této uživatelské příručce je mimo normálního textu vysázeného písmem Century Schoolbook použit i další druh písma, které slouží k odlišení předkládané informace:

```
FGUARD /H
```

Příklady jsou vysázeny písmem Courier, do počítače je možné je vkládat ve velkých i malých písmenech. Pokud je vytištěná příkazová řádka delší než jedna řádka textu, je další řádka odsazena a do počítače se vkládá bez nové řádky. Klávesou Enter se ukončí až celý příkaz.

```
SGUARD [/K] [/L] [/N] [/D] soubor1 suma1 [soubor2
  suma2 [...]]
```

Obecná specifikace spuštění programu je také vysázena písmem Courier. Objekty uzavřené mezi hranaté závorky jsou volitelné (není nutné je zadat), ostatní jsou povinné. [...] označuje další opakování předchozího objektu. Například:

```
SGUARD
```

je špatně (chybí povinné parametry soubor suma),

```
SGUARD IO.SYS 12345
```

je dobře (následuje soubor a suma),

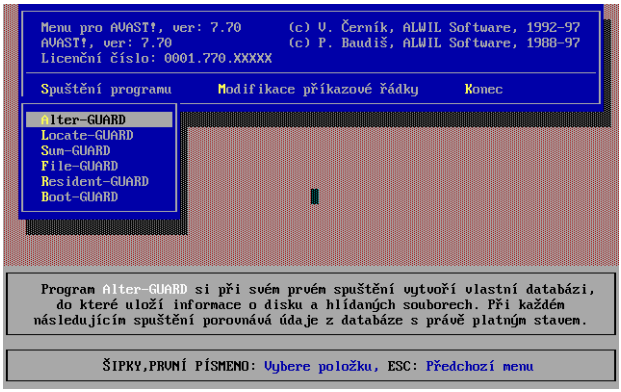
```
SGUARD /L IO.SYS 12345 COMMAND.COM 23456
```

je také dobře,

```
SGUARD /X IO.SYS 12345
```

je špatně (neznámý přepínač /X).

Obrazovky jsou v příručce ve formě obrázků, ať se jedná o programy pro MS–DOS nebo Windows. Např.:


Menu pro AVAST!, ver: 7.70
(c) V. Černík, ALWIL Software, 1992-97
AVAST!, ver: 7.70
(c) P. Baudiš, ALWIL Software, 1988-97
Licenční číslo: 0001.770.XXXXX
Spuštění programu
Modifikace příkazové řádky
Konec
Alter-GUARD
Locate-GUARD
Sum-GUARD
File-GUARD
Resident-GUARD
Boot-GUARD
Program Alter-GUARD si při svém prvém spuštění vytvoří vlastní databázi,
do které uloží informace o disku a hlídaných souborech. Při každém
následujícím spuštění porovnává údaje z databáze s právě platným stavem.
ŠIPKY,PRVNÍ PÍSMENO: Vybere položku, ESC: Předchozí menu


AVAST!

Tato stránka je úmyslně prázdná

Instalace programů AVAST!

Programové vybavení AVAST! je určeno pro osobní počítače kompatibilní s IBM PC, IBM PC/XT a IBM PC/AT s minimálně 256 KB operační paměti. Vyžaduje operační systém MS–DOS či PC–DOS verze 3.30 a vyšší, pracuje se všemi standardními adaptéry zobrazení (MDA, CGA, EGA, VGA, EGC, Hercules Graphics Card apod.).

Programové vybavení AVAST! je standardně dodáváno na distribučních disketách, které jsou chráněny proti zápisu. Pro správnou instalaci **nejdříve zaveďte systém z originální systémové diskety**, kterou jste dostali s počítačem. Pak vytvořte kopii distribuční diskety (popřípadě disket) následujícím příkazem (je nutno opakovat pro všechny diskety):

```
DISKCOPY A: A:
```

Napřed vložte do jednotky distribuční disketu (Source) a pak novou disketu (Target). Pak postupujte podle pokynů programu DISKCOPY. Po zkopírování originální distribuční diskety uschovejte a pro instalaci již použijte nově vytvořené kopie. Ty je **nutno opatřit ochranou proti zápisu** – pro pětačtvrtpalcové přelepením postranního otvoru, pro třiapůlpalcové otevřením okénka.

Instalace pro MS–DOS

Vlastní instalace je velmi jednoduchá. Je zajištěna pomocí zvláštního programu INSTALL, který se nachází na distribuční disketě. Tento program nejprve otestuje vaši disketovou jednotku, zda neumožňuje zápis na diskety, které jsou proti tomu chráněné, poté prověří, zda se na vašem počítači nenachází některý ze známých počítačových virů a nakonec zkopíruje všechny potřebné soubory do vámi zvoleného adresáře. Program se spouští následujícími příkazy:

```
A:
INSTALL
```

Po spuštění programu postupujte podle jednoduché nápovědy. Jak již bylo uvedeno, program INSTALL testuje, zda je možno na vaší disketové jednotce zapisovat na disketu, která je chráněna proti zápisu. Pokud by byla tato činnost možná, jedná se o poruchu disketové jednotky a je nutno ji nechat opravit. V naší praxi jsme se zatím setkali se třemi takovými případy, takže se nejedná o příliš častou poruchu. Může to však být z hlediska počítačových virů velmi nebezpečné! Kvůli tomuto testu musí být instalační diskety **chráněny proti zápisu**. Originální kopie jsou takto chráněny automaticky, pokud pracujete s vytvořenými kopiemi, musíte tuto ochranu zajistit sami.

AVAST! obsahuje i programy, které pracují v prostředí Windows. Pro jejich instalaci je nutno **v prostředí Windows** spustit program AVINST, který provede správnou instalaci.

Program INSTALL vytváří i modifikovanou inicializační příkazovou dávku (AUTOEXEC.BAT či START.BCH), která je uložena do souboru v hlavním adresáři disku C: a jmenuje se AVAST!.NEW. Pokud ji chcete používat, musíte tento soubor sami přejmenovat.

Kromě instalace na pevný disk je vhodné, aby si uživatel vytvořil speciální **„záchrannou“ disketu**, obsahující prostředky pro oživení systému v případě napadení virem. Pro vytvoření takové diskety doporučujeme následující postup:

1. Zaveďte systém z originální systémové diskety, kterou jste dostali s počítačem.
2. Připravte si předem systémovou disketu o kapacitě alespoň 720 KB příkazem FORMAT /S.
3. Spusťte z diskety program INSTALL a zadejte v prvním řádku disk, ve kterém je umístěna disketa a ve druhém řádku adresář, ve kterém je instalován soubor programů AVAST!. Zvolte položku „Vytvoření záchranné diskety“ a postupujte podle pokynů programu.
4. Záchrannou disketu opatřete ochranou proti zápisu, dobře ji označte a **vyzkoušejte, zda je funkční**!! Potom ji důkladně uschovejte. Později se vám může velmi hodit!

Instalace pro Windows

Instalační program AVINST.EXE je určen pro dokončení instalace systému AVAST! pro práci ve Windows. Jedná se o velice jednoduchý program, který má za úkol správně konfigurovat parametry Windows tak, aby uživatel mohl bez dlouhého otálení používat všechny antivirové programy, které jsou součástí produktu.

Druhou hlavní činností programu je možnost deinstalace produktu AVAST! tak, že po něm nezbudou v konfiguračních souborech Windows žádné stopy. Pokud se rozhodnete deinstalovat systém AVAST!, použijte rovněž program AVINST, který rozezná, kterou operaci požadujete.

Instalace systému AVAST! pro Windows neproběhne bohužel na některých počítačích bez problémů. Ty se týkají hlavně instalace programů SGW a FGW do startovací skupiny Windows. Pokud po proběhnutí programu AVINST nenajdete ve skupině StartUp nebo Spustit při startu tyto dva programy, zkopírujte je sem ručně z vytvořené skupiny AVAST!. Po ručním zkopírování programu SGW je nutno upravit jeho vlastnost tak, aby se ze startovací skupiny Windows spouštěl v minimalizovaném tvaru.

Jak, kdy a které programy použít?

Obecný antivirový program AGUARD je určen pro periodické spouštění při profylaxi systému. Je nesmírně důležité ho používat, protože tvoří velmi důležitou část ochrany proti virům. Je schopen obecně odstranit viry z napadených souborů, ale jen tehdy, pokud je pravidelně používán!! Stejným způsobem je možno používat i program AGUARD pro Windows – AGW.

Vyhledávací program LGUARD je potřeba spouštět vždy, když byly do systému přidány nové programy. Mimo to je lze spouštět periodicky pro ověření „čistoty“ osobního počítače. Program LGUARD s parametrem /M (pouze test paměti a zaváděcího sektoru) je vhodné spouštět při každém zavedení systému v příkazové dávce AUTOEXEC.BAT.

Kromě toho doporučujeme programem LGUARD periodicky testovat všechny diskety, které by mohly obsahovat viry (cizí

diskety a dále diskety, které byly používány na jiném počítači, v jiné organizaci apod.).

Program LGUARD pro Windows (LGW) může být zařazen do skupiny Startup a být tak spouštěn při každém startu programu Windows. Je schopen práce na pozadí, kdy periodicky testuje disky počítače a dokud nenalezne nějaký virus, uživatel jeho přítomnost ani nezaregistruje.

Paměťově rezidentní program RGUARD je určen pro testování zaváděcích sektorů vložených disket a případně k prověření všech spuštěných programů. Nezjistí sice o nic více než program LGUARD, ale přítomnost virů testuje průběžně, takže uživatelé nemusí na spouštění programu LGUARD myslet.

Obecné antivirové programy SGUARD a FGUARD by neměly v žádném případě chybět v souboru příkazové dávky AUTOEXEC.BAT, aby mohly v rámci prevence včas odhalit činnost virů.

Program SGUARD pro Windows (SGW) je vhodné zařadit do skupiny „Spustit_při startu“ (StartUp) a určit mu, které soubory má při každém spuštění Windows testovat (např. systémové soubory DOSu a důležité aplikace).

O programu BGUARD jsme si již řekli, že by měl být součástí „záchranné“ diskety, která by měla být vytvořena pro každý počítač. Kromě toho je vhodný pro odstraňování boot virů z infikovaných disket. Dá se využít i v rámci prevence pro ošetření všech datových disket.

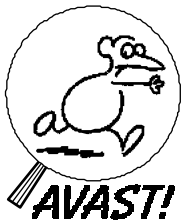
Správným používáním programového vybavení AVAST! můžete včas předejít napadení vašeho systému počítačovými viry, a tím zabránit velkým škodám, které vám mohou tyto viry způsobit!!

Upozornění pro uživatele starších verzí

Nová verze programu AGUARD neumožňuje spolupráci se staršími verzemi databáze AGUARD.DAT. Proto vám doporučujeme před instalací nové verze naposledy otestovat obsah souborů starým programem AGUARD a poté spustit novou verzi programu. Pokud tento nový program najde nekompatibilní databázi AGUARD.DAT, nabídne vám její smazání a poté vytvoří databázi novou. Program SGUARD může při

změně ze starší verze za určitých podmínek hlásit změnu v systémové oblasti disku. Je to způsobeno tím, že nyní se již netestuje 15 slabik, ve kterých je uložen Volume Label a sériové číslo (změna jména disku způsobila falešný poplach).

Program LGUARD je od verze 4.30 typu EXE. Proto je soubor LGUARD.COM (ze starších verzí) automaticky vymazán, pokud instalujete AVAST! programem INSTALL do stejného adresáře, ve kterém byla verze starší. Pokud soubory z distribuční diskety pouze zkopírujete (což nedoporučujeme!) či instalujete do jiného adresáře než byly, musíte původní soubor LGUARD.COM vymazat sami. Starší verze je možno jednoduše poznat jednak podle čísla verze, jednak podle toho, že neobsahují informace o verzi souboru VPS v pravé horní části obrazovky. Jeho smazání je nutné proto, že při spouštění programů má soubor s rozšířením COM přednost před rozšířením EXE.



Tato stránka je úmyslně prázdná

Problematika počítačových virů

V druhé polovině osmdesátých let se objevilo pro uživatele počítačů nové velké nebezpečí. Jsou jím počítačové viry. Od té doby se tato oblast vyvíjí nesmírně rychle a počet známých druhů virů a škody jimi způsobené se neustále zvyšují.

O počítačových virech existuje spousta mylných představ, například že se jedná o jistou formu života, že se viry vyznačují určitou umělou inteligencí, že se mohou přenést mezi počítači bez fyzického kontaktu, že mohou přežít v obvodech i při vypnutém proudu, v paměti CMOS a podobně.

Čím tedy počítačové viry skutečně jsou? Jedná se o programy, které mají schopnost napadat ostatní programy a zkopírovat do nich samy sebe, a to bez vědomí, přání či přímé akce uživatele. Napadené programy se tak stávají dalšími nosiči virů, čímž je umožněno jejich další šíření.

Jak se počítačové viry šíří? Viry mohou napadat jakýkoli kód, který je v počítači prováděn. V praxi to vypadá tak, že napadají tzv. systémovou oblast disku (sektor s tabulkou rozdělení disků či zaváděcí sektor) nebo soubory, ve kterých jsou uloženy programy.

Co mohou počítačové viry způsobit? Kromě modifikace programů při svém šíření (což již samo o sobě představuje velké nebezpečí při zásazích do fungujících programů) mohou počítačové viry způsobit i jiné velké škody. Viry zabírají místo v paměti, na disku, zpomalují počítač, mohou zničit, modifikovat či poškodit soubory nebo systémovou oblast disku, mohou zformátovat či přepsat disk nebo disketu, psát různé zprávy na obrazovku, předefinovat klávesnici a podobně. Mohou být vytvořeny a šířeny z legrace, ze zlomyslnosti, z pomsty nebo mohou sloužit k ničení programů a dat, k sabotáži, poškození konkurence atd. Obecně tak lze říci, že žádný virus není neškodný. Všechny narušují kód hostitelského programu a žádný z nich není do systému zván a vítán.

Ochrana proti počítačovým virům může být velmi problematická. Viry totiž mohou mít různou podobu a způsob činnosti. Jejich počet se v posledním období velmi rychle zvyšuje. Přesto existují metody, jak viry včas odhalit, a tak předejít nebezpečí, které z jejich strany hrozí. Takové odhalení může probíhat různými způsoby.

Pokud je již znám konkrétní virus, je možno proti jeho působení napsat jednoúčelově zaměřený program. Takový program je však samozřejmě zcela neúčinný proti jiným typům virů.

Dalším typem antivirových programů jsou tzv. vyhledávací programy (často nazývané programy typu „scan“). Tyto programy pracují bez podrobné znalosti konkrétního viru, pouze s určitou charakteristikou – například s určitou částí jeho kódu. Při spuštění pak prohledávají všechny specifikované soubory a testují, zda neobsahují danou sekvenci slabik. Pokud takovou sekvenci naleznou, může se jednat o virus. Samozřejmě záleží na tom, kolik sekvencí je takový program schopen nalézt. Problémem této skupiny programů je jednak počet nových virů a s tím související požadavek na častou aktualizaci, jednak i trend posledních let – tzv. polymorfní viry, které jsou v každé své kopii jiné a u kterých není možno jednoduchým způsobem vybrat charakteristický vzorek.

Velkým přínosem mohou být obecné antivirové programy, které působí i proti dosud neznámým druhům počítačových virů. Takovým programem může být například program, který uchovává zhuštěnou informaci o ostatních souborech a je schopen zjistit veškeré změny, které v těchto souborech nastaly, popřípadě i obnovit původní stav. Dalším příkladem je program, který v reálném čase kontroluje pokusy o zápis a modifikaci uživatelských programů a pro provedení nebezpečné činnosti vyžaduje souhlas uživatele.

Nejdůležitějším způsobem ochrany proti počítačovým virům zůstává jednoznačně prevence. Nelze samozřejmě zaručit, že bude mít stoprocentní účinnost, ale i zde, stejně jako v jiných oborech platí, že největší problémy má ten, kdo je na hrozící nebezpečí nejméně připraven. Prevence spočívá v důsledném dodržování následujících pravidel:

– nespouštějte programy s nejasným původem,

- diskety zabezpečujte proti přepsání, originální diskety před instalací programu opatřete nálepkou proti přepisu, zkopírujte, uložte na bezpečné místo a pokud možno vícekrát nepoužívejte,
- diskety zanechávejte v jednotce jen po nezbytně nutnou dobu, po ukončení práce s disketou ji okamžitě vyjměte; pokud na ní nechcete zapisovat, opatřete ji ochranou proti zápisu,
- přehodnoťte svůj postoj k nelegálně získanému programovému vybavení; jeho cesta od výrobce až k vám mohla být dosti trnitá (jeho použití je navíc nezákonné),
- často a pravidelně zálohujte data (to se může vyplatit, i když žádné viry nablízku nejsou),
- používejte veškeré dostupné prostředky pro antivirovou prevenci (obecné i jednoúčelově zaměřené programy),
- nepouštějte ke svému počítači cizí osoby, případně používejte prostředky pro řízený přístup k PC (např. SUP).

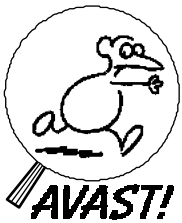
Každá bariéra, umístěná do cesty počítačovému viru, snižuje jeho šanci na infikování chráněných systémů!

Počítačové viry se objevily v roce 1988 i v Československu. Jejich šíření bylo od počátku podporováno širokým nasazením osobních počítačů, u kterých dochází k velké výměně programového vybavení a používání počítačů lidmi, kteří si často hrozící rizika a příznaky nebezpečí vůbec neuvědomují. Občas k tomu přispívá i distribuce programového vybavení od nerenomovaných dovozců, kteří se snaží zvýšit zisk nákupem programového vybavení od neautorizovaných překupníků, a dále i rozsáhlé šíření nelegálně získaného programového vybavení.

Soubor antivirových programů AVAST! byl prvním obecným souborem takových programů, který byl v Československu k dispozici. Od té doby jej neustále vyvíjíme podle nejnovějších poznatků v této velice dynamické oblasti. Přitom spolupracujeme s řadou zahraničních odborníků. Poslední verze tohoto souboru obsahuje řadu samostatných antivirových programů, proto je jako celek velmi komplexní.

Nejoblíbenějšími jsou vyhledávací programy pro MS–DOS i Windows, které jsou schopny (díky pravidlené aktualizaci) nalézt prakticky všechny viry, které se mezi uživateli vyskytnou. Další je paměťově rezidentní program se stejnou

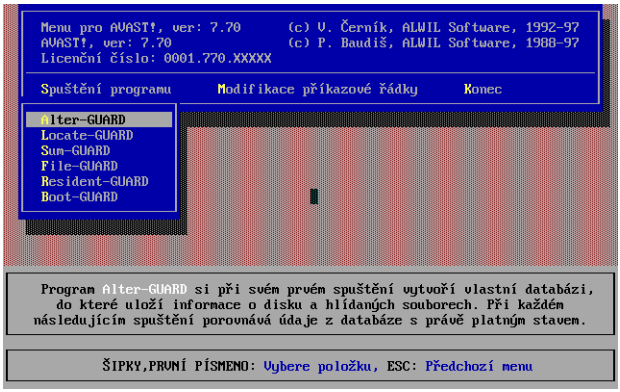
funkcí. Následují čtyři programy, které jsou obecné, takže je lze použít i proti dosud neznámým druhům počítačových virů. Obecné programy nemusí mít stoprocentní účinnost za všech okolností, přesto však mohou při správném používání většinu virů zjistit, a tak umožnit včas předejít obrovským škodám. Navíc jsou důležité i z metodického hlediska, protože svým okruhem působnosti ukazují možnosti, kterými je možno se proti virům bránit a zabezpečit. Vyhledávací programy ani obecné programy neznají strukturu viru, proto nemohou žádný virus odstranit, umožňují pouze včas upozornit na jeho přítomnost. Další činnost již záleží na uživateli. V každém případě by mělo platit to, že jakoukoli další antivirovou činnost musí vykonávat člověk, obeznámený se systémem a s hrozícími následky!!!



Integrované prostředí AVAST!

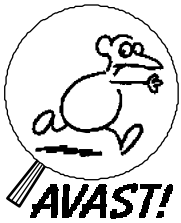
Jednotlivé komponenty systému AVAST! jsou vytvořeny tak, aby je bylo možno používat samostatně pro ty účely, pro které jsou určeny. Uživatel je může spouštět z příkazového řádku nebo z dávek, přičemž zadává parametry tak, jak je to popsáno v dalších kapitolách. Kromě toho však může použít i program AVAST.EXE, který vytváří integrované prostředí v sytému DOS. Z něho lze nastavit jednak parametry všech programů a jednak vlastní programy vyvolávat. Pokud si to uživatel přeje, může parametry uložit do zvláštního konfiguračního souboru AVAST.INI, ze kterého jsou opět přečteny při příštím spuštění.

Základní obrazovka programu AVAST vypadá takto:



V programu AVAST jsou použita roletová menu, ve kterých je možno pohybovat se pomocí kurzorových kláves, stisknutí zvýrazněného písmena či pomocí myši. První menu je určeno ke spouštění programů, druhé k zadávání a modifikaci příkazového řádku. Při modifikaci příkazového řádku je na obrazovce vypsána podrobná nápověda pro daný program, ze které je zřejmý význam všech možných parametrů. Z tohoto pro–

gramu nelze poprvé spouštět (a tím instalovat do paměti) programy FGUARD a RGUARD, je však možno nastavovat jejich parametry. Tyto programy by měly být instalovány při spuštění počítače pomocí startovací dávky systému.



Vyhledávací antivirové programy

Jedná se o programy, které jsou zaměřeny na známé konkrétní typy virů. Protože však dokáží počítačový virus pouze nalézt, nemusí znát jeho způsob šíření, jeho příznak ani manipulační činnost, ale pouze jeho určitou charakteristiku. Touto charakteristikou je například určitá posloupnost instrukcí, tj. charakteristická data obsažená v každém programu, který byl napaden virem. Pro přidání nového viru proto nemusí být virus složitě analyzován, dokonce ani fyzicky přítomen, stačí znát pouze jeho charakteristiku. Je proto zřejmé, že tento typ programů dokáže daleko pružněji reagovat na výskyt nových druhů virů. To na druhé straně vede k nesmyslné soutěži jak mezi firmami, které vyvíjejí antivirové programy, tak mezi uživateli, které takové programy používají. Spory o to, že některý program umí vyhledat 8300 a jiný 9500 druhů virů, nemají naprosto žádný význam, protože s většinou virů se uživatel stejně nesetká (např. s některými exotickými viry, jež se vyskytly například pouze v Izraeli či Tchaj–wanu). Navíc je skutečný počet virů těžko srovnatelný, protože se často jedná o více variant menšího počtu virů. Mnohem důležitější proto je, aby bylo možno program rutinně a pohodlně používat, aby v případě infekce dokázal program správným způsobem zareagovat a aby nehlásil výskyt viru tam, kde žádný virus není – tzv. „falešný poplach“.

Výhodou tohoto typu antivirových programů je tedy poměrně velký počet známých řetězců, které umí programy vyhledat (v současnosti se toto číslo pohybuje mezi 8000 až 11000 a neustále roste), a také snadná modifikace, tedy přidávání dalších charakteristik nových druhů virů. To je možno umocnit tím, že uživatel může přidávat další charakteristiky sám.

Vyhledávací programy mají však i několik nevýhod. Velký nárůst počtu charakteristik vede k neúměrnému zvětšování velikosti databáze, a k potřebě neúměrně časté aktualizace. To může být velkou nevýhodou už v nedaleké budoucnosti, pokud se počet charakteristik přiblíží k mnoha tisícům. Dalším problémem je pak získávání ověřených charakteristik jednotlivých virů. Pokud dochází k jejich zveřejňování a výměně, vzniká nebezpečí, že někdo bude modifikovat existující viry tak, že vyhledávací programy virus nenaleznou. Další nectností vyhledávacích programů je to, že mohou vyvolat falešný poplach, tedy označit za nosič viru takový program, který ve skutečnosti virus neobsahuje.

Slabinou vyhledávacích programů je i to, že nedokáží pomocí jednoduché charakteristiky vyhledat některé typy virů, které se v posledních letech objevily, a to prostě proto, že u těchto „polymorfních" virů nelze žádnou charakteristiku zvolit. Viry jsou v každé své kopii jinak kódovány a i jejich část, která slouží k jejich rozkódování a která je jejich nutnou součástí, bývá „znáhodněna" tak, že určení charakteristiky je nemožné. Vyhledávání musí být prováděno algoritmicky na základě analýzy viru, což samozřejmě znehodnocuje princip vyhledávacích programů.

Přesto je zřejmé, že tento typ programů může být v oblasti prevence velmi účinný. AVAST! obsahuje celkem tři vyhledávací programy, z nichž každý má svoji zvláštní funkci a své zvláštní místo v antivirové ochraně. První je klasický vyhledávací program, druhý je určen pro práci v prostředí Windows a třetí je paměťově rezidentní, tj. umí vyhledávat viry v reálném čase.

Všechny naše vyhledávací programy dokáží nalézt ke dni 13. ledna 1995 kolem 3139 druhů virů. Tento počet se každým dnem zvyšuje, a proto je pravděpodobné, že verze, kterou jste obdrželi, obsahuje i další typy virů.

Všechny tři programy obsahují speciální algoritmus pro vyhledávání virů, který je schopen vyhledávat všechny charakteristiky paralelně. Je také schopen zvládnout řádově desítky tisíc různých charakteristik. Díky tomu jsou naše programy srovnatelné s nejrychlejšími vyhledávacími programy na světě.

Locate–GUARD

Upozornění: Změnila se struktura datového souboru LGUARD.VPS, takže VPS verze 7.7 není kompatibilní s předchozí verzí.

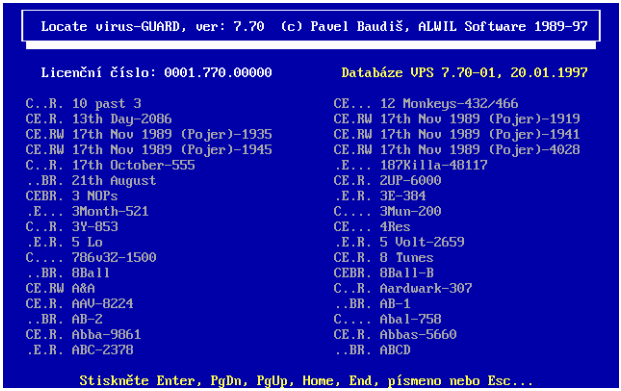
Na tomto místě jsme kdysi uveřejňovali seznam virů, který je schopen program LGUARD nalézt. Tento seznam však dnes narostl do takových rozměrů, že není možné ani efektivní ho na tomto místě uvádět. Navíc nemůže být úplný, protože program LGUARD je schopen detekovat i řadu dalších variant a mutací těchto základních druhů virů. Jejich počet může však být jen těžko přesně určen a nemá (kromě bombastické reklamy) ani valný smysl. Aktuální seznam virů můžete uložit do souboru VIRLIST.TXT, pokud spustíte program LGUARD s parametry /V a /R.

Databáze charakteristik virů je uložena v externím souboru LGUARD.VPS. To umožňuje provádět aktualizace distribucí pouze tohoto souboru. Verze souboru LGUARD.VPS a datum, kdy byl vytvořen, jsou vypisovány v pravé horní části obrazovky při každém spuštění programu. Ve verzi 7.5 došlo ke změně číslování verzí LGUARD.VPS: číslo verze nyní sestává ze dvou částí: např. 7.50–12. Druhé číslo udává pořadí aktualizovaného souboru. LGUARD vypisuje číslo své verze a verze souboru VPS, pokud si navzájem neodpovídají.

Do vyhledávacích programů byla přidána korektní detekce makro virů včetně správné analýzy OLE2 souborů. Pro detekci makrovirů již není potřeba prohledávat celý soubor, program jej sám analyzuje, vyhledá makra, pokud jsou přítomna, a detekuje makroviry. Ty jsou detekovány dvojím způsobem – jednak přesnou identifikací konkrétního makroviru, založenou na kontrolním součtu maker viru, jednak pomocí vyhledávacích řetězců, které umožňují zjistit přítomnost i nových virů z dané rodiny makrovirů. DOSový program LGUARD umožňuje dokonce odstranění makro virů z dokumentu, které může být velmi užitečné, protože po odstranění maker je možno dokument bez problémů použít. Pro smazání maker je možno použít stejný parametr, jako pro smazání souborů napadených klasickým virem. Pokud je zjištěn

makrovirus, program se ptá, zda se mají odstranit pouze makra daného viru (pouze při přesné identifikaci), všechna makra, či má li být smazán celý dokument. Podobný požadavek je možno specifikovat i na příkazovém řádku, pokud je za /Z uvedeno M (jen Makra viru), V (Všechna makra) nabo S (celý Soubor). Program se pak zeptá pouze na to, zda má dané odstranění provést (Ano či Ne). To je možno využít i s parametrem /P pro plynulé odstranění. Pokud program pracuje plynule a je uvedeno pouze /Z, předpokládá se /ZM pro přesně identifikované viry a /ZV pro rodiny virů.

Vývoj programu LGUARD není ukončen, pravidelně probíhá jeho aktualizace tak, jak se objevují nové viry. Pokud již od doby vytvoření souboru LGUARD.VPS uběhlo více než půl roku, program LGUARD vás na tuto skutečnost automaticky upozorní a doporučí vám získat aktualizovanou verzi programu. V rámci naší antivirové služby je aktualizace prováděna přibližně každý měsíc. Aktuální stav programu i seznam známých virů je možno zjistit jeho spuštěním s parametrem **/V** (na následujícím obrázku je pouze první stránka výpisu):



Kromě právě platného seznamu virů program LGUARD vypíše i cíle, které jednotlivé viry napadají. Ty jsou označeny následujícími písmeny:

C virus napadá soubory typu COM,

E virus napadá soubory typu EXE,

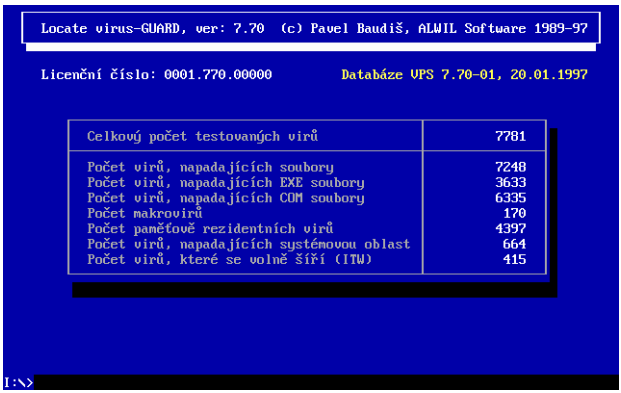
B virus napadá systémovou oblast disku (sektor tabulky rozdělení disků a/nebo zaváděcí sektor disku),
R virus zůstává umístěn rezidentně v operační paměti.

Program LGUARD dále rozeznává zvláštní kategorii virů, které se volně šíří mezi uživateli (tj. jsou In the Wild, zkratka ITW). Údaj o tom, že virus je ITW se zobrazuje jak v seznamu virů (znakem W), tak i v případě nalezení viru speciálním upozorněním v popisu viru (klávesa F1). Ve výpisu virů jsou makroviry označeny písmenem M.

W virus je rozšířen mezi uživateli (In the Wild).
M makrovirus napadající dokumenty.

Po jednotlivých obrazovkách výpisu je možno se pohybovat klávesami PgUp, PgDn, Home a End. Při stisknutí libovolného písmena se vypíše obrazovka se jmény virů, které daným písmenem začínají.

Nakonec program vypíše celkovou statistiku, tj. počet sledovaných virů, počet virů, které napadají soubory, COM soubory a EXE soubory, počet virů, které napadají systémovou oblast disku, počet paměťově rezidentních virů, počet makrovirů a počet ITW virů:



Program LGUARD po svém spuštění nejdříve prohledá paměť počítače a testuje, zda v ní nejsou některé z výše uvedených virů instalovány. Pokud program najde v paměti charakteristiku viru, oznámí tuto skutečnost uživateli. Jestliže k tomu dojde, doporučujeme vypnout počítač a pak zavést

systém z originální systémové diskety, chráněné proti zápisu (popřípadě z předem pro tento účel připravené diskety). Poté je třeba z kopie distribuční diskety AVAST! spustit originální program LGUARD. Bez tohoto kroku by totiž mohlo dojít k tomu, že virus napadne všechny soubory, které jsou programem LGUARD testovány!

Pokud program LGUARD zjistí virus v operační paměti, nabídne možnost nového zavedení systému počítače. Pokud s tím uživatel souhlasí, je vyzván, aby vložil do jednotky A systémovou disketu a poté je systém znovu zaveden. Pro zavedení systému z originální diskety však doporučujeme počítač úplně vypnout a zapnout.

Po testu paměti program LGUARD prohlédne systémovou část disku (zaváděcí sektor a sektor s tabulkou rozdělení disků) a testuje přítomnost tzv. „boot virů“. Tyto viry nenapadají soubory, ale šíří se právě přes systémovou oblast. Pokud LGUARD takový virus nalezne, opět to oznámí uživateli. LGUARD je schopen rozpoznat, zda běží pod Windows NT, a pak **netestuje** systémovou oblast.

Pokud je paměť počítače i systémová oblast disku v pořádku, LGUARD o tom vypíše zprávu na obrazovce a tři vteřiny čeká. Čekání je možno ukončit stisknutím libovolné klávesy. V dalším kroku LGUARD prohledává soubory na disku a testuje přítomnost virů. Uživatel může specifikovat disk a adresář, který má být prohledán (implicitně hlavní adresář právě platného disku a všechny jeho podadresáře). Specifikovat je možno více disků najednou, pokud jsou testována výměnná média, LGUARD se ptá, zda má být testováno další médium, a pokud ano, vyžádá si jeho vložení do jednotky. Dále je možno zadat rozšíření (file extension) testovaných souborů (implicitně jsou testovány všechny programy – soubory s rozšířením COM, EXE, SYS, OV? a BIN). Program LGUARD vždy testuje nejdříve sám sebe, protože pokud není umístěn na médiu chráněném proti zápisu, může být některými viry při svém spuštění napaden. Je testován vždy bez ohledu na to, zda se nachází na testovaném disku. Testování souborů je možno kdykoli přerušit pomocí stisknutí klávesy **Esc**. Program LGUARD se poté zeptá, zda má opravdu ukončit svoji činnost a pokud ano, učiní tak. Pokud bylo při spuš–

tění programu LGUARD zadáno heslo, je nutno pro ukončení činnosti toto heslo správně zadat.

Pokud program LGUARD nalezne soubor, který obsahuje charakteristiku viru, oznámí to uživateli. Uživatel má možnost stiskem klávesy F1 zjistit základní vlastnosti viru, ktreré obsahují informace o cíli napadení a o tom, zda je virus paměťově rezidentní. LGUARD nabízí speciální popisy pro viry, které nelze odstranit příkazem FDISK /MBR (Onehalf, Starship, Volga, Monkey apod). Stisknutím klávesy F2 se zobrazí základní informace o souboru zobrazuje se velikost souboru, datum a čas poslední modifikace a atributy.

Informace o tom, že soubor obsahuje virus, je pouze informativní, podezření je proto třeba prověřit! Platí to zejména o virech, vytvořených ve vyšších programovacích jazycích (Pascal, C), u kterých je obtížné vytypovat jednoznačnou „charakteristiku“ viru. Příkladem takového viru, který může způsobit falešný poplach, je virus Kamikaze. Pro pokračování programu je nutno stisknout kteroukoli klávesu. Na závěr své činnosti vypíše LGUARD přehlednou statistickou tabulku, ve které je uveden počet testovaných souborů a nalezených virů.

Na vypracování rychlého a efektivního algoritmu pro vyhledávání charakteristik virů jsme kladli opravdu velký důraz. Výsledkem je to, že náš vyhledávací program patří k nejrychlejším produktům tohoto druhu na světě. Přesto může být čas potřebný k testování disku příliš dlouhý (zvláště při velkém počtu souborů na discích). Vzhledem k vlastnostem naprosté většiny známých virů jsme se rozhodli implicitně testovat pouze začátek a konec každého souboru, a to v dostatečné délce 8192 slabik. Pomocí přepínače **/C** lze však určit, že bude testován **celý obsah** souborů. Celý obsah souborů bude také automaticky testován v případě, že již byl nalezen nějaký virus.

Program LGUARD je schopen rozpoznat soubory komprimované pomocí různých programů (např. Pklite, Lzexe a Diet) a některými spojovacími programy (linker). Takové soubory mohou být napadeny dvojím způsobem: interně (tj. před komprimací) nebo externě (tj. po komprimaci). Program LGUARD je schopen testovat i obsah souborů, které byly **komprimovány** některým ze standardních komprimačních

pro–gramů Diet, Lzexe, Pklite, Ice a Shrink. Tento test se provádí, pokud bylo zadáno testování celých souborů (nebo pokud již byl dříve nalezen nějaký virus). V komprimovaných souborech se netestuje přítomnost polymorfních virů. Hlá–šení o vnitřním testu je vypisováno na obrazovku i do report souboru.

Pokud není žádný virus nalezen, zobrazuje program LGUARD informaci o tom, zda soubor obsahuje nějaká makra, zda je šablonou či dokumentem Word či zda se jedná o soubor OLE2.

Program LGUARD dokáže odhalit řadu polymorfních virů. Ty jsou kódovány takovým způsobem, že jsou v každé své kopii jiné a není tudíž možno určit žádný vzorek, podle kte–rého by je bylo možno nalézt. Je proto nutno odhalit je algo–ritmicky. Příkladem takových virů mohou být Flip, Maltská Amoeba, Tremor, Slovakia, viry používající MtE (Mutation Engine) či slovenský One half.

Pokud je program LGUARD spuštěn s parametrem **/W[he–slo]**, pak je při nalezení viru na obrazovce zobrazena vy–centrovaná dvouřádková zpráva, definovaná uživatelem a uložená v textovém souboru **LGUARD.MSG**. Pokud je parametr /W použit, musí tento soubor existovat ve stejném adresáři, ve kterém je umístěn program LGUARD.EXE. Obsah tohoto souboru (maximálně 2 řádky po 76 znacích) může sloužit k vyvolání správné reakce i laické obsluhy po–čítače při výskytu viru, například:

```
Na tomto počítači se vyskytl virus, zavolejte Frantu Vonáska
na lince 441, do jeho příchodu s počítačem nic nedělejte!!
```

Jestliže je na příkazovém řádku zadáno za parametrem /W i heslo, je nutno toto heslo napsat na klávesnici před dalším pokračováním programu. Toto heslo tak může sloužit k tomu, že obsluha počítače skutečně další činnost provádět nebude. Toto heslo je nutno zadat i při případném přerušení činnosti programu. Lze tak zabezpečit, že testování opravdu proběhne až do konce. Pokud byl jako heslo zadán znak „**+**“, je zpráva vypsána na obrazovku ihned (jako test pro zobrazení zprávy).

Ukázkový soubor LGUARD.MSG je i na distribuční disketě. Jestliže chcete tuto vlastnost použít, nezapomeňte obsah souboru změnit, aby uživatel opravdu nevolal Frantu Vonáska!

Pokud je program LGUARD spuštěn s parametrem **/P**, pak pracuje plynule, bez pauzy po testování paměti a při nalezení viru. Při testování je pak možno reagovat pouze na hodnotu návratového kódu.

Pokud je program LGUARD spuštěn s parametrem **/I**, pak se při testování výměnných médií (např. disket) neptá, zda má být testováno další médium, ale ukončí svoji činnost.

Jestliže je program LGUARD spuštěn s parametrem **/R**, vytvoří výstupní soubor se seznamem zjištěných virů a přehlednou statistickou tabulkou. Pokud je za parametrem /R znak „*“, jsou do výstupního souboru zaznamenány i soubory, ve kterých nebyl žádný virus nalezen.

Pokud je program LGUARD spuštěn s parametrem **/Z**, nabídne při detekci viru možnost smazání podezřelého souboru.

Pokud je program LGUARD spuštěn s parametrem **/X**, nabídne při detekci viru možnost přejmenování podezřelého souboru. Prvním znakem rozšíření je po přejmenování písmeno „V“ (např. z COM se stane VOM, z EXE VXE atd.).

Program LGUARD má i další zajímavou vlastnost. Je jí možnost uživatelsky **definovat další charakteristiky virů**, a tak velmi pružně reagovat na výskyt nových virů, se kterými se uživatel může setkat. Pomocí přepínače **/F** lze specifikovat jméno textového souboru, který obsahuje tyto charakteristiky. Řádky v tomto souboru, které začínají znakem „*“, jsou považovány za komentáře a jsou ignorovány. Definice charakteristiky viru se skládá ze tří řádků. Na prvním se nachází jméno viru, dlouhé maximálně 29 znaků, na druhém řádku se nachází specifikace objektů, které virus napadá (pomocí velkých písmen „**C**“, „**E**“, „**B**“ a „**R**“ tak, jak to bylo uvedeno v předchozích odstavcích. Na třetím řádku se nachází vlastní charakteristika viru ve formě hexadecimálního řetězce znaků bez jakýchkoli oddělovačů (na každou slabiku připadají dva znaky) o maximální délce 32 slabik, tj. 64 znaků. Charakteristika může obsahovat i „žolíky“ (wildchars), které znamenají, že na dané pozici může být libovolný znak. To se definuje pomocí dvou znaků „**??**“. Žolíky se nesmí vyskytovat

na prvních dvou pozicích. Při jejich častém používání se však zvyšuje riziko falešných poplachů, proto je nutno s nimi šetřit! Lépe nám vše přiblíží následující ukázka fiktivních (tj. neexistujících!) virů:

```
* ==============================
* toto je komentář: ukázka definice fiktivních neexistujících virů
* následující virus napadá systémovou oblast disku a je rezidentní:
Modrovous
BR
8CC88EAD8EDA0BCBBF0FBA2367CA2097
*
* následující virus napadá pouze programy typu COM a obsahuje „žolíky“:
Alenka
C
F687772A01081740F3??DB??FF4D01BC
*
* následující virus napadá programy typu COM i EXE, navíc je rezidentní:
HUHU
CER
FA8B8005BEB310172A0B74D0131C75F8
* ==============================
```

Pokud je charakteristika viru vhodně zvolena, měla by být dostatečná délka 16 slabik (tj. 32 znaků). Z hlediska rychlosti algoritmu programu LGUARD je výhodné, pokud charakteristika viru nezačíná binární nulou (tj. znaky „**00**“).

Program LGUARD podporuje také počítačovou síť Novell. Kromě toho, že je samozřejmě možné testovat síťové disky, nabízí i možnost poslat vybranému uživateli sítě zprávu o tom, že na pracovní stanici byl nalezen virus. Tato volba je specifikována parametrem **/U**, za kterým může následovat jméno uživatele – příjemce. Pokud není žádné jméno uvedeno, je zpráva odeslána uživateli Supervisor. Uživatel zprávu obdrží pouze tehdy, když je do sítě přihlášen a má povolen příjem zpráv. Kromě toho je zpráva o výskytu viru odeslána (spolu s datem a časem) i na systémovou konzoli sítě, např:

```
01.12. 16:12 NOVAK[05]virus Anti-Telefonica (CSFR)
```

Zpráva je odeslána pouze při prvním nalezeném viru během jednoho spuštění programu. Pokud LGUARD nalezne virů více, další zprávy již posílány nejsou. Tato funkce je určena k většímu zabezpečení počítačových sítí, jejichž provoz může být viry ohrožen v daleko větší míře. Parametr /U může být nahrazen definováním proměnné environmentu **AVASTMES**. Tato proměnná určuje uživatele sítě Novell, jemuž bude poslána zpráva o nalezeném viru, a slouží k pružnějšímu hlášení výskytu virů v síti. Pokud je definována, není nutno parametr

/U vůbec zadávat. Nově může být uvedeno více uživatelů, jejichž jména se oddělují středníkem.

Zpráva o viru na dané pracovní stanici může být poslána i uživateli, který se nachází v jiném kontextu (platí u sítě Novell od verze 4.00). Takového uživatele je nutno specifikovat přesně ve stejném tvaru, v jakém ho vypisuje program NLIST s parametry USER /A /B. Jedinou vyjímkou je to, že znak „=“ musí být pro proměnnou AVASTMES nahrazen znakem „:“, aby se vyhovělo syntaxi operačního systému DOS.

Nastavení může být následující:

```
SET AVASTMES=Novak
```

kde Novak je jméno uživatele, jemuž má být zpráva o zjištěném viru odeslána.

Hlavní nevýhodou vyhledávacích programů je neúměrně častá potřeba aktualizace databáze virů. Půl roku starý program již nemusí být dostatečně schopen reagovat na dynamický vývoj této oblasti. Proto program LGUARD testuje datum, kdy byla vytvořena databáze LGUARD.VPS a pokud od té doby uplynulo více než půl roku, vypíše o tom zprávu na obrazovku. Pak pokračuje v činnosti normálním způsobem.

Chování programu LGUARD je možno částečně ovlivnit nastavením proměnné environmentu **AVAST**, která umožňuje určit kód výpisu programů AVAST, AGUARD, LGUARD a SGUARD a potlačit pípání u programů AGUARD a LGUARD. Nastavení této proměnné může být následující:

```
SET AVAST=[K|L|N][S]
```

kde K, L a N určují kód výpisu a S znamená potlačení zvukových varování.

Způsob spuštění programu

```
LGUARD /H
LGUARD /V
LGUARD [[d:\]cesta][.][/E[ext1[;ext2;...]]][/D]
   [/C][/M][/Fsoubor][/W[heslo|+|-]] [/U[uživatel]]
   [/P][/R[soubor]][/Z][/X][/I][/S][/Q][/K][/L][/N]
```

Přepínač /H či /?

Program LGUARD vypíše **návod** na použití a ukončí svoji činnost.

Přepínač /V

Program LGUARD vypíše **aktuální seznam virů**, které umí vyhledat, a ukončí svoji činnost.

Parametr d:\cesta

Tento parametr umožňuje uživateli specifikovat **disk a adresář**, jehož soubory mají být testovány. Je–li tento parametr vynechán, jsou testovány soubory v hlavním adresáři právě platného disku. Specifikovat je možno více disků najednou, pokud jsou testovány diskety, LGUARD se ptá, zda má být testována další disketa, a pokud ano, vyžádá si její vložení do jednotky.

Parametr d:\cesta\soubor

Při specifikaci kompletního jména soubopru LGUARD otestuje samostatný soubor. Soubor MUSÍ existovat!

Parametr .

Tento parametr umožňuje uživateli specifikovat, že bude **testován právě platný adresář na právě platném disku**.

Parametr *:

Tento parametr umožňuje uživateli specifikovat, že budou **testovány všechny lokální pevné disky**.

Parametr #:

Tento parametr umožňuje uživateli specifikovat, že bude **testovány všechny síťové disky.** Program hlásí chybu, pokud je zadán parametr #: a není nalezen žádný síťový disk.

Přepínač /E

Tento přepínač umožňuje uživateli specifikovat **rozšíření (file extensions)** testovaných souborů. Může být specifikováno až 10 různých rozšíření, oddělených středníkem. Rozšíření mohou obsahovat znaky ? a * pro zadání masky (více souborů najednou). Je–li tento přepínač vynechán, jsou testovány soubory s rozšířením COM, EXE, SYS, OV? a BIN.

Přepínač /D

Tento přepínač určuje, že **nebudou testovány soubory v podadresářích** daného adresáře. Je–li tento přepínač vynechán, jsou testovány kromě souborů daného adresáře i soubory ve všech jeho podadresářích.

Přepínač /C

Tento přepínač určuje, že se testuje **kompletní obsah souborů**. Implicitně se testuje pouze začátek a konec souboru o délce 8192 slabik, což je mnohem rychlejší. Po nalezení libovolného viru program automaticky přepne do režimu testování celých souborů.

Přepínač /M

Tento přepínač určuje, že se testuje pouze **přítomnost virů v paměti a v zaváděcím sektoru disku**. Nejsou testovány žádné soubory. Toto vyvolání programu může sloužit k rychlému otestování stavu systému například v inicializační dávce AUTOEXEC.BAT.

Přepínač /B

Tento přepínač určuje, že se nebude testovat **přítomnost virů v operační paměti**. Pokud jste si jisti, že počítač neobsahuje žádné viry a chcete například otestovat obsah disket, může tento přepínač celý proces urychlit.

Přepínač /A

Tento přepínač určuje, že se testuje i **přítomnost boot virů v souborech**. To může sloužit k otestování souborů, které obsahují „obraz" systémové oblasti disku bez toho, aby bylo nutno je kopírovat zpět na disk či disketu. Po nalezení libovolného viru program automaticky přepne do režimu testování všech typů virů.

Přepínač /Fsoubor

Tento přepínač určuje, že se z daného souboru přečtou další, uživatelské charakteristiky virů. To umožňuje uživatelům aktuálně zařadit do programu i nové typy virů, které se u nich nebo v jejich okolí vyskytly.

Přepínač /W[heslo|+|–]

Tento přepínač určuje, že při zjištění viru se na obrazovce **vypíše uživatelsky definovaná zpráva**, sloužící k informování obsluhy o správné akci. Zpráva je uložena v souboru LGUARD.MSG, umístěném ve stejném adresáři jako spouštěný program LGUARD.EXE. Pokud je zadáno i heslo, je nutno před pokračováním programu při nalezení viru nebo při přerušení činnosti toto heslo zadat pomocí klávesnice. Parametr „+" slouží k otestování funkčnosti zprávy. Parametrem „/W–" zastaví při nalezení viru počítač.

Přepínač /U[uživatel]

Tento přepínač určuje, že při zjištění viru je v síti Novell **odeslána zpráva o viru vybranému uži–**

vateli sítě. Pokud není uživatel uveden, je zpráva poslána uživateli Supervisor. Uživatel – příjemce musí být přihlášen do sítě a musí mít povolen příjem zpráv. Kromě toho je zpráva odeslána i **na systémovou konzoli sítě**.

Přepínač /P

Tento přepínač určuje, že program bude pracovat **plynule** bez pauz po testování systémových oblastí disku a bez čekání na odezvu uživatele při zjištění viru. Pro informaci o výsledku testování je možno použít definované návratové kódy.

Přepínač /R[soubor]

Tento přepínač určuje, že bude vytvořen **výstupní textový soubor se seznamem zjištěných virů** a přehlednou statistickou tabulkou (report file). Pokud není jméno souboru specifikováno, je výstupním souborem LGUARD.RPT v právě platném adresáři. Pokud je za parametrem /R znak „*“, jsou do výstupního souboru zaznamenány i soubory, ve kterých žádný virus nalezen nebyl.

Přepínač /Z

Tento přepínač určuje, že podezřelé soubory, které obsahují charakteristiky virů, budou nabídnuty ke **smazání** uživatelem. Pro odstranění makrovirů je možné přepínač /Z doplnit o další písmeno specifikující požadovanou akci. Pokud je za /Z uvedeno M odstraní se jen Makra viru, písmeno V zajistí vymazání Všech maker dokumentu, S vymaže celý Soubor. Program se pak zeptá pouze na to, zda má dané odstranění provést (Ano či Ne). To je možno využít i s parametrem /P pro plynulé odstranění. Pokud program pracuje plynule a je uvedeno pouze /Z, předpokládá se /ZM pro přesně identifikované viry a /ZV pro rodiny virů.

Přepínač /X

Tento přepínač určuje, že podezřelé soubory, které obsahují charakteristiky virů, budou nabídnuty k **přejmenování** uživatelem. Prvním znakem rozšíření je po přejmenování písmeno „V“ (např. z COM se stane VOM, z EXE VXE atd.).

Přepínač /I

Tento přepínač je určen pro **ignorování výměnných médií**. Pokud je testováno médium v jednotce, která podporuje výměnná média, program se normálně ptá, zda bude testováno další médium. Pokud je zadán parametr /I, program po otestování média skončí svoji činnost.

Přepínač /S

Tento přepínač určuje, že zjištěné viry **nebudou indikovány pípnutím**. Implicitně jsou všechny zjištěné charakteristiky zvukově indikovány.

Přepínač /Q

Tento přepínač určuje, že **neproběhne verifikace VPS souboru**, takže načtení (např. z diskety) je mnohem rychlejší.

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu „MJK“** (kód bratrů Kamenických).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu PC Latin 2**.

Přepínač /N

Tento přepínač určuje, že veškerý text bude zobrazen **bez diakritických znamének**.

Návratové kódy

V okamžiku ukončení činnosti program LGUARD vrátí operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce pomocí příkazu IF ERRORLEVEL. Návratový kód programu LGUARD může nabývat pouze následujících hodnot, které mají tento význam:

0 program normálně ukončen, žádný virus nenalezen,
1 nalezen virus v paměti,
2 nalezen virus na disku, ale ne v paměti,
3 program přerušen uživatelem, dosud žádný virus nenalezen,
4 při práci došlo k chybě, dosud žádný virus nenalezen.
98 program vypisoval seznam virů, které umí vyhledat,
99 program vypisoval návod na použití.

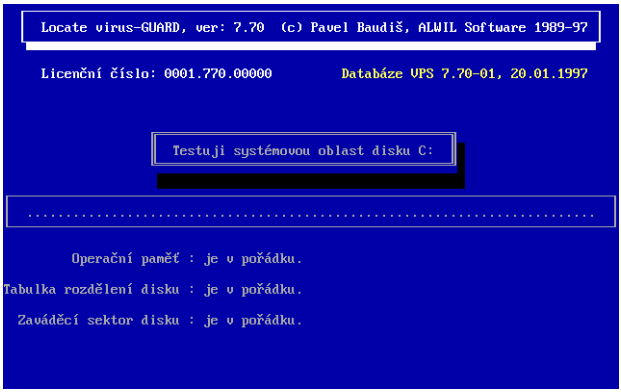
Takto definované návratové kódy je možno použít především v příkazových dávkách pro jejich větvení při zjištění viru. Příkladem může být příkazová dávka SCAN.BAT, která se nachází na distribuční disketě a která demonstruje využití návratového kódu programu LGUARD a test více disků. Způsob využití návratového kódu a příkazu IF ERRORLEVEL je zřejmý i z následující ukázky (význam jednotlivých funkcí je zřejmý i z názvů návěští pro skok):

```
..
lguard c:
if errorlevel 4 goto chyba
if errorlevel 3 goto přerušení
if errorlevel 2 goto diskvir
if errorlevel 1 goto memvir
echo ** na disku c: nebyly žádné viry
nalezeny **
..
```

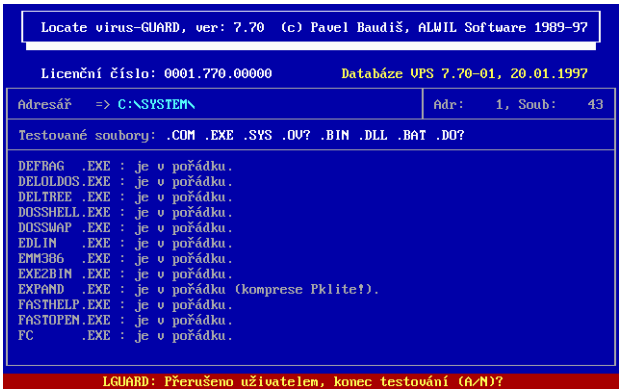
Příklady použití

LGUARD C:\SYSTEM

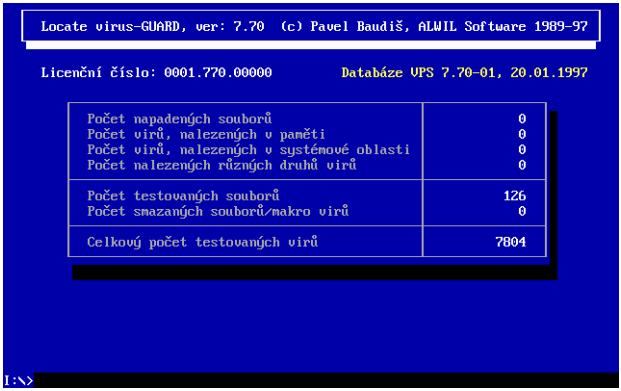
spuštění programu pro adresář SYSTEM na disku C:, testovány jsou všechny soubory typu COM, EXE, SYS, OV? a BIN v tomto adresáři. Nejdříve se testuje paměť a zaváděcí sektor pevného disku. Pokud je všechno v pořádku, objeví se následující informace:



Poté se postupně testují jednotlivé soubory, o čemž je uživatel informován na obrazovce:



Na závěr se na obrazovce objeví výsledná tabulka:



V této tabulce je uveden počet virů, nalezených v operační paměti, v systémové oblasti disku, celkový počet napadených souborů a také počet souborů, které byly uživatelem smazány. Pro informaci je zde uveden i počet charakteristik virů, které je program LGUARD schopen nalézt.

Resident-GUARD

Kromě klasických vyhledávacích programů, které musí být spouštěny uživatelem, obsahuje systém AVAST! i paměťově rezidentní program, který může vykonávat stejnou funkci,

ovšem automaticky. Umožňuje totiž před spuštěním libovolného programu otestovat jeho obsah a vyhledat v něm případné počítačové viry.

Obecně existují u tohoto typu programu dva velké problémy. Prvním jsou velké paměťové nároky a druhým částečné zdržení při testování programů. U programu RGUARD jsme první problém vyřešili tak, že si je možno vybrat, co se bude testovat, a část programu pro testování souborů zabírá **kolem 1 KB** operační paměti. Pro řešení druhého problému byla zvolena nejrozumnější varianta – obsah souborů je testován pouze při spouštění programů a ne při jejich čtení, kdy dochází k velkému zdržení. Infikované programy je proto možno libovolně kopírovat, ale není možné je spustit. Zdržení se proto projevuje pouze při spouštění aplikace, při práci se soubory žádné omezení neexistuje.

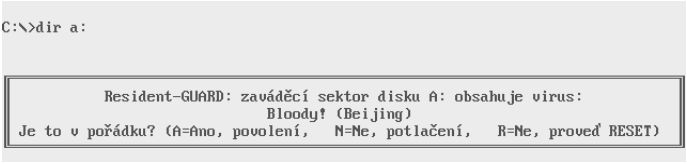
Další problémy s testováním mohou nastat v počítačových sítích. Pokud má uživatel právo programy pouze spouštět a ne číst (atribut Execute only), nemůže být ze zcela zřejmých důvodů obsah souboru na přítomnost virů otestován. Přesto program RGUARD v tomto případě umožní spuštění programu.

Program RGUARD využívá pro testování stejnou databázi virů jako program LGUARD, která je uložena v souboru LGUARD.VPS. Z toho vyplývá, že program RGUARD nemůže nalézt jiné viry než LGUARD. Přesto může být jeho nasazení výhodné, protože přítomnost virů kontroluje průběžně. Pro řadu uživatelů je tento typ programů velmi důležitý.

Pokud již od doby vytvoření souboru LGUARD.VPS uběhlo více než půl roku, program RGUARD vás na tuto skutečnost automaticky upozorní a doporučí vám zajímat se o aktualizaci programu. V rámci naší antivirové služby AVS je aktualizace prováděna přibližně každý měsíc.

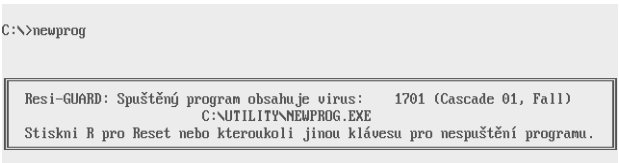
Program RGUARD nabízí dva samostatné druhy vyhledávání. Prvním je testování systémové oblasti používaných disků a disket. Pokud při své práci použijete disketu (třeba i jen obsahující datové soubory), je její zaváděcí sektor prohlédnut, zda neobsahuje nějaké boot viry. Jediným kanálem, jak boot virus může napadnout počítač, je totiž pokus o zavedení systému z infikované diskety. Uživatelé často zapome-

nou použitou disketu v jednotce, a z ní se při zavedení systému virus může rozšířit na pevný disk. Tento druh testování nezpůsobuje žádné zpomalení práce s počítačem a zabírá asi 8 KB operační paměti (od verze 7.7 vyžaduje pro svou činnost paměť typu XMS). Pokud RGUARD nalezne v zaváděcím sektoru diskety virus, oznámí to uživateli pomocí zvláštního okna:



Odpověď **N (ne)** znamená potlačení operace čtení. Pokud uživatel chce přes přítomnost viru na disketě s jejím obsahem pracovat (například použít datové soubory na ní uložené), může zvolit odpověď **A (ano)**. Stejný význam má i klávesa **Enter**. Kromě toho má uživatel k dispozici další volbu **R (ne, proveď RESET)**, pomocí které je znovu zaveden systém počítače (obdoba známé trojkombinace kláves **Ctrl+Alt+Del**). Uživatel je pak vyzván, aby do jednotky A vložil originální systémovou disketu a pak vypnul a zapnul počítač.

Druhou možností programu RGUARD je už výše zmíněné testování obsahu spouštěných souborů. Kód pro tento test je velmi malý, zabírá kolem 1 KB operační paměti. Pro testování je použit soubor RGUARD.OVL, který musí být umístěn ve stejném adresáři jako program RGUARD.COM. Vyhledávání virů v souboru je provedeno před spuštěním aplikačního programu a pokud je v jeho kódu nalezen virus, opět se na obrazovce objeví okénko se zprávou:



Uživatel má v takovém případě pouze dvě možnosti. Po stisknutí písmena **R** je proveden Reset počítače, po stisknutí libovolné jiné klávesy je řízení předáno zpět. Infikovaný program však za žádných okolností nemůže být spuštěn!

Program RGUARD implicitně testuje přítomnost diskety v jednotce A, a pokud je stisknuto Ctrl–Alt–Del, nepovolí restart počítače, dokud není disketa odstraněna. Tato funkce se dá vypnout pomocí parametru /R (je možno použít na počítačích bez disket, nebo pokud je zakázáno zavádění systému z diskety v setupu počítače.

I pro program RGUARD je možno využít uživatelsky **definované charakteristiky virů**. Pomocí přepínače **/F** lze při instalování programu RGUARD specifikovat jméno textového souboru, který obsahuje tyto charakteristiky. Způsob zadávání charakteristik virů je popsán u programu LGUARD.

Program RGUARD automaticky rozpozná instalaci ovladačů sítě Novell a upraví svoji činnost tak, že je schopen testovat i programy, spouštěné ze síťových disků. Pro kontrolu síťových disků na ostatních počítačových sítích je třeba program instalovat do paměti až po zavedení ovladačů sítě.

Program RGUARD podporuje prostředí počítačové sítě Novell i jinak. Nabízí možnost poslat vybranému uživateli sítě zprávu o tom, že na pracovní stanici byl nalezen virus. To, že program posílá zprávu, je specifikováno parametrem **/U**, za kterým může následovat jméno uživatele – příjemce. Pokud není žádné jméno uvedeno, je zpráva odeslána uživateli Supervisor. Uživatel zprávu obdrží pouze tehdy, když je do sítě přihlášen a má povolen příjem zpráv. Kromě toho je zpráva o výskytu viru odeslána (spolu s datem a časem) i na systémovou konzoli sítě, např:

```
01.12. 16:20 DVORAK[07] virus Arusiek
```

Zpráva je odeslána při pokusu o spuštění infikovaného programu i při zjištění boot viru. Zpráva o nalezení boot viru je odeslána pouze tehdy, pokud jsou instalovány v paměti obě části programu (viz dále). Je také poslána s určitým zpožděním. Celá tato funkce je určena k většímu zabezpečení počítačových sítí, jejichž provoz může být viry ohrožen v daleko větší míře. Parametr /U může být nahrazen definováním pro–

měnné environmentu **AVASTMES**. Tato proměnná určuje uživatele sítě Novell, jemuž bude poslána zpráva o nalezeném viru, a slouží k pružnějšímu hlášení výskytu virů v síti. Pokud je definována v okamžiku instalace programu RGUARD, není nutno parametr /U vůbec zadávat.

Zpráva o viru na dané pracovní stanici může být poslána i uživateli, který se nachází v jiném kontextu (platí u sítě Novell od verze 4.00). Takového uživatele je nutno specifikovat přesně ve stejném tvaru, v jakém ho vypisuje program NLIST s parametry USER /A /B. Jedinou vyjímkou je to, že znak „=“ musí být pro proměnnou AVASTMES nahrazen znakem „:“, aby se vyhovělo syntaxi operačního systému DOS.

Nastavení může být následující:

```
SET AVASTMES=Novak
```

kde Novak je jméno uživatele, jemuž má být zpráva o zjištěném viru odeslána.

Program RGUARD je schopen využívat paměť typu XMS, a proto může zabírat pouhých 6,2 KB základní paměti i v případě, že jsou instalovány obě jeho funkce. Může být instalován i do paměti UMB mimo základní paměť. Při jeho instalaci do paměti UMB může za určitých podmínek dojít k hlášení „Nedostatek UMB paměti“. V tom případě je nutno přesunout jeho instalování před jiné rezidentní programy nebo do základní paměti.

Poznámka pro programátory:

Program RGUARD může dále spolupracovat s uživatelsky vytvořenými programy, které v případě výskytu viru mohou vykonat další potřebnou činnost. Pokud program RGUARD nalezl nějaký virus, pošle o tom pomocí přerušení zprávu systému. Pro tuto zprávu bylo vytvořeno následující rozhraní, realizované pomocí multiplexoru (přerušení 2Fh):

a) při nalezení boot viru v systémové oblasti disku

```
registr AX          = DAD1h
registr BX          = 1
registr DL          = číslo testovaného disku (0=disketa A, 80h=první pevný disk)
registry ES:DI      = ukazatel na jméno zjištěného viru, zakončené nulou.
```

b) při nalezení viru ve spouštěném programu

```
registr AX          = DAD1h
registr BX          = 2
registry DS:DX      = ukazatel na jméno spouštěného programu, zakončené nulou
registry ES:DI      = ukazatel na jméno zjištěného viru, zakončené nulou.
```

Způsob spuštění programu

```
RGUARD /H
RGUARD /V
RGUARD [/B[+|-]][/E[+|-]][/U[uživatel]][/3[+|-]]
   [/Fsoubor][/X][/W][/O][/D][/K][/L][/N]
```

Přepínač /H či /?

RGUARD vypíše **návod** na použití a ukončí svoji činnost.

Přepínač /V

RGUARD vypíše **aktuální seznam BOOT virů**, které umí vyhledat, a ukončí svoji činnost.

Přepínač /B [+|–]

Tento přepínač umožňuje uživateli specifikovat, že se budou testovat systémové oblasti disků a disket na **přítomnost boot virů**. Pokud je použit při instalování programu RGUARD, je v paměti vyhrazeno místo pro toto testování. Pomocí parametrů „**+**“ a „**–**“ je možno testování kdykoli aktivovat a deaktivovat, ovšem pouze v případě, že pro test bylo při instalaci vyhrazeno příslušné místo.

Přepínač /E [+|–]

Tento přepínač umožňuje uživateli specifikovat, že se budou testovat spouštěné programy na **přítomnost virů**. Pokud je použit při instalování programu RGUARD, je v paměti vyhrazeno místo pro toto testování. Pomocí parametrů „**+**“ a „**–**“ je možno testování kdykoli aktivovat a deaktivovat, ovšem pouze v případě, že pro test bylo při instalaci vyhrazeno příslušné místo.

Přepínač /U[uživatel]

Tento přepínač určuje, že při zjištění viru je v síti Novell **odeslána zpráva o viru vybranému uživateli sítě**. Pokud není uživatel uveden, je zpráva poslána uživateli Supervisor. Uživatel – příjemce

musí být přihlášen do sítě a musí mít povolen příjem zpráv. Kromě toho je zpráva odeslána i **na systémovou konzoli sítě**.

Přepínač /3[+|–]

Tento přepínač umožňuje uživateli specifikovat povolení či zakázání 32–bitového přístupu na disk v prostředí Windows.

Přepínač /Fsoubor

Tento přepínač určuje, že se z daného souboru přečtou další, uživatelské charakteristiky virů. To umožňuje uživatelům aktuálně zařadit do programu i nové typy virů, které se u nich nebo v jejich okolí vyskytly.

Přepínač /X

Tento přepínač určuje, že jsou **zakázány** jakékoli **změny parametrů** a režimů činnosti při následujících spouštěních nebo pomocí Hot Key.

Přepínač /W

Tento přepínač určuje, že bude **ignorována instalace sítě Novell**. Ovladače sítě pak mohou být odstraněny z paměti, RGUARD však není v tomto případě schopen monitorovat činnost sítě.

Přepínač /R

Netestuje se přítomnost diskety při stisku kombinace Ctrl+Alt+Del.

Přepínač /O

Tento přepínač je určen pro použití s **floptickými disky** či jinak nestandardními disketovými jednotkami.

Přepínač /D

Tento přepínač určuje, že **na diskety, infikované boot virem, nebude povolen přístup**. Data z této

diskety pak není možno vůbec číst, uživatel je upozorněn na to, že na disketě je virus, a je požádán, aby disketu z jednotky okamžitě vyjmul.

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu „MJK“** (kód bratrů Kamenických).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu PC Latin 2**.

Přepínač /N

Tento přepínač určuje, že veškerý text bude zobrazen **bez diakritických znamének**.

Návratové kódy

V okamžiku ukončení činnosti program RGUARD vrátí operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce příkazem IF ERRORLEVEL. Návratový kód programu RGUARD může nabývat pouze následujících hodnot, které mají tento význam:

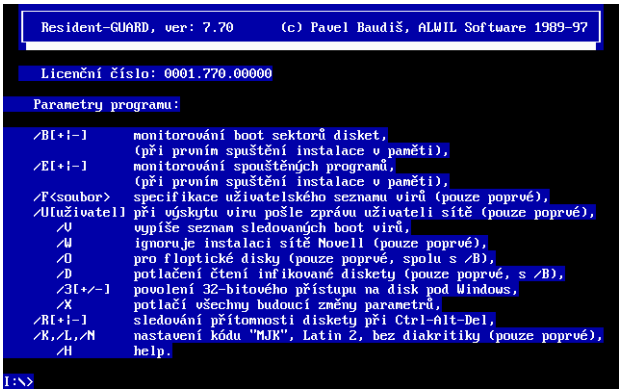
0 program byl instalován v paměti,
1 program byl již dříve nainstalován v paměti,
2 došlo k chybě, program není možno do paměti instalovat,
98 program vypisoval seznam virů, které umí vyhledat,
99 program vypisoval návod na použití.

Takto definované návratové kódy je možno použít především v příkazových dávkách pro jejich větvení při instalování programu do paměti.

Příklady použití

```
RGUARD /?
```

program vypíše jednoduchý návod

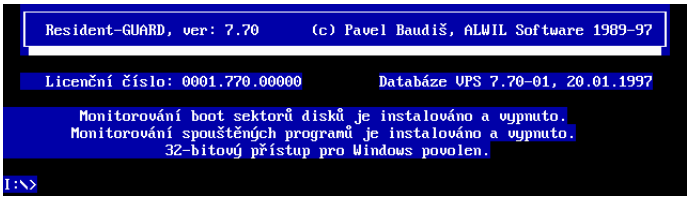


RGUARD

při prvním spuštění je instalován program RGUARD do paměti a všechny ochrany jsou zapnuty (viz obrázek); při dalších spuštěních je zobrazen právě nastavený stav programu.

RGUARD /B- /E-

při prvním spuštění je instalován program RGUARD do paměti, pro oba druhy testování je vyhrazeno v paměti místo, všechny ochrany jsou však vypnuty (viz obrázek); při dalších spuštěních jsou zapnuté ochrany vypnuty.


Resident-GUARD, ver: 7.70 (c) Pavel Baudiš, ALWIL Software 1989-97
Licenční číslo: 0001.770.00000 Databáze VPS 7.70-01, 20.01.1997
Monitorování boot sektorů disků je instalováno a vypnuto.
Monitorování spouštěných programů je instalováno a vypnuto.
32-bitový přístup pro Windows povolen.
I:\>

Obecné antivirové programy

Velmi vhodným obranným prostředkem proti počítačovým virům jsou obecné antivirové programy. Tyto programy nejsou zaměřeny proti konkrétnímu typu viru, ale mají obecnou platnost. Nemají sice vždy a za všech podmínek zaručenou stoprocentní spolehlivost jako zmíněné jednoúčelové antivirové programy, jejich význam je však veliký zejména v oblasti **prevence**, tj. předcházení infekci, popřípadě při včasném detekování viru v již infikovaném systému. Mohou totiž odhalit činnost i dosud neznámého typu viru, stejně jako mohou včas indikovat napadení osobního počítače již známým počítačovým virem.

Tyto programy vycházejí z jednoduchých principů. Viry se totiž mohou šířit jen pomocí modifikace kódu, který je počítačem vykonáván. Tento kód může být umístěn pouze ve výkonných souborech a v systémové oblasti pevných disků a disket. Viry při svém šíření **musí** změnit tento výkonný kód. Obecné antivirové programy hlídají a testují integritu, tj. neporušenost dat. Každá změna integrity je oznámena uživateli, který po zjištění její příčiny může správným způsobem zareagovat.

To však není jediná vhodná metoda. U počítačových virů je možno vypozorovat i určité vlastnosti a společné rysy, které jsou charakteristické pro jejich šíření. Pro napadení souborů viry používají určitým způsobem služby operačního systému, pro infikování systémové oblasti volají určité služby BIOSu. Je možno vytypovat i konkrétní funkce, často využívané v manipulační činnosti virů. Tyto funkce mohou být přitom velice nebezpečné. Díky architektuře procesoru i vlastnostem operačního systému je možno vyvinout paměťově rezidentní program, který monitoruje funkce operačního systému a BIOSu a všechny podezřelé okolnosti okamžitě nějakým způsobem indikuje.

Velmi vhodným prostředkem může být i program, který uloží a později je schopen obnovit kritické systémové oblasti pevných disků. Takový program je schopen velmi jednoduše odstranit jakýkoli boot virus.

V souboru antivirových programů AVAST! jsou čtyři obecné antivirové programy. Jejich nasazení umožňuje včas předejít virové nákaze osobního počítače, jednoduše viry odstranit, a tak zabránit možným velkým škodám.

Sum–GUARD

Nejjednodušším obecným antivirovým programem v systému AVAST! je program SGUARD (Sum–GUARD, hlídač součtů). Tento program umožňuje velmi rychlým a jednoduchým způsobem kontrolovat, zda se změnil obsah určeného souboru, systémové oblasti disku, popřípadě operační paměti. Je velmi vhodný ke kontrole často používaných programů a důležitých souborů. Lze ho použít například ke kontrole obsahu systémových programů (IO.SYS, MSDOS.SYS a COMMAND.COM operačního systému MS–DOS firmy Microsoft; resp. IBMIO.COM, IBMDOS.COM a COMMAND.COM systému PC–DOS firmy IBM) při každém zapnutí počítače. Velmi důležité je i testování změn v operační paměti.

Program pracuje ve dvou různých režimech. V režimu počítání vygeneruje kontrolní součet pro zadaný soubor. Jméno souboru v tomto případě může obsahovat znaky * a ? pro specifikaci více souborů. Kontrolní součty jsou pak postupně spočítány pro všechny soubory, které odpovídají zadané masce (bližší informace je možno nalézt v uživatelské příručce operačního systému). Pokud je jako jméno souboru zadáno klíčové slovo **„.SYSTEM.X“**, kde **X** znamená písmeno označující disk, je vygenerován kontrolní součet systémové oblasti daného disku (klíčové slovo začíná tečkou, aby se odlišilo od jmen souborů).

Pokud je jako jméno souboru zadáno klíčové slovo **„.MEMORY“**, není testována žádná část disku ale operační paměť. V úvahu se berou vektory důležitých přerušení, klíčové údaje z operačního systému, celková velikost paměti a začátek volné paměti. Díky této vlastnosti programu SGUARD je

možno spolehlivě detekovat i neznámé typy virů, jejichž přítomnost v systému se musí v uvedeném testu projevit. Tato funkce je velmi vhodná na začátku souboru AUTOEXEC.BAT. Falešný poplach může způsobit pouze změna konfigurace počítače (například přidání nějakého ovladače do souboru CONFIG.SYS). Protože se v tomto testu projeví každý rezidentní program, je vhodné do souboru AUTOEXEC.BAT napsat řádek:

```
SGUARD .MEMORY 0
```

Při prvním spuštění počítače po této změně ohlásí program SGUARD chybu kontrolního součtu včetně skutečně zjištěné hodnoty. Tu je pak třeba zadat pro spouštění místo hodnoty 0.

V režimu verifikace porovnává právě platný kontrolní součet daného souboru se součtem, který je specifikován uživatelem na příkazovém řádku. Uživatel může na příkazovém řádku specifikovat více dvojic [soubor suma] pro kontrolu více souborů. Pokud právě platný součet odpovídá součtu, zadanému uživatelem, program je normálně ukončen s návratovým kódem 0, který je předán operačnímu systému. Pokud je zjištěna nějaká nesrovnalost, je tato nesrovnalost spolu se zvukovou indikací vypsána na obrazovce a program je ukončen s návratovým kódem 1. Pokud je jako jméno souboru zadáno klíčové slovo **„.SYSTEM.X“**, kde **X** znamená písmeno označující disk, je porovnán následující součet s právě platným součtem systémové oblasti daného disku, při zadání klíčového slova **„.MEMORY“**, je porovnán následující součet s právě platným součtem vybraných oblastí operační paměti.

Program může být spuštěn s parametrem /D, který určuje dávkové zpracování. V režimu počítání pak výstup programu odpovídá syntaxi příkazové dávky (tu lze velmi snadno vytvořit přesměrováním standardního výstupu do souboru s rozšířením BAT tak, jak je to uvedeno v jednom z příkladů). V režimu verifikace pak nehlásí nesrovnalosti na obrazovce, ale pouze pomocí návratového kódu operačního systému, který je vhodný pro další zpracování v příkazové dávce. Návratový kód může být v dávkách testován pomocí příkazu IF ERRORLEVEL a podle jeho hodnoty mohou být učiněna příslušná opatření. Program SGUARD vrací návratový kód

roven nule v případě, že všechny kontrolní součty souhlasí, a roven jedné v případě, že alespoň jeden ze součtů nesouhlasí.

Chování programu SGUARD je možno částečně ovlivnit nastavením proměnné environmentu **AVAST**, která umožňuje určit kód výpisu. Nastavení této proměnné může být následující:

```
SET AVAST=[K|L|N][S]
```

kde K, L a N určují kód výpisu a S znamená potlačení zvukových varování.

Způsob spuštění programu

```
SGUARD [/H]
SGUARD [/K][/L][/N][/D] maska
SGUARD [/K][/L][/N][/D] soubor1 suma1 [soubor2
  suma2 [....]]
```

Přepínač /H či /?

Program SGUARD vypíše návod na použití a ukončí svoji činnost.

Přepínač /D

Tento přepínač umožňuje uživateli specifikovat, že program SGUARD má pracovat s výstupem pro dávkový režim (viz výše).

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v kódu „MJK“ (kód bratrů Kamenických).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v kódu PC Latin 2.

Přepínač /N

Tento přepínač určuje, že veškerý text bude zobrazen bez diakritických znamének.

Parametr: maska

Toto je obecná specifikace jména souboru pro režim počítání. Pokud je jako jméno souboru zadáno klíčové slovo „.SYSTEM.X“, kde X znamená písmeno označující disk, je vygenerován kontrolní součet systémové oblasti daného disku. Při zadání klíčového slova „.MEMORY“ je vygenerován kontrolní součet vybraných oblastí operační paměti.

Parametry: soubor1 suma1

Toto je specifikace dvojice [soubor,suma] pro režim verifikace. Pokud je jako jméno souboru zadáno klíčové slovo „.SYSTEM.X“, kde X znamená písmeno označující disk, je verifikována systémová oblast daného disku. Při zadání klíčového slova „.MEMORY“ je verifikována operační paměť.

Návratové kódy

Jak již bylo řečeno, program SGUARD je možno spouštět v režimu verifikace s parametrem /D. Program pak hlásí nesrovnalosti pouze pomocí návratového kódu operačnímu systému. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce pomocí příkazu IF ERRORLEVEL. Návratový kód programu SGUARD může nabývat pouze následujících hodnot, které mají tento význam:

0 žádná změna nezjištěna, všechny kontrolní součty souhlasí,

1 detekována změna v alespoň jednom zadaném kontrolním součtu.

99 program vypisoval návod na použití.

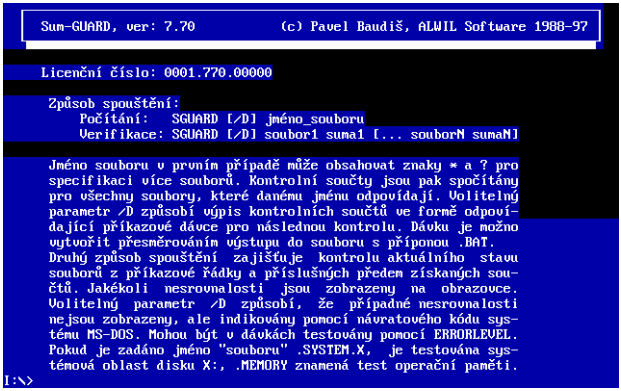
Takto definované návratové kódy je možno použít především v příkazových dávkách pro jejich větvení při zjištění viru. Způsob využití návratového kódu a příkazu IF ERRORLEVEL je zřejmý z následující ukázky:

```
..
sguard c:\io.sys 12345 c:\msdos.sys 67890
if errorlevel 1 goto změna
rem ** testovaný soubor je v pořádku **
..
:změna
echo  Pozor: systém byl modifikován!! nutno
  prověřit!
..
```

Příklady použití

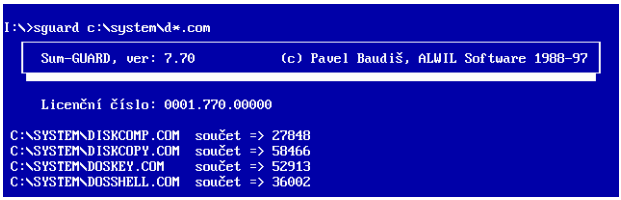
SGUARD /?

zobrazí jednoduchou nápovědu programu SGUARD:



SGUARD *.COM

spuštění programu v režimu počítání, jsou vygenerovány kontrolní součty všech programů typu COM v právě platném adresáři a zobrazeny na obrazovce:

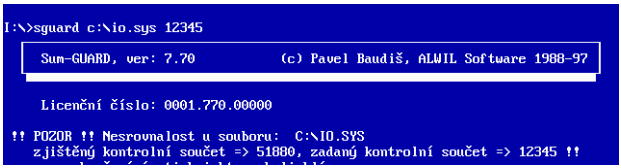


SGUARD /D C:*.* >CHECK.BAT

spuštění programu v režimu počítání, je vytvořena příkazová dávka CHECK.BAT vhodná pro testování všech souborů v hlavním adresáři disku C:.

SGUARD C:\IO.SYS 12345

spuštění programu v režimu verifikace, je spočítán právě platný kontrolní součet souboru IO.SYS a porovnán se součtem, který je na příkazovém řádku (12345). Případný rozdíl je zvukově indikován a zobrazen na obrazovce:



SGUARD /D .MEMORY 55932 .SYSTEM.C 26775 C:\IO.SYS 46514 C:\MSDOS.SYS 51716 C:\COMMAND.COM 58487

spuštění programu v režimu verifikace, jsou spočítány právě platné kontrolní součty systémové oblasti a specifikovaných souborů a porovnány se součty, které jsou zadány na příkazovém řádku. Případný rozdíl je díky přepínači /D indikován pouze pomocí návratového kódu.

Alter–GUARD

Druhým programem je AGUARD (Alter–GUARD, hlídač změn). Tento program provádí v principu podobnou činnost jako předchozí SGUARD, je však mnohem komplexnější. Také jeho možnosti jsou bohatší. Při prvním spuštění si v hlavním adresáři daného disku vytváří vlastní databázi, datový soubor se jménem AGUARD.DAT (na síťových discích je tento soubor uložen do adresáře \AVAST!), do kterého ukládá veškeré informace o systémových oblastech disku a o hlídaných souborech. Do této databáze si kromě jména souboru ukládá i jeho atributy, velikost, datum a čas poslední modifikace a pomocí několika kontrolních součtů i informaci o jeho obsahu. Při každém následujícím spuštění porovnává právě platný stav všech uvedených položek s údaji v databázi,

a tak je schopen zjistit veškeré modifikace systémových oblastí i hlídaných souborů. Nakonec vypíše seznam všech souborů, které byly od poslední aktualizace databáze modifikovány, které jsou navíc (nové soubory) a které naopak chybí (smazané). Uživatel má možnost selektivně určit, které z těchto souborů mají být v databázi aktualizovány. Některé změny programů mohou být legální: například nová verze programu, smazání již nepotřebného programu. Legální změnou programu může být i jeho vlastní modifikace, kterou některé programy provádějí při ukládání své konfigurace (např. LIST, LapLink III, WordPerfect 4.2, Fastlynx, Sourcer). Díky tomuto programu tak může uživatel snadno zjistit, které soubory byly změněny (ať už díky virům či jinému způsobu poškození dat).

Program AGUARD však umí mnohem více. Je schopen detekovat i známé druhy virů mezi modifikovanými či novými soubory a má dokonce schopnost odstranit viry obecnou cestou (bez znalosti podstaty viru) a obnovit původní soubory. S těmito schopnostmi se AGUARD stává **nejdůležitějším a nejmocnějším prostředkem** antivirového souboru AVAST!.

Program AGUARD je obecným programem, který umožňuje při správném používání včas indikovat přítomnost virů v počítači a jejich odstranění. Je však účinný nejen proti virům, ale také proti jakémukoli jinému poškození dat.

Program AGUARD je schopen rozpoznat disk, který je komprimován programem Stacker. V tom případě není prováděn test zaváděcího sektoru, protože se nejedná o skutečný sektor disku ale o fiktivní sektor programu Stacker, který se navíc průběžně mění. Zpráva o přítomnosti Stackeru je zobrazena na tři sekundy na obrazovce, poté program pokračuje normálně v další činnosti. Pokračování je možno urychlit stisknutím libovolné klávesy.

Chování programu AGUARD je možno částečně ovlivnit nastavením proměnné environmentu **AVAST**, která umožňuje určit kód výpisu programů AVAST, AGUARD, LGUARD a SGUARD a potlačit pípání u programů AGUARD a LGUARD. Nastavení této proměnné může být následující:

SET AVAST=[K|L|N][S]

kde K, L a N určují kód výpisu a S znamená potlačení zvukových varování.

Program AGUARD je schopen zpracovávat data i na extrémně velikých discích. Pro takové disky však vyžaduje dostatek paměti typu XMS, jinak může dojít k chybovému hlášení. Implicitní nastavení je možné modifikovat přepínačem /B[xx]. AGUARD je schopen rozpoznat, zda běží pod Windows NT, a pak netestuje systémovou oblast.

Upozornění:

AGUARD a AGW mají změněnou strukturu databáze, která není kompatibilní s předchozí. Doporučujeme naposled zkontrolovat soubory pomocí předchozí verze a pak vytvořit novou databázi.

Způsob spuštění programu

```
AGUARD /H
AGUARD [[d:\]cesta][.][/E[ext1[;ext2;..]]][/D]
   [/S][/A][/R][/F][/C][/C][/P][/O][/T][/B[xx]][/
   K][/L][/N]
```

Přepínač /H či /?

AGUARD vypíše **vícestránkový návod** na použití a ukončí svoji činnost.

Parametr d:\cesta

Tento parametr umožňuje uživateli specifikovat **disk a adresář**, jehož soubory mají být testovány. Je–li tento parametr vynechán, jsou testovány soubory v hlavním adresáři právě platného disku.

Parametr d:\cesta\soubor

Při specifikaci kompletního jména souboru AGUARD otestuje samostatný soubor. Soubor musí existovat!

Parametr .

Tento parametr umožňuje uživateli specifikovat, že bude **testován právě platný adresář na právě platném disku**.

Parametr *:

Tento parametr umožňuje uživateli specifikovat, že budou **testovány všechny lokální pevné disky**.

Parametr #:

Tento parametr umožňuje uživateli specifikovat, že bude **testovány všechny síťové disky.** Program hlásí chybu, pokud je zadán parametr #: a není nalezen žádný síťový disk.

Přepínač /E

Tento přepínač umožňuje uživateli specifikovat **rozšíření (file extensions)** testovaných souborů. Může být specifikováno až 10 různých rozšíření, oddělených středníkem. Rozšíření mohou obsahovat znaky ? a * pro zadání masky (více souborů najednou). Je–li tento přepínač vynechán, jsou testovány soubory s rozšířením COM, EXE, BAT, SYS, BIN, OV? a VPS. Pokud chcete testovat všechny soubory, můžete použít parametr /E*.

Přepínač /D

Tento přepínač určuje, že **nebudou testovány soubory podadresářů** daného adresáře. Je–li tento přepínač vynechán, jsou testovány kromě souborů daného adresáře i soubory ve všech jeho podadresářích.

Přepínač /S

Tento přepínač určuje, že zjištěné nesrovnalosti **nebudou indikovány pípnutím**. Implicitně jsou všechny nesrovnalosti i čekání na vstup uživatele zvukově indikovány.

Přepínač /A

Tento přepínač určuje, že změna **archivního bitu** testovaných souborů není významná. Archivní bit slouží zálohovacím programům pro určení změny programu (při zálohování ho vynulují a při dalším spuštění testují, zda je nulový; v tom případě není archivace provedena). Tento bit nemá jinak žádný význam, implicitně je však testována změna všech atributů hlídaných souborů.

Přepínač /R

Tento přepínač určuje, že program bude pracovat v **režimu Report**. Probíhá pouze kontrola daných souborů, ale není možno provést aktualizaci databáze.

Přepínač /F

Tento přepínač určuje, že při testování **se nemá provádět kontrola obsahu** souborů pomocí kontrolních součtů. Protože pro kontrolu obsahu je nutno číst všechny testované soubory, může pro velký objem dat trvat tato činnost dlouho, tato volba umožňuje velmi rychlou kontrolu všech položek adresáře (atributy, datum a čas, velikost). Není možno provést aktualizaci databáze na disku.

Přepínač /C

Tento přepínač určuje, že se provede **rychlé testování integrity**, při kterém je testován obsah jen těch souborů, u kterých se změnila některá ze základních položek: datum, čas, atributy či velikost. Výhodou proti rychlému testování (/F) je to, že je možno aktualizovat databázi.

Přepínač /G

Tento přepínač určuje, že se provede automatická obnova infikovaných souborů (funguje jako výše uvedené Ctrl–R).

Přepínač /P

Tento přepínač určuje, že program pracuje **plynule**, bez zásahů uživatele.

Přepínač /O

Tento přepínač určuje, že v právě platném adresáři mají být vytvořeny dva textové soubory, které obsahují **výpis obsahu databáze**. První z nich se nazývá AGUARD–X.ALL a obsahuje údaje o všech souborech, uložených v databázi, druhý se jmenuje AGUARD–X.DIF a obsahuje údaje o všech změnách mezi stavem uloženým v databázi a stavem zjištěným na disku. Pokud nebyla zjištěna žádná změna, druhý soubor není vytvořen. Písmeno X v názvu souboru je nahrazeno jménem testovaného disku.

Přepínač /T

Tento přepínač určuje, že všechny nové a modifikované soubory budou testovány na přítomnost známých druhů virů (odpovídý stisknutí Ctrl a T ve výsledkovém menu programu AGUARD).

Přepínač /X

Tento parametr umožňuje netestování systémové oblasti disku, což může být užitečné při testování integrity souborů přenesených elektronicky např. mezi notebookem a stolním počítačem.

Přepínač /B[xx]

AGUARD umí pracovat s **extrémně velkými disky** (řádově desítky tisíc adresářů a max. 65 000 souborů). Pro práci s adresáři se využívá paměť XMS, která ale může někdy způsobit problémy; proto byl zaveden nový parametr /B[xx], který specifikuje, že budou testovány veliké disky. Číslo xx určuje max. počet adresářů (nutné pro alokaci), pokud není uvedeno, implicitní počet je 6000.

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu „MJK“** (kód bratrů Kamenických).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu PC Latin 2**.

Přepínač /N

Tento přepínač určuje, že text bude zobrazen **bez diakritických znamének**.

Návratové kódy

V okamžiku ukončení činnosti program AGUARD vrátí operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce přikazem IF ERRORLEVEL. Návratový kód programu AGUARD může nabývat pouze následujících hodnot, které mají tento význam:

0 program normálně ukončen, žádná data nezměněna,
1 zjištěna změna dat, ale databáze nebyla aktualizována,
2 zjištěna změna dat a databáze byla aktualizována,
3 program přerušen uživatelem,
4 při práci došlo k chybě,
5 úspěšná obnova souboru,
6 neúspěšná obnova,
7 nalezen virus v souboru,
99 program vypisoval návod na použití.

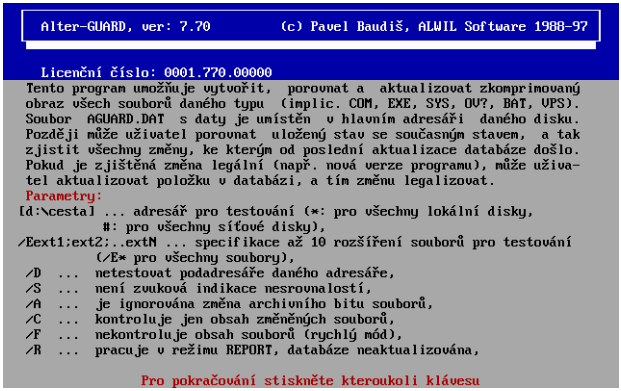
Takto definované návratové kódy je možno použít především v příkazových dávkách pro jejich větvení při zjištění viru. Příkladem může být příkazová dávka CHECK.BAT, která se nachází na distribuční disketě a která demonstruje využití návratového kódu programu AGUARD a test více disků. Způsob využití návratového kódu a příkazu IF ERRORLEVEL je zřejmý i z následující ukázky (význam jednotlivých funkcí je zřejmý i z názvů návěští pro skok):

```
..
aguard c:
if errorlevel 4 goto chyba
if errorlevel 3 goto přerušení
if errorlevel 2 goto změna
if errorlevel 1 goto ne_změna
echo ** na disku c: nebyly zjištěny žádné změny
   dat **
..
```

Příklady použití

AGUARD /?

program vypíše jednostránkovou nápovědu:



AGUARD

spuštění programu pro právě platný disk, testovány jsou všechny soubory typu COM, EXE, BAT, SYS, OV?, BIN a VPS na tomto disku.

AGUARD C:\SYSTEM /D /S

spuštění programu pro adresář SYSTEM na disku C:. Nejsou testovány soubory v podadresářích, nesrovnalosti nejsou indikovány pípnutím.

AGUARD C:\ /E* /F /S

spuštění programu pro velmi rychlou kontrolu všech souborů na disku C:. Není kontrolován obsah souborů, a proto je test velmi rychlý.

AGUARD D:\SUBDIR /Edwg;com;dat;doc /A /F

spuštění programu pro kontrolu souborů s rozšířením DWG, COM, DAT a DOC v adresáři SUBDIR na disku D:, přičemž není kontrolován obsah souborů, pouze položky adresáře, a je ignorována změna archivního bitu.

AGUARD C:\ /O

spuštění programu pro kontrolu souborů s rozšířením COM, EXE, BAT, SYS a OV?. Na právě platném disku jsou vytvořeny dva textové soubory: soubor AGUARD–C.ALL s úplným obsahem databáze a soubor AGUARD–C.DIF, který obsahuje rozdíly, zjištěné při tomto spuštění programu. Tyto soubory pak mohou vypadat následovně:

Soubor AGUARD–C.ALL:

```
AGUARD, verze 7.00 - Právě platný obsah databáze.   01.01.1995 11:11

 Adresář
 Jméno        Délka       Datum       Čas       Atr   Kontrolní součty

Adresář =>  C:\
 COMMAND .COM      23612  07.07.1986  12:00:00  ..RA  8180 0606 C7FB
 CONFIG  .SYS        264  24.09.1995  17:30:08  ...A  B076 6872 48F8

Adresář =>  C:\SYSTEM\
 ANSI    .SYS       1651  07.07.1986  12:00:00  ...A  C9B7 55AF 9B9B
 APPEND  .COM       1725  07.07.1986  12:00:00  ...A  AE92 B8B8 BAAB
 ASSIGN  .COM       1523  07.07.1986  12:00:00  ...A  FA16 FEDA 1F51
 ATTRIB  .EXE       8234  07.07.1986  12:00:00  ...A  2EB2 CACA A74C
 BACKUP  .EXE      23404  07.07.1986  12:00:00  ...A  439A 5A5A 3D26
 NEWFILE .EXE      87443  13.07.1989  09:12:42  ...A  EDAD 4545 3B76
```

Soubor AGUARD–C.DIF:

```
AGUARD, verze 7.00 - Rozdíly zjištěné v databázi.   01.01.1995 11:11

Adresář
Druh změny Jméno        Délka       Datum       Čas       Atr   Kontrol. součty

Adresář =>  C:\SYSTEM\
Změněn z:  BACKUP  .EXE      23404  07.07.1986  12:00:00  ...A  439A 5A5A 3D26
      na:  BACKUP  .EXE      23404  07.07.1986  12:00:62  ...A  5324 245C 112F
Vytvořen:  NEWFILE .EXE      87443  13.07.1989  09:12:42  ...A  EDAD 4545 3B76
```

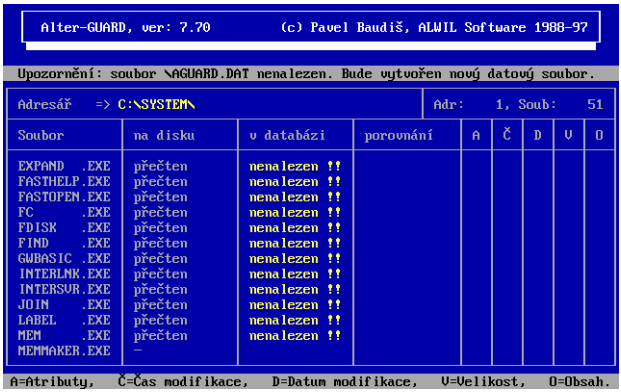
Komunikace programu s uživatelem

Program AGUARD je nejsložitějším z programů souboru AVAST! a nabízí uživateli mnoho možností, proto je v tomto odstavci uveden příklad činnosti programu a jeho komunikace s uživatelem.

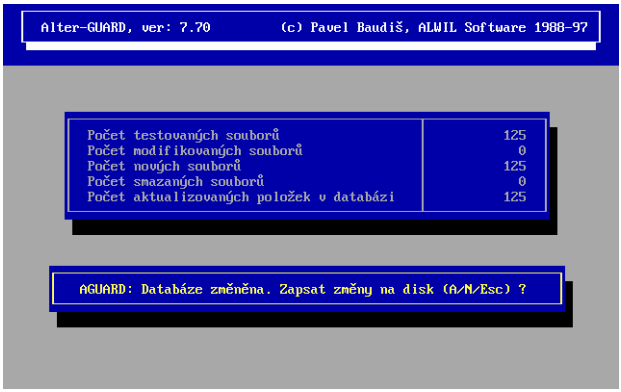
Program spustíme poprvé příkazem:

```
AGUARD C:
```

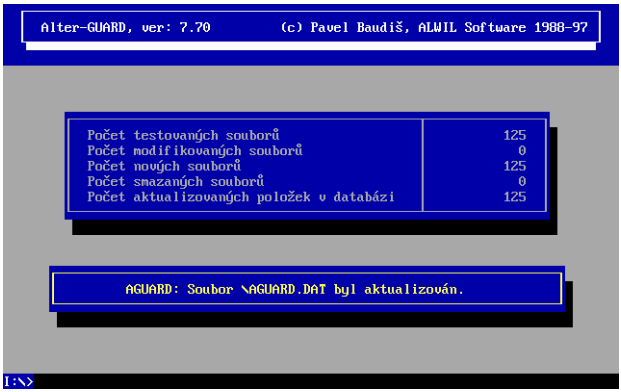
Nenajde–li program v hlavním adresáři daného disku soubor AGUARD.DAT, vytvoří automaticky zcela novou databázi, a v tomto případě není vyžadován souhlas uživatele pro přidání programů do databáze, automaticky jsou do ní zahrnuty všechny soubory, které vyhovují podmínkám na příkazovém řádku (adresář, podadresáře, rozšíření). Soubor AGUARD.DAT má nastaven atribut „READ ONLY“, což znamená, že ho nelze omylem příkazy operačního systému smazat ani modifikovat. Na obrazovce se objeví tato informace:



Z obsahu obrazovky je vidět, že databáze bude vytvořena, u všech souborů je uvedeno, že nebyly nalezeny. Proto ani nebylo provedeno žádné porovnání. Program se zeptá, zda má být databáze uložena na disk:



Zápis do databáze uživatel odsouhlasí stiskem klávesy **A** (**Ano**). O provedené aktualizaci je informován na obrazovce:



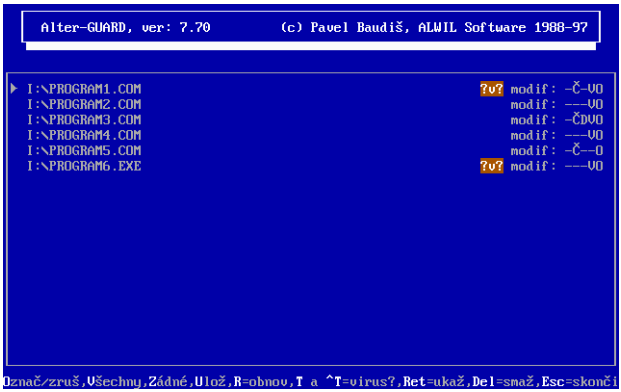
Pokud změníme několik souborů adresáře C:\PROGRAMS a vyzkoušíme reakci programu AGUARD tak, že program spustíme příkazem:

```
AGUARD C:
```

Najde–li program v hlavním adresáři daného disku soubor AGUARD.DAT, přečte jeho obsah a poté kontroluje právě platný stav sledovaných položek jednotlivých souborů s údaji v databázi. Veškeré nesrovnalosti jsou vyznačeny v přísluš–ných sloupcích tabulky na obrazovce. V tabulce je vidět, že všechny soubory byly v databázi nalezeny a mohlo být prove–

deno jejich porovnání. Souhlas je v příslušném sloupci vyznačen **tečkou**, nesouhlas **obdélníkem**. Pokud je zjištěn souhlas ve všech položkách je ve **sloupci porovnání** uvedeno **OK**. Ostatní soubory mají označení **není OK !!** a budou nabídnuty uživateli k dalšímu zpracování.

Pokud nebyly zjištěny žádné změny, je program ukončen. Pokud k některým změnám došlo, objeví se na obrazovce seznam všech souborů, které byly nějakým způsobem modifikovány, které jsou na disku nové a které nebyly nalezeny. Po tomto seznamu je možné pohybovat **ukazovátkem** (trojúhelníkový znak) pomocí **šipek** a kláves **PgUp**, **PgDn**, **Home** a **End**.



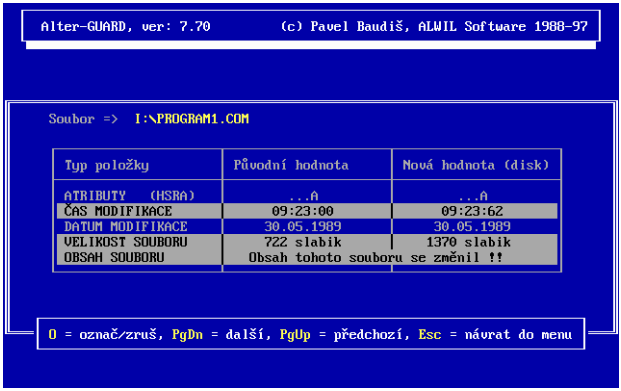
Uživatel může klávesou **O (označ/zruš)** selektivně volit soubory pro aktualizaci databáze (tj. takové soubory, které byly legálně změněny, které jsou na disku nové, nebo které byly smazány). Opětovný stisk této klávesy označení souboru zruší. Klávesa **V (označ vše)** označí pro aktualizaci databáze všechny soubory, klávesa **Z (zruš vše)** zruší označení všech souborů. Pokud nebyl program AGUARD spuštěn v režimu Report, je možno nové a modifikované soubory smazat. Po stisknutí klávesy **Del** je uživatel vyzván, aby potvrdil smazání zvýrazněného souboru. Pokud uživatel vymazání schválí, je daný soubor trvale smazán z disku.

Od verze 7.5 byly doplněny možnosti při vybírání souborů: pro označení všech modifikovaných souborů je to **Ctrl–M**, pro

označení všech nových souborů **Ctrl–N**, pro označení všech smazaných souborů **Ctrl–S** (v anglické verzi Ctrl–D), pro označení všech souborů s pouze změněným archivním bitem **Ctrl–A** a pro označení všech souborů v daném adresáři **Ctrl–F**. Pro vyhledání následujícího adresáře, který obsahuje nějaké změny, lze použít klávesové kombinace **Ctrl–E**. Program po stisknutí F1 v tabulce změn vypíše krátkou nápovědu.

Klávesou **Esc** je možno program AGUARD ukončit. Po stisknutí klávesy **U (Ulož a skonči)** se provede aktualizace všech označených souborů v databázi (položky modifikovaných souborů jsou aktualizovány, položky nových souborů jsou přidány do databáze a položky smazaných souborů jsou v databázi zrušeny).

Po stisknutí klávesy **Enter** jsou pro vybraný soubor zobrazeny všechny sledované položky jednak z databáze a jednak ty, které právě platí. Všechny změny jsou vyznačeny inverzním zobrazením. Pokud jsme umístili ukazovátko (trojúhelníkový znak) například na soubor PROGRAM1.COM a stiskli klávesu Enter, dostali jsme na obrazovce tuto informaci:



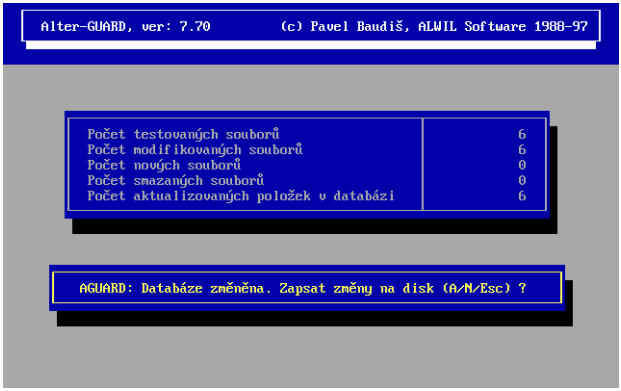
Pro každý modifikovaný soubor je z této informace vidět druh změny. Pro případ napadení souboru virem má obzvlášť velký význam rozdíl délek původního souboru a jeho modifikované verze. Tento rozdíl je pro mnohé viry charakteristický. V našem případě činí rozdíl 648 slabik, což spolu

s časem poslední modifikace (62 sekund) ukazuje na virus 648. O tom, zda je tomu skutečně tak, se přesvědčíme za chvilku.

I v tomto „podrobném“ menu je možno označit soubor pro aktualizaci databáze klávesou **O (označ/zruš)**. I zde opětovný stisk této klávesy označení souboru zruší.

Mezi jednotlivými soubory je možné se pohybovat pomocí kláves **PgUp** a **PgDn**. Z režimu zobrazování jednotlivých položek se vrátíme zpět stisknutím klávesy **Esc**.

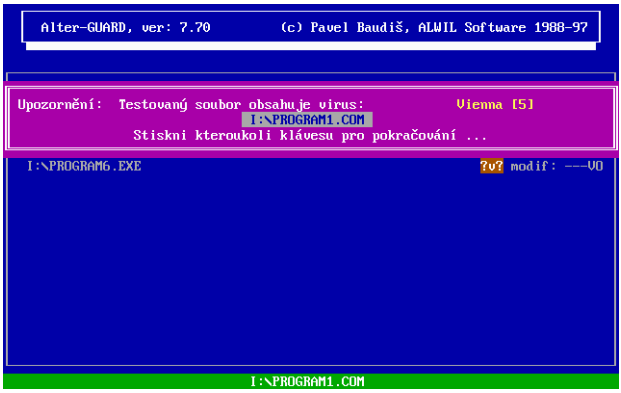
V případě, že považujeme odhalené změny testovaných souborů za korektní, můžeme stisknout klávesu **V (označ všechny)** a klávesu **U (ulož a skonči)**. Uvedeným postupem se databáze změnila a program se zeptá, zda má změny zapsat na disk:



Zápis do databáze uživatel odsouhlasí stiskem klávesy **A (Ano)**. O provedené aktualizaci je informován na obrazovce:

Jak postupovat, pokud pro zjištěnou změnu obsahu databáze není racionální vysvětlení? V první řadě AGUARD umí rozpoznat podezřelé soubory, které mohou obsahovat virus.

Pokud zjistí např. prodloužení souboru bez změny času poslední modifikace, přičemž začátek programu spadá do tohoto prodloužení, vypíše v tabulce změn varování. V tomto případě je pravděpodobné, že došlo k infikaci souborů virem. O tom, je–li tomu skutečně tak, se uživatel může přesvědčit velmi jednoduše. AGUARD totiž nabízí možnost **testování přítomnosti známých druhů virů**. To může být velmi užitečné v případě, že se vaše soubory a programy začnou bez jakékoli příčiny měnit. V okamžiku, kdy program AGUARD zobrazí tabulku se všemi zjištěnými změnami, uživatel může velmi jednoduše otestovat, zda libovolný soubor obsahuje virus, který je znám programům LGUARD a RGUARD, a to pouhým stisknutím klávesy „**T**“ (Testuj, zda je virus). Najednou lze otestovat i více souborů, a to pomocí kláves **„Ctrl T**“. V tomto případě jsou otestovány všechny soubory od právě zvýrazněného až do konce seznamu. Tento test může být kdykoli přerušen pomocí klávesy **Esc**. AGUARD při tomto testování spolupracuje s programem RGUARD. Proto musí být soubory RGUARD.OVL a LGUARD.VPS umístěny ve stejném adresáři, ve kterém je soubor AGUARD.COM. Na následujícím obrázku můžete vidět virus Vienna 648, zjištěný ve výše uvedeném souboru:



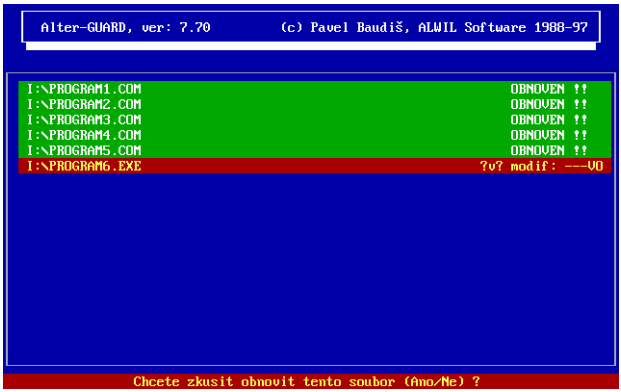
Přítomnost viru v souboru je pak zvýrazněna na obrazovce. Pokud byl nalezen v některém souboru virus, v příslušném řádku je uveden text „**=V!**“. Pokud testování dopadlo dobře,

u příslušného souboru je uvedeno „**Ok!**“. Uživatel má možnost smazat napadený soubor nebo se pokusit o jeho obnovení.

Obecné obnovení infikovaných souborů a odstranění virů je jednou z hlavních předností programu AGUARD. Ten k tomu využívá výhody, které jako program pro hlídání integrity dat má. AGUARD má totiž k dispozici spoustu informací o původním souboru (nové soubory, napadené viry, nemohou být touto metodou obnoveny). AGUARD na požádání (klávesou „**R**“) vyzkouší několik různých metod pro odstranění viru a obnovení původního souboru. Hlavní výhodou je to, že AGUARD je schopen rozhodnout, zda byl úspěšný, tj. zda je soubor **přesně ve stejném stavu**, v jakém byl před napadením. Příkaz „**R**“ není možno použít, pokud jsou použity parametry /F nebo /R nebo pokud je testované médium chráněno proti zápisu. Pro obnovení více souborů naráz. můžete stisknout **Ctrl–R**

Důležitá poznámka:

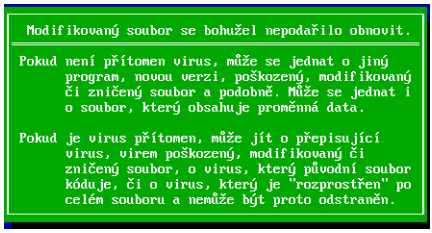
Pokud chcete **obnovit** některé soubory, měli byste **vypnout počítač**, pak ho opět zapnout a zavést systém z **originální systémové** diskety a pak spustit program AGUARD ze **záchranné diskety**, vytvořené při instalaci systému AVAST!. Pak si můžete být jisti, že žádný virus není aktivní a soubory mohou být výše uvedeným způsobem jednoduše obnoveny.



Použitím této metody mohou být odstraněny téměř všechny viry. Přesto existuje několik výjimek. Například přepisující viry zničí obsah původního souboru, takže ten nemůže být rekonstruován a musí být znovu nahrán ze záložní kopie. Také viry, které kódují původní soubor nebo jsou „roztroušeny“ po celém hostitelském programu nemohou být programem AGUARD obnoveny. Tyto typy virů jsou velice vyjímečné, bohužel k nim patří virus One Half.

Na druhé straně je AGUARD nyní **schopen odstranit i nové a dosud neznámé druhy virů**, nepotřebuje k tomu časté aktualizace a je účinný například i proti polymorfním virům, jež jsou namířeny zejména proti vyhledávacím programům.

Pokud AGUARD není schopen obnovit původní soubor, zobrazí následující zprávu:



Program AGUARD neumožňuje přímé odhalení podstaty činnosti viru. Umožňuje včas detekovat změny souborů mezi dvěmi aktualizacemi databáze, způsobené virem. Změny, které byly aktualizovány v databázi, již nemohou být při následujícím spuštění odhaleny. Doporučujeme proto program AGUARD pravidelně spouštět (denně, jedenkrát týdně apod.) a soubor AGUARD.DAT uchovávat odděleně například na disketě. Vždy před spuštěním je nutno datový soubor zkopírovat do hlavního adresáře příslušného disku. Tím je zajištěno to, že nikdo neaktualizoval databázi bez vědomí oprávněné osoby.

Detailnější popis toho, jak postupovat v případě podezření na přítomnost viru můžete najít ve zvláštní kapitole **„Likvidace virů v systému“.**

File–GUARD

Dalším obecným antivirovým programem, který je součástí souboru AVAST! je program FGUARD (File–GUARD, hlídač souborů). Tento program se od předchozích dvou principiálně odlišuje. Je to paměťově rezidentní program (zabírá cca 10,5 KB operační paměti), který v reálném čase hlídá pokusy o modifikaci sledovaných souborů (pokusy o smazání, otevření pro zápis, zápis, přejmenování, zrušení příznaku „READ ONLY“).

Kromě své základní činnosti – hlídání modifikace souborů – je program FGUARD schopen sledovat i případnou destruktivní činnost viru. Umožňuje hlídat pokus o formátování stopy, přímý zápis na disk pomocí DOSu či BIOSu a u počítačů kategorie IBM PC/AT navíc i obsah konfigurační paměti CMOS. Dále umožňuje sledovat pokusy o krokování přerušení 13h, 21h a 40h, což některé viry používají ke zjištění adresy uvnitř systému, kterou pak volají přímo a tím obcházejí antivirovou ochranu. Krokování je umožněno vlastnostmi procesorů firmy Intel a způsobuje to, že po každé vykonané instrukci je předáno řízení obslužné rutině přerušení 1. Běžně této vlastnosti využívají ladící prostředky (DEBUG), lze ji však zneužít i výše uvedeným způsobem. V tu chvíli má totiž takový program téměř absolutní kontrolu nad činností procesoru. FGUARD též umožňuje sledovat změny nastavení vektorů přerušení 13h, 21h, 26h a 40h. Změny těchto vektorů většinou provádějí paměťově rezidentní programy ale i viry, které se instalují v operační paměti.

V případě zjištění pokusu o tento druh činnosti se na obrazovce objeví okénko, ve kterém je zpráva o požadované činnosti a její další specifikace (jméno souboru, číslo formátované stopy, číslo sektoru, clusteru apod.). Uživatel je vyzván, aby potvrdil, zda je prováděná činnost v pořádku (například při mazání souborů či formátování disket). Pokud uživatel určí, že požadovaná činnost v pořádku není, je operace potlačena.

Pokud uživatel chce pouze sledovat provoz počítače a nechce odpovídat na výše uvedené dotazy, je možné použít jiný režim činnosti (tzv. REPORT), při kterém se v pravém horním

rohu obrazovky na minimálně 10 sekund objeví zpráva o tom, že k dané události došlo (například ke smazání souboru, k formátování stopy apod.).

Činnost programu FGUARD může být dočasně potlačena, a to dvojím způsobem. Jednak z příkazového řádku pomocí přepínače, a jednak stisknutím kombinace kláves **„Ctrl 5“** v numerické části klávesnice. V obou případech je pomocí zvukové signalizace indikováno zapnutí (tři vzestupné tóny) a vypnutí (tři sestupné tóny) činnosti programu FGUARD.

Uživatel si sám pomocí přepínačů může zvolit, které činnosti má program FGUARD hlídat (viz dále). Vždy se hlídá zápis do sektoru s tabulkou rozdělení disků a zápis do zaváděcího sektoru pevného disku. Kromě toho si uživatel může zvolit, které typy souborů (pomocí specifikace až deseti rozšíření souboru) budou programem FGUARD hlídány.

Program FGUARD umožňuje odhalit většinu druhů virů již v okamžiku, kdy se poprvé snaží napadnout operační systém, nebo kdy se snaží infikovat další „zdravé“ programy. Tím je velmi usnadněna identifikace tzv. nosičů viru – programů zodpovědných za jejich šíření. Pokud viry pro své šíření nepoužívají služby operačního systému (veškerou práci se soubory si zabezpečují ve vlastní režii, což znamená radikální zvětšení délky jejich kódu) nebo jiným způsobem operační systém obcházejí, nemohou být pomocí programu FGUARD odhaleny. Program FGUARD také může částečně zabránit případné destruktivní činnosti viru (formátování disku, zápis pomocí DOSu a BIOSu, modifikace paměti CMOS).

Program FGUARD je paměťově rezidentní program, který je velmi vhodné spustit v inicializační příkazové dávce systému.

Programu FGUARD je možno zadat soubory, které nemají být hlídány. To je výhodné tehdy, jestliže například některá aplikace vyvolává časté falešné poplachy. Seznam takových souborů je možno uložit do speciálního souboru FGUARD.EXC, který se musí nacházet ve stejném adresáři, ve kterém je vlastní program FGUARD. Při instalaci (prvním spuštění a zavedení do paměti) je pak nutno pomocí parametru /E programu sdělit, že má pracovat s daným souborem výjimek. Do datového souboru FGUARD.EXC se ukládá

seznam jmen nehlídaných souborů tak, že každé jméno (bez zadání adresáře) je umístěno na zvláštním řádku. Jména nesmějí obsahovat znaky „?“ a „*“. Pokud tedy nechci hlídat soubory PROGRAM1 a PROGRAM2, musím zadat:

```
PROGRAM1.COM
PROGRAM2.EXE
```

Na tomto místě je třeba poznamenat, že některé programy otevírají zcela nekorektně soubory pro čtení a zápis i v případě, že jde pouze o jejich čtení. To se týká zejména programů vytvořených pomocí Turbo Pascalu. To samozřejmě vede k „falešným“ poplachům, hlášeným programem FGUARD.

Pro libovolné monitorování lze vybrat jeden z režimů činnosti. U každého přepínače je možno zadat jeden ze tří doplňujících parametrů: znaky „**+**“, „**–**“ či písmeno „**R**“. Znak „+“ označuje aktivní monitorování v interakčním módu, znak „–“ označuje neaktivní (vypnuté) monitorování a znak „R“ označuje monitorování v režimu REPORT. Kromě toho je možno použít i speciální přepínač: /R+ nastaví všechna aktivní monitorování do režimu REPORT, /R– nastaví všechna aktivní monitorování do interakčního režimu.

Program FGUARD automaticky rozpozná instalaci ovladačů sítě Novell a upraví svoji činnost tak, že je schopen testovat i programy, spouštěné ze síťových disků. Pro kontrolu síťových disků na ostatních počítačových sítích je třeba program instalovat do paměti **až po** zavedení ovladačů sítě.

Velmi složitý je problém komunikace mezi paměťově rezidentním programem a uživatelem, zejména pokud právě probíhající program používá některý z grafických módů či pokud pracuje v jiném režimu než reálném (základní režim procesoru 8086). Pokud program FGUARD pracuje v režimu REPORT, v grafických módech signalizuje detekovanou činnost pomocí zvukové indikace. V ostatních případech přepne mód záznamu do textového režimu a po skončení komunikace přepne zpět do původního grafického módu. Program obnoví veškeré nastavení barev, kurzoru apod, ale ne původní obsah grafické obrazovky. Ten je nutno obnovit v příslušném aplikačním programu. Tento jev nenastává v prostředí Windows, pokud používáte program FGW, popsaný dále.

Způsob spuštění programu:

```
FGUARD /H
FGUARD [ext1 [ext2..]][/I+][/F+][/D+][/B+][/C+]
   [/R+][/V+][/S+][/A+][/E][/X][/W][/3+][/K][/L]
   [/N]
FGUARD [ext1 [ext2..]][/I-][/F-][/D-][/B-][/C-]
   [/R-][/V-][/S-][/A-][/E][/X][/W][/3-][/K][/L]
   [/N]
FGUARD [ext1 [ext2..]][/IR][/FR][/DR][/BR][/CR]
   [/VR][/SR][/E][/X][/W]
```

Přepínač /H či /?

Program FGUARD vypíše **návod** na použití.

Parametr ext1 ext2...

Tyto parametry umožňují uživateli zadat až deset různých **rozšíření** souborů, a tak určit, které typy souborů mají být hlídány. Může být specifikováno až 10 různých rozšíření, oddělených mezerou. Rozšíření mohou obsahovat znaky ? a * pro zadání masky (více souborů najednou). Implicitně jsou hlídány soubory typu COM, EXE, SYS, OV?, BIN a VPS.

Přepínač /I

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/I+), pouze oznámené (/IR) nebo neaktivní (/I–) hlídání **formátování stopy disku** (přerušení 13h, 40h). U pevných disků nelze formátování trvale vypnout, je možno ho pouze potlačit do konce programu. Standardní nastavení je I+.

Přepínač /F

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/F+), pouze oznámené (/FR) nebo neaktivní (/F–) hlídání **modifikace specifikovaných typu souborů** (přerušení 21h). Standardní nastavení je F+.

Přepínač /D

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/D+), pouze oznámené (/DR) nebo neaktivní (/D–) hlídání **přímého zápisu pomocí DOSu** (přerušení 26h). U pevných disků nelze trvale vypnout zápis do zaváděcího sektoru, je možno ho pouze potlačit do konce programu. Standardní nastavení je D+.

Přepínač /B

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/B+), pouze oznámené (/BR) nebo neaktivní (/B–) hlídání **přímého zápisu pomocí BIOSu** (přerušení 13h a 40h). U pevných disků nelze trvale vypnout zápis do zaváděcího sektoru a sektoru s tabulkou rozdělení disků, je možno ho pouze potlačit do konce programu. Protože se jedná o fyzické disky, jsou diskety označeny písmeny (A,B) a pevné disky čísly (1,2). Standardní nastavení je B–. V okamžiku spouštění programu Windows by měl být parametr nastaven do neaktivního stavu!

Přepínač /C

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/C+), pouze oznámené (/CR) nebo neaktivní (/C–) hlídání **obsahu paměti CMOS** u počítačů kategorie PC/AT. Pokud je hlídání aktivní, je obsah paměti CMOS periodicky (cca jedenkrát za sekundu) testován a případné změny jsou hlášeny uživateli. Pokud uživatel specifikuje, že změna není legální, je programem FGUARD obnoven původní obsah paměti CMOS. Standardní nastavení je C–.

Přepínač /R

Tento přepínač umožňuje uživateli zvolit, zda bude program FGUARD při zjištění podezřelé činnosti vyžadovat **odpověď** od uživatele (/R–), či zda bude pouze vypisovat zprávu o zjištěné činnosti v pravém horním rohu obrazovky (/R+). Pomocí tohoto

parametru je možno přepnout všechna aktivní monitorování do režimu REPORT či do interakčního režimu. Standardní nastavení je R–.

Přepínač /V

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/V+), pouze oznámené (/VR) nebo neaktivní (/V–) hlídání **změny vektorů přerušení 13h, 21h, 26h a 40h**. Standardní nastavení je V–.

Přepínač /S

Tento přepínač umožňuje uživateli zvolit, zda bude aktivní (/S+), pouze oznámené (/SR) nebo neaktivní (/S–) hlídání **krokování vektorů přerušení 13h, 21h a 40h**. Standardní nastavení je S+.

Přepínač /A

Tento přepínač umožňuje uživateli zvolit, zda bude program FGUARD **aktivní** (/A+) nebo neaktivní (/A–). Pokud není program FGUARD aktivní, je testován pouze pokus o čtení a modifikaci tabulky rozdělení disků a modifikaci zaváděcího sektoru disku. Stejnou funkci má i stisknutí kombinace klávesy **„Ctrl 5“** v numerické části klávesnice. Vypnutí a zapnutí je zvukově indikováno. Standardní nastavení je A+.

Přepínač /E

Tento přepínač umožňuje uživateli zvolit, že **soubory**, jejichž jména (bez adresářů) jsou uvedeny v souboru FGUARD.EXC, **nebudou hlídány**. Pokud parametr není uveden, žádné výjimky se nepřipouštějí.

Přepínač /X

Tento přepínač určuje, že jsou **zákázány** jakékoli **změny parametrů** a režimů činnosti při následujících spouštěních nebo pomocí Hot Key.

Přepínač /W

Tento přepínač určuje, že bude **ignorována instalace sítě Novell**. Ovladače sítě pak mohou být odstraněny z paměti, FGUARD však není v tomto případě schopen monitorovat činnost sítě.

Přepínač /3[+|–]

Tento přepínač umožňuje uživateli specifikovat povolení či zakázání 32–bitového přístupu na disk v prostředí Windows.

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu „MJK“** (kód bratrů Kamenických). Přepínač má smysl pouze při prvním spuštění programu (instalace v paměti).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu PC Latin 2**. Přepínač má smysl pouze při prvním spuštění programu (instalace v paměti).

Přepínač /N

Tento přepínač určuje, že veškerý text bude zobrazen **bez diakritických znamének**. Přepínač má smysl pouze při prvním spuštění programu (instalace v paměti).

Hodnoty jednotlivých přepínačů je možno kdykoli změnit opětovným spuštěním programu FGUARD s jinými parametry (mimo /K, /L a /N).

Návratové kódy

V okamžiku ukončení instalace program FGUARD vrátí operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce příkazem IF ERRORLEVEL. Návratový kód programu FGUARD může nabývat pouze následujících hodnot, které mají tento význam:

0 program byl instalován v paměti,

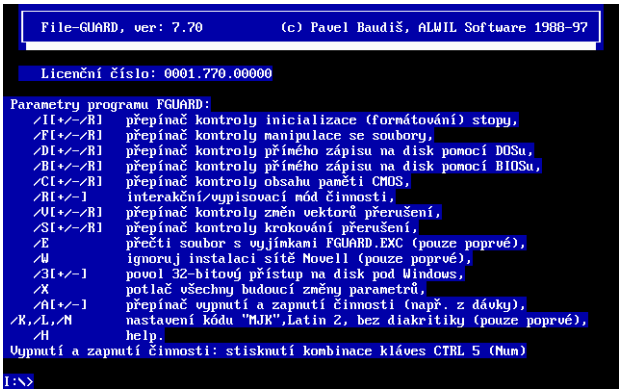
1 program byl již dříve nainstalován v paměti,
2 došlo k chybě, program není možno do paměti instalovat,
99 program vypisoval návod na použití.

Takto definované návratové kódy je možno použít především v příkazových dávkách pro jejich větvení při instalování programu do paměti.

Příklady použití

FGUARD /?

zobrazí jednoduchou nápovědu programu FGUARD:



FGUARD

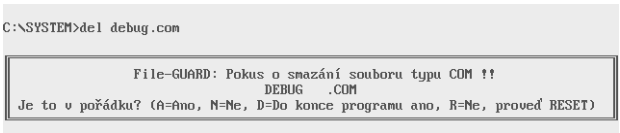
spuštění programu se standardními parametry.

FGUARD /D- /C+

spuštění programu s potlačením hlídání přímého zápisu na disk pomocí funkcí DOSu a s aktivací hlídání paměti CMOS.

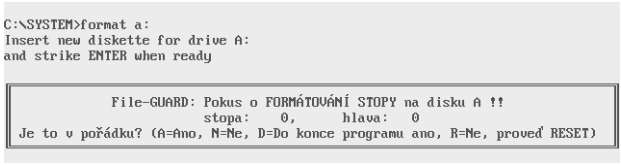
Uveďme si několik příkladů činnosti odhalené programem FGUARD:

a) Smazání souboru příkazem DEL:



V tomto případě odpovíme stiskem klávesy **A (ano)**, pokud chceme soubor vymazat, **N (ne)** v opačném případě.

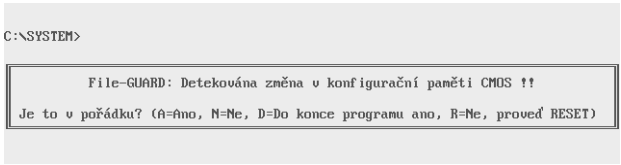
b) Formátování diskety v mechanice A:



V tomto případě je vhodné použít odpověď **D (do konce programu)**, protože jinak by se program dotazoval na formátování každé stopy.

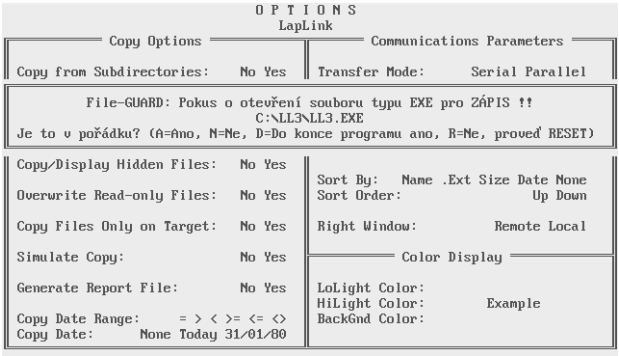
c) Změna obsahu konfigurační paměti CMOS:

Konfigurační paměť CMOS počítače třídy AT obsahuje základní informace o systému a její obsah je měněn programem SETUP. Za normálních okolností ke změně jejího obsahu nedochází.



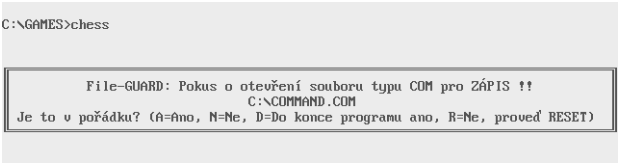
d) Program modifikuje sám sebe:

Některé programy neukládají svou konfiguraci do zvláštního souboru, ale ukládají ji tak, že modifikují samy sebe. Pokus o takovou změnu program FGUARD samozřejmě zachytí. Např. populární komunikační program LapLink III firmy Travelling Software umožňuje modifikovat mnoho parametrů pomocí menu. V okamžiku požadavku na uložení nové konfigurace se přes menu programu LapLink objeví známé okno programu FGUARD:



V tomto případě odpovíme stiskem klávesy **A (ano)**, protože se jedná o změnu legální.

e) Napadení souboru virem:



V tomto případě se uživatel rozhodl poněkud si odpočinout od práce a zahrát si novou hru. K jeho překvapení program chce manipulovat se systémovým programem COM–MAND.COM. Bez instalovaného programu FGUARD by byl systém virem napaden a ze souboru COMMAND.COM by se virus velice rychle rozšířil.

Kromě volby **A (ano)**, **N (ne)** a **D (do konce programu)**, má uživatel k dispozici další volbu **R (ne, proveď RESET)**, pomocí které je znovu zaveden systém počítače (obdoba kom–binace kláves **„Ctrl Alt Del“**). Tuto funkci je možno použít v případě, že by mohlo okamžitě po potlačení šíření viru dojít k další destruktivní činnosti. Uživatel je vyzván, aby do jed–notky vložil originální systémovou disketu a pak vypnul a za–pnul počítač.FGUARD vyžaduje potvrzení operace Reset po–čítače. Resetu je možno zabránit pomocí Alt–N či Alt–A.

Boot–GUARD

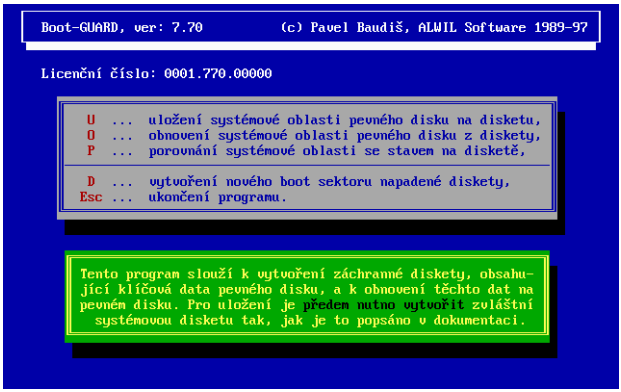
Program Boot–GUARD má v souboru antivirových programů AVAST! poněkud zvláštní místo. Není určen pro denní používání, a pokud vše bude probíhat bez problémů, stačí jej spustit pouze jedenkrát. Přesto má pro ochranu proti počítačovým virům nesmírný význam. Umožňuje totiž uložit kritická místa pevného disku na disketu a později je z této diskety v případě potřeby obnovit. Jedná se o **systémovou oblast disku**, která se skládá ze sektorů s tabulkou rozdělení disků (někdy nazývaných Master Boot Record) a zaváděcích sektorů. BGUARD by měl být určitě spuštěn při vytváření speciální „záchranné“ diskety v rámci instalace programového vybavení AVAST! tak, jak je to popsáno v příslušné kapitole. Pokud dojde na vašem počítači z jakýchkoli důvodů k poškození této oblasti disku (jednou z nejčastějších příčin jsou boot viry, které infikují pevný disk), je možno velmi jednoduchým způsobem původní data na disku obnovit. Tento krok může zcela deaktivovat a odstranit boot viry z pevného disku.

Program BGUARD má i další velmi důležitou funkci. Umožňuje totiž **odstranit boot viry z infikovaných disket**.

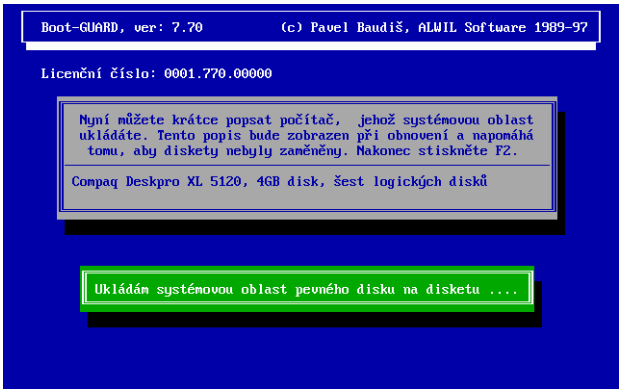
Program BGUARD lze nyní ovládat interaktivně i parametry příkazové řádky a o dalším postupu v dávce rozhodnout na základě návratového kódu.

Interaktivní ovládání programu

Program BGUARD je možné spoustit jednoduchým zadáním jeho jména na příkazové řádce. Další komunikace probíhá interakčně pomocí voleb uživatele. Na obrazovce se objeví následující okno:

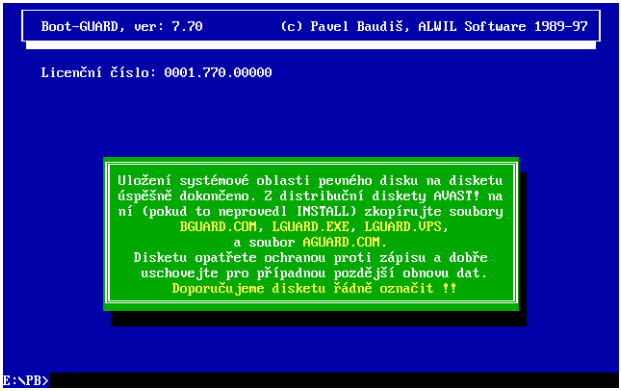


Uživatel má k dispozici tři základní volby: **U** pro **uložení** systémové oblasti disků, **O** pro **obnovení** systémové oblasti disků, **P** pro **porovnání** dat na disketě se současným stavem na pevném disku a **D** pro **vytvoření nového boot sektoru** napadené diskety. Pokud uživatel stiskne klávesu U, program se zeptá, zda chce opravdu provést uložení dat. Pokud na tuto otázku odpoví uživatel kladně, musí zadat jednotku, ve které se nachází předem připravená systémová disketa, jež byla vytvořena například při instalaci souboru AVAST!

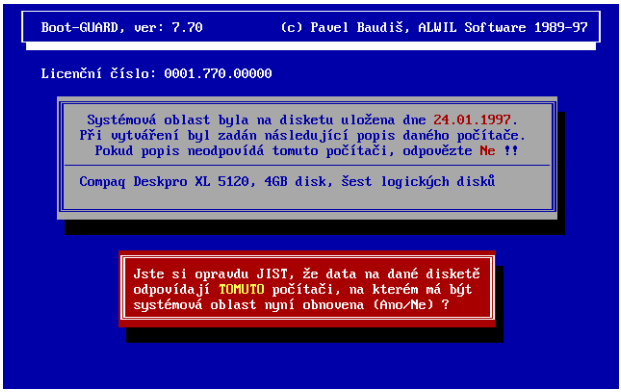


Program BGUARD pak na tuto disketu uloží systémovou oblast disku. Uživatel je vyzván také k zadání stručného popisu ukládaného počítače. To může mít velký význam při ob–

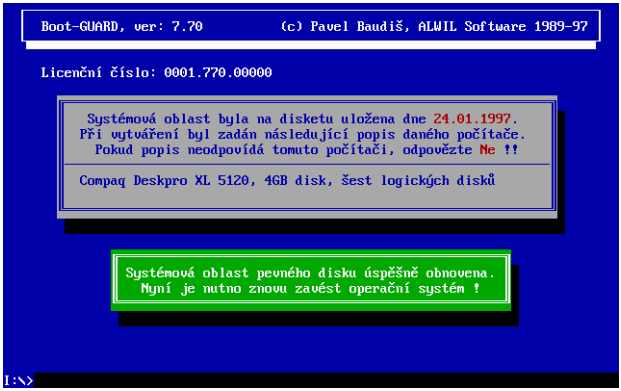
novování dat. Po úspěšném uložení dat na disketu vás vyzve BGUARD k jejímu uschování. Doporučujeme disketu opatřit ochranou proti zápisu, řádně označit a důkladně uschovat. Jelikož se obsah systémové oblasti může u různých počítačů lišit (záleží na konkrétní konfiguraci, typu disku, počtu logických disků a jejich velikosti apod.), měla by pro každý počítač existovat jedna zvláštní disketa – proto výše uvedený popis.



Pokud dojde ke změně systémové oblasti disku (například při výskytu boot viru), je možné data na pevném disku pomocí programu BGUARD z diskety obnovit. Předtím je třeba zavést operační systém z originální systémové diskety nebo z diskety připravené při instalaci. Pak je potřeba ze záchranné diskety spustit program BGUARD a v menu zadat příkaz **O** (obnovení systémové oblasti disku). Program BGUARD si vyžádá potvrzení toho, že má data na pevném disku skutečně přepsat, a pak se ještě zeptá, zda vložená disketa skutečně odpovídá tomu počítači, na kterém mají být data obnovena. Přitom zobrazí popis, jenž byl zadán při vytváření počítače, společně s datem vytvoření či posledního uložení dat.



Jestliže je na počítači instalován aktivní program FGUARD, ohlásí pokus o zápis do sektoru s tabulkou rozdělení disků. Tato činnost je samozřejmě legální, a proto je potřeba zadat **A** (Ano). Pokud máte více fyzických disků jsou obnovena data na všech discích. Poté, co jsou data v pořádku obnovena, je možno zavést systém a pokračovat v činnosti. Pomocí programů SGUARD a AGUARD je možno ověřit, zda jsou data opravdu stejná, jako dříve.



Upozornění

- Pokud změníte konfiguraci počítače, tj. například přidáte nový disk, změníte počet či velikost logických disků, verzi operačního systému a podobně, je **vždy třeba uložit platný stav** na záchrannou disketu! Tato manipulace se nejčastěji provádí programem FDISK. Proto musíte vždy po takové změně spustit program BGUARD!!
- BGUARD byl upraven tak, aby Scan či AVG nehlásily falešný poplach – virus SVC.
- BGUARD je schopen ukládat i nestandardní boot sektory – napíše upozornění a zeptá se, zda má pokračovat či ne. Uložení dat nemůže být provedeno, pokud je na počítači instalován nějaký systém pro ochranu disků před přístupem ze systémové diskety (příkladem může být ochrana LOCKSUP systému SUP z naší produkce).

Třetí funkcí programu BGUARD je **vytvoření nového boot sektoru infikovaných disket**. To je totiž úkon, který nemůže být žádným z prostředků operačního systému dosažen s výjimkou programu SYS, který ovšem kromě přepsání boot sektoru na disketu zkopíruje i systémové soubory, což často není žádoucí. Program BGUARD umí přepsat boot sektor **standardních disket** a tak odstranit boot virus bez jakékoli předem uložené informace. Kód, který do boot sektoru zapíše, může mít navíc i vysoce preventivní účinek. Pokud totiž uživatel zapomene takto „ošetřenou“ disketu v jednotce a pokusí se z ní zavést systém, objeví se následující zpráva:

```
Varovani AVAST!: Nezapominejte vyndavat diskety!!
Muzete tak predejit sireni pocitacovych boot virů.
Nyni vyjmete tuto disketu a stisknete cokoli...
```

Pokud je někdy později taková disketa napadena boot virem a je z ní zaveden systém, je schopna změnu rozpoznat a ohlásit následujícím způsobem:

```
Varovani AVAST!: POZOR!! Boot sektor diskety modifikován!!
Pravdepodobne se jedna o boot virus, ktery je jiz aktivni!
```

Z těchto důvodů je možné a vhodné programem BGUARD upravit všechny datové diskety, které používáte. Může to značně přispět ke snížení rizika napadení boot virem a k eliminaci případných škod.

Upozornění:

- Protože viry často přepisují i důležité parametry diskety, které jsou v zaváděcím sektoru uloženy, umí program BGUARD pracovat pouze se standardními formáty disket (tj. 360 KB a 1,2 MB u disket 5,25 palce, 720 KB, 1,44 a 2,88MB u disket 3,5 palce, stejně jako to provádí program FORMAT). Pokud je disketa zformátována nestandardním způsobem, nebo pokud zvolíte chybný formát, může dojít ke ztrátě dat, na disketě uložených!
- BGUARD je schopen rozpoznat a pracovat i s disketami 2,88 MB.
- Toto ošetření není možno použít na systémových (tj. bootovacích) disketách. Na ně je třeba použít systémový příkaz SYS. Takové diskety by měly být vždy **chráněny proti zápisu!!!**

Přepínače programu BGUARD

Program BGUARD má pouze čtyři možné přepínače, které určují kód pro komunikaci s uživatelem a zpracování disket:

Přepínač /D

Tento přepínač určuje, že bude přímo vyvolána funkce obnovy systémové oblasti infikovaných disket.

Přepínač /F

Tento přepínač určuje, že BGUARD uloží systémovou oblast do souboru, jehož jméno uživatel interakčně zadá.

Přepínač /K

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu „MJK“** (kód bratrů Kamenických).

Přepínač /L

Tento přepínač určuje, že veškerý text bude zobrazen v **kódu PC Latin 2**.

Přepínač /N

Tento přepínač určuje, že veškerý text bude zobrazen **bez diakritických znamének**.

Dávkové spouštění programu BGUARD

Dále uvedené přepínače jsou určeny pro neinteraktivní ovládání programu BGUARD. V tomto případě je na příkazové řádce nutné uvést kompletně požadovanou činnost programu. Doporučujeme využívat tohoto režimu systémovými administrátory ve speciálně navržených dávkových souborech.

BGUARD clean <disketa> <size>

BGUARD vytvoří nový boot sektor diskety. Parametr disketa může být A nebo B, parametr size určuje kapacitu diskety a může nabývat hodnot 360, 720, 1.2, 1.44, 2.88. Použití nesprávné velikosti bude mít za následek ztrátu dat!!!

BGUARD save <disketa> "popis"

Uloží systémové oblasti pevných disků na disketu. Popis může obsahovat údaje o daném počítači. Musí být v uvozovkách!:

BGUARD restore <disketa>

Obnoví systémové oblasti pevných disků z údajů uložených na disketě.

BGUARD compare <disketa>

Porovná systémové oblasti pevných disků se stavem uloženým na disketě.

Pokud jsou tyto parametry použity, není na obrazovce nic zobrazeno a veškerý výstup je realizován pouze pomocí návratového kódu.

Návratové kódy

V okamžiku ukončení činnosti program BGUARD vrátí operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce pomocí příkazu IF ERRORLEVEL. Návratový kód programu BGUARD může nabývat pouze následujících hodnot, které mají tento význam:

1 data na pevném disku byla obnovena,
2 data na pevném disku byla uložena,
3 došlo k chybě při ukládání či načítání dat (disketa),
4 došlo k chybě při ukládání či načítání dat (pevný disk),
5 chyba při práci s pevným diskem,
6 porovnání je v pořádku,
7 porovnání není v pořádku,
99 program vypisoval návod na použití.

Tato stránka je úmyslně prázdná

Programy pro Windows

V poslední době vzrůstá počet uživatelů grafického uživatelského rozhraní Windows. Proto jsme doplnili soubor AVAST! o několik programů, které jsou plnohodnotnými aplikacemi Windows. Tyto programy úzce spolupracují a v několika případech přímo využívají programů pro prostředí DOS.

File–GUARD pro Windows

FGW je program, který v reálném čase hlídá pokusy o modifikaci sledovaných souborů (pokusy o smazání, otevření pro zápis, přejmenování, zrušení příznaku READ–ONLY) během práce systému Windows, dovoluje uživateli interaktivně povolit či zakázat modifikaci nebo, podle přání uživatele, resetovat počítač a umožňuje sledovat stav BOOT sektoru disket.

Při této činnosti program FGW úzce spolupracuje s programy FGUARD a RGUARD pro DOS, jejichž činnost by se bez této spolupráce mohla v systému Windows projevit dost nepříjemným způsobem (například „zamrznutím“ v nejméně vhodný okamžik).

Stručná charakteristika

FGW je program pro systém Windows 3.1 a novější, který má zabudovány některé schopnosti spolupráce se systémem DOS. Pokud je program aktivní, veškeré sledované činnosti programů FGUARD a RGUARD pro DOS vyvolané buď aktivitou Windows (práce se soubory) nebo jakoukoli nelegální činností (například činností virů) jsou programy pro DOS zachyceny a odeslány do systému Windows, kde jsou zpracovány.

DOS a Windows představují dva úplně odlišné systémy, jejichž spolupráce není jednoduchá a není možno v kterémkoli okamžiku z DOSu zavolat program ve Windows. Také některé schopnosti programů pro DOS nemají v chráněném režimu Windows smysl (například sledování změn reálných vektorů přerušení). Proto pokud dojde k tomu, že některý z programů pro

DOS zachytí pokus o sledovanou činnost (modifikace souboru, změna vektorů přerušení, ...) a není možno nebo není zapotřebí zavolat FGW, je sledovaná činnost povolena bez informování uživatele.

V případě zavolání programu pro Windows se na obrazovce objeví okno, které umožní výběr mezi několika variantami odpovědi. Zároveň je potlačena možnost jakékoli práce systému až do okamžiku odpovědi uživatele.

Pokud uživatel chce pouze sledovat provoz počítače a nechce odpovídat na výše uvedené dotazy, lze použít jiný režim činnosti (tzv. REPORT), při kterém se v pravém horním rohu obrazovky na 10 sekund (s přesností 0,1 sekundy a v závislosti na dalších prováděných programech) objeví zpráva blíže specifikující důvod vyvolání programu. Tato zpráva je umístěna v samostatném okně, které je umístěno vždy nad všemi ostatními okny.

Činnost FGW může být na rozdíl od programů pro DOS, potlačena pouze nastavením příslušných přepínačů v hlavním okně. V programu není implementována žádná „horká" klávesa ani zvuková signalizace. Tyto způsoby ovládání nejsou sice v systému Windows zakázány, ale porušují konzistenci obsluhy systému, která je založena na jiných postupech.

Uživatel si sám pomocí přepínačů v hlavním okně programu může zvolit, které činnosti má program FGW hlídat a které z nich nastavit pro hlídání při opuštění systému Windows.

Zde je třeba poznamenat, že FGW je ve sledování jakýchkoli činností plně závislý na programech pro DOS. Pokud některý z programů pro DOS nezachytí signál, nebo zachytí signál falešný (nekorektní otevírání souboru pro čtení), může FGW ohlásit falešný poplach nebo neohlásí poplach žádný.

Instalace a způsob spuštění

Program FGW se skládá ze dvou hlavních částí, souborů AVAST.386 a FGW.EXE. První z nich, tzv. virtuální driver, je program, který obsahuje kritické části nevyhnutelné pro spolupráci s DOSem a tvoří spojovací článek mezi programy pro DOS a FGW. Druhý z nich, soubor FGW.EXE, je standardní

aplikace pro systém Windows, která obsahuje obsluhu vlastní komunikace s uživatelem a zobrazovací rutiny.

Všechny části antivirového balíku AVAST!, které jsou nutné pro práci v systému Windows, jsou automaticky nahrány na pevný disk při instalaci. Vlastní průběh instalace podpory Windows je velice jednoduchá. Stačí kladně odpovědět na příslušný dotaz a instalační program sám nakopíruje potřebné soubory. Pro dokončení instalace je potřeba spustit program AVINST z prostředí Windows.

Při startu Windows bude program FGW automaticky spuštěn, což doporučujeme jako ideální způsob jeho používání. Doporučujeme program ponechat aktivní až do ukončení práce s Windows a nezabývat se jeho ukončováním. Je však nevyhnutné, aby byl v paměti počítače zaveden program FGUARD nebo RGUARD nebo oba společně, jinak se program FGW ohlásí chybové hlášení a nespustí se.

Program FGW potřebuje ke své práci i další soubory: virtuální driver (soubor AVAST.386), soubory s nápovědou k programu a některé knihovny. Tyto soubory automaticky nakopíruje na disk do adresářů, ve kterých mají být tyto soubory umístěny.

FGW může být spuštěn jenom v jedné kopii. Při pokusu o spuštění druhé kopie programu se ozve varovný tón a na obrazovce se rozvine hlavní okno první kopie.

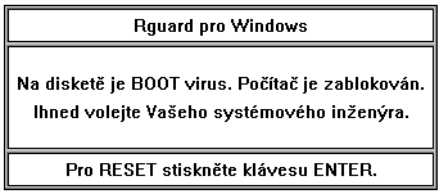
Parametry příkazového řádku

Program při startu prohledá příkazový řádek, a hledá v něm podporované parametry, které mohou začínat znaky „/“ nebo „–“. Při jejich zápisu je možné použít libovolné kombinace velkých a malých písmen. FGW verze 7.0 podporuje dva parametry na příkazové řádce, které se vztahují k sledování činnosti programem RGUARD a umožňují zablokovat pokračování úlohy, která vyvolala reakci programu RGUARD. Tyto parametry jsou:

/SB – zablokování počítače v případě přístupu na disketu, která obsahuje BOOT virus.

/SE – zablokování počítače, pokud je ve spuštěném programu virus.

Při použití některého z parametrů se zobrazí zpráva o zjištěné skutečnosti a systém Windows nepokračuje v další činnosti. Systém však není zcela zablokován a umožní systémovému pracovníku vykonat nezbytná opatření pro odstranění příčiny varování.



Standardní a rozšířený mód

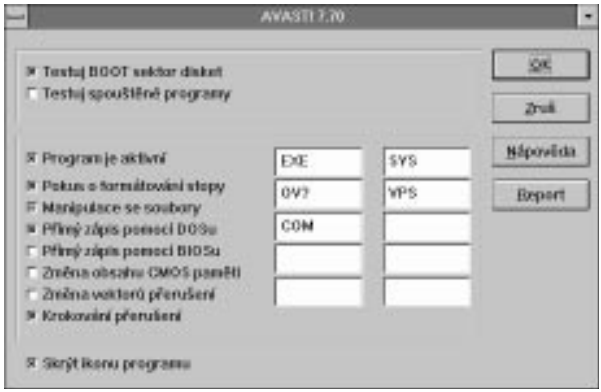
Program FGW podporuje pouze rozšířený mód systému Windows. Ve standardním módu není možné program FGW použít. Při pokusu o jeho spuštění je na obrazovce vypsáno hlášení o této skutečnosti a program okamžitě skončí. Tato skutečnost však neznamená, že se při práci ve standardním režimu musíte vzdát ochrany vašeho systému programy pro DOS. Ochrana je schopna fungovat bez jakýchkoli problémů se sledováním všech činností, které po něm požadujete. Na rozdíl od rozšířeného režimu práce, ve standardním módu při zachycení události program pro DOS přepne obrazovku do textového režimu, počká na odpověď uživatele a po ní vrátí řízení systému Windows. Po návratu do grafické obrazovky systému Windows je však nutné manuálně obnovit stav obrazovky, například zvětšením libovolného okna na maximum a jeho opětovným zmenšením do původní velikosti. V rozšířeném režimu FGW již samostatně obsluhuje sledované události v příslušných oknech a komunikuje s uživatelem způsobem přirozeným systému Windows.

Ovládání programu

Ovládání programu je velice jednoduché. Kdo umí ovládat systém Windows, umí pracovat i s programem FGW. Program se ovládá stejným způsobem jako systém Windows, to znamená myší, klávesnicí nebo jejich kombinací.

Po nahrání do paměti se program zobrazí jako ikona na spodním okraji obrazovky. Pro jakoukoli změnu nastavení musíte vyvolat hlavní okno programu dvojitým „kliknutím“ myši na tuto ikonu. Zobrazí se hlavní okno, ve kterém je možno nastavit všechny potřebné parametry.

Hlavní okno programu je rozděleno do několika částí, které se vztahují k odlišným činnostem programu. Ve vrchní části je oblast pro nastavování parametrů programu RGUARD, ve spodní nastavování parametrů pro FGUARD a při pravém a spodním okraji jsou obecně použitelná tlačítka.



Nastavování parametrů pro RGUARD

Program RGUARD má dvě oblasti činnosti, které mohou být instalovány nezávisle na sobě. Tomu odpovídají dvě tlačítka, které jsou umístěna ve vrchní části hlavního okna programu. Pokud je příslušná část programu RGUARD pro DOS instalována v paměti, je možné příslušné tlačítko nastavovat. Pokud není, je tlačítko společně s popisem zobrazeno jako neaktivní (tmavě šedivá barva) a jeho stav není možné měnit. Aktivní tlačítka je možné nastavit do dvou stavů, které znamenají zapnutí nebo vypnutí sledování nastavované činnosti. Pokud je tlačítko zaškrtnuto, program sleduje nastavenou činnost.

Nastavování parametrů pro FGUARD

Pro nastavování parametrů programu FGUARD slouží většina hlavního okna programu. Základní tlačítko je umístěno hned jako první. Může nabývat dvě hodnoty – globálně zapíná nebo vypíná aktivitu programu FGUARD. Pokud je tlačítko zaškrtnuto, je program aktivní, to znamená, že sleduje požadované činnosti. Pokud zaškrtnuto není, program ignoruje všechny další parametry a je v neaktivním stavu.

Každý přepínač pro sledování činnosti je možno nastavit do některého ze tří stavů. Prázdné tlačítko znamená vypnuté monitorování, označené znamená aktivní monitorování a tlačítko ve třetím stavu (šedivý vzor) znamená REPORT mód. Kromě toho je možno použít speciální tlačítko, které slouží na globální ovládání REPORT módu programu, které přepne všechna aktivní tlačítka do REPORT režimu nebo všechna REPORT tlačítka do aktivního režimu.

Jednotlivá tlačítka můžete nastavit použitím myši nebo klávesnice stejným způsobem, jako v jiných programech určených pro prostředí Windows. Význam jednotlivých položek je blíže popsán v části věnované programu FGUARD pro DOS.

Pro nastavování parametrů programu slouží také deset editačních boxů, do kterých můžete vepsat typy souborů.

Report mód

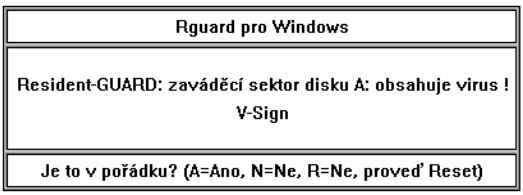
Pokud chcete pouze sledovat provoz počítače a nechcete odpovídat na dotazy, lze použít tzv. Report mód, při kterém se v pravém horním rohu obrazovky asi na 10 sekund (v závislosti na jiné práci) objeví okno se zprávou o některé ze sledovaných činností počítače. Tato zpráva je umístěna v samostatném okně a po dobu své existence je na povrchu všech aktivních programů (není možné ji umístit pod aktivní okno).

Report mód můžete nastavit jednotlivě pro každý typ sledované činnosti nebo globálně pro všechny aktivně sledované činnosti tlačítkem REPORT.

Ovládání odpovědí na varování

Pokud dojde ke sledované události, je na obrazovce vypsáno varování, které je umístěno v samostatném okně. Protože vyvolání okna bylo způsobeno programem pro DOS (to znamená programem pracujícím v reálném módu procesoru 386) je během zobrazování varování přerušena práce systému (nepracuje žádný jiný program) a systém čeká na odpověď uživatele. Pro pokračování v práci musíte stlačit některé písmeno, které je vypsáno ve spodní části okna. Podle vaší odpovědi bude program dále postupovat a sledovanou činnost povolí, zakáže, přepne do REPORT módu nebo resetuje počítač. V horní části varování je zobrazeno jméno programu, který varování vyvolal a v hlavní části je zobrazen bližší popis ohlašovaného varování.

V programu pro Windows je vypuštěna možnost potvrzení „Do konce programu“ z FGUARDu pro DOS, ze zcela zřejmých důvodů víceúlohového charakteru systému Windows. Hlášení pro FGUARD a RGUARD mohou mít následující tvar:



Obsluha varování virtuálním driverem

Virtuální driver, soubor AVAST.386, představuje základní část podpory systému Windows. Jeho hlavním úkolem je zprostředkovat oboustranné spojení mezi FGW a DOSem. V pří-

padě, že program FGW není v systému instalován, virtuální driver přebírá odpovědnost za varování uživatele. Pro jejich zobrazování používá standardní prostředky systému Windows, které jsou pro tento druh komunikace určeny. Příklad takového hlášení můžete vidět, když se pokusíte RESETovat počítač z klávesnice ve Windows. Při zjištění sledované události je AVAST.386 schopen zobrazit varování ve správné jazykové mutaci (stejnou jako má nastavenou program v DOSu) a vypsat srozumitelné hlášení (samozřejmě v textovém módu). Uživatel musí však odpovědět pomocí standardních kláves systému Windows (které jsou rozdílné podle verze systému). V anglické verzi jsou možné odpovědi:

Y	ano, povol, v pořádku,
N	ne, zakaž, není v pořádku,
Esc	reset počítače,
Enter	jako klávesa Y.

V jiných mutacích systému Windows mohou být pro odpověď použity jiné klávesy, ale jejich význam je stejný.

Během zobrazování zprávy je potlačena jakákoli další činnost počítače. Proto v tuto chvíli nepracuje ani myš. Po zadání odpovědi je obnoven obsah grafické obrazovky a přerušená aplikace pracuje podle zadané odpovědi.

Jiné parametry

Program FGW komunikuje v češtině nebo v „cestine“. Pro svoji práci program používá kódování podle tabulky CP1250, která je podporována naprostou většinou dostupných implementací národních prostředí. Použití jazykové mutace je zcela automatické, uživatel se o něj nemusí starat. Rozlišení, zda používat nebo nepoužívat mutaci s diakritikou spočívá ve zjištění aktuálního nastavení systému Windows podle proměnné „sCountry“ v souboru WIN.INI. Instalace češtiny je rozeznána, pokud tato proměnná obsahuje řetězec „CZECH“ nebo „Česk“.

Pokud potvrdíte uložení parametrů tlačítkem OK nebo zrušíte poslední změny tlačítkem Zruš, hlavní okno programu se automaticky zmenší do tvaru ikony.

Tvar ikony programu závisí na tom, zda je sledování činností aktivní nebo ne, a na tom, zda jsou instalovány oba

programy pro DOS (FGUARD i RGUARD). Pravidla pro zobrazování ikony jsou:
písmeno F – instalován program FGUARD pro DOS nebo oba
písmeno R – instalován jenom program RGUARD pro DOS
uzamčený zámek – program je aktivní
odemčený zámek – program není aktivní

Ukončení programu

Program FGW je určen pro nepřetržitou práci během celé doby činnosti systému Windows. Pokud však chcete odstranit program z paměti, můžete to udělat. V tom případě však přijdete o možnost interaktivně měnit jeho nastavení. Veškeré sledování činností nastavené při ukončení programu bude aktivní i nadále a program pro výpis hlášení používá systémové hlášení ve tvaru, který můžete vidět například při pokusu o RESET systému Windows.

Seznam zpráv, varování chyb a dotazů.

Nekompatibilita verzí. Program není schopen pracovat z důvodu nekompatibility s podpůrnou knihovnou (AVAST.386).

FGW potřebuje pro svou práci knihovnu, která je dodávaná s používanou verzí EXE souboru nebo, v některých případech, můžete novější verzi knihovny. Aktuálně instalovaná verze není s programem FGW kompatibilní. Chyba byla způsobena nedokončenou instalací nebo manipulací s nainstalovanými soubory. Opakujte instalaci.

Program není instalován. – v paměti počítače není FGUARD nebo RGUARD pro DOS. – programy FGUARD nebo RGUARD a FGW nejsou vzájemně kompatibilní. Ukončete systém Windows a spusťte FGUARD nebo RGUARD.

Pro správnou práci programu FGW je nutno mít v paměti počítače program FGUARD, RGUARD nebo oba programy společně. Pokud není žádný

z nich instalován, FGW nemůže pracovat. Dalším důvodem může být nekompatibilita verzí, která může být způsobena jenom nesprávnou instalací systému.

Interní chyba DPMI. Nemohu alokovat struktury nutné pro přístup k datům. Program není schopen pracovat. Doporučuji ukončit práci ve Windows.

Program FGW zjistil chybu při práci s velice citlivými strukturami chráněného režimu Windows. Jedinou smysluplnou reakcí je uložení všech dat na disk a ukončení systému Windows.

Interní chyba při změně dat. Zobrazovaná data neodpovídají datům, které jsou brány do úvahy při chránění systému.

Program FGW zjistil chybu při ukládání změn do interních dat rezidentních programů DOSu. Je velké nebezpečí, že uložená data přepsala důležité části jiných programů a může dojít k zablokování počítače.

Chyba inicializace programu. Není volný žádný časovač, který je nutný pro práci. Ukončete některý program a zkuste znova.

Program FGW potřebuje pro svou práci časovač, kterých není neomezeně mnoho. Bez volného časovače není možná práce programu.

Chyba při vytváření REPORT okna. Hlášení nebude zobrazeno.

Program FGW nemůže z nějakých důvodů vytvořit okno s REPORT hlášením. Chyba vznikla v systému Windows.

Chyba alokace paměti. Nemohu alokovat paměť DOSu. Sledování spuštěných programů je vypnuto.

Program FGW potřebuje pro svou práci alokovat paměť na lineárních adresách, které odpovídají

reálnému režimu práce procesoru. Tato paměť není velká, ale nebylo možné ji alokovat.

Spouštěné programy nebudou testovány. Knihovna pro jejich testování (AWANTI.386) není instalována.

Pro antivirové testování je nutná instalace podpůrné knihovny AWANTI.386. V případě, že není instalována, nebo se její instalace nepovede, není možné testovat spouštěné programy.

Chyba detekce rozšířeného módu. Program není schopen pracovat v jiném módu. Ukončete Windows a použijte příkaz 'WIN /3'.

Program FGW je schopen pracovat pouze v rozšířeném režimu práce Windows 3.1 nebo lepších. Pokud není tento režim aktivován, program FGW se nespustí.

Locate-GUARD pro Windows

LGW je vyhledávací antivirový program (typu „scan"), který je určen výhradně pro použití v systému Windows. Program umí vyhledat všechny viry a je funkčně stejný jako program LGUARD pro DOS. Oba umějí nalézt velké množství známých počítačových virů včetně mnoha mutací a polymorfních druhů.

Program LGW je primárně určen pro nepřetržité monitorování systému na kterém byl spuštěn, ale program je samozřejmě možné používat i na pravidelné nebo nepravidelné testování Vašeho počítače bez nutnosti ponechávat ho po celou dobu v činnosti.

Program je implementací originálního programu Lguardu pro DOS do prostředí operačního systému Windows s využitím množství zlepšení a výhod, který tento systém nabízí. Zároveň však zaručuje přesnou kompatibilitu programu na úrovni počtu a druhů nalezených virů při použití stejných parametrů v obou systémech. Postup testování je principiálně stejný, ale vlastní implementace programu používá všech výhod procesorů 80386, pro který je LGW navržen.

Program je navržen tak, aby v co nejmenší míře blokoval ostatní činnost počítače, a až jako druhé hledisko byla brána jeho velikost a spotřeba paměti. Program neustále monitoruje činnost myši a celého systému. Zjištěné prodlevy využívá k vlastní práci, takže uživatel prakticky nemůže zjistit žádné zdržení nebo prodlevy ostatních programů.

Instalace a způsob spuštění

LGW se instaluje společně s ostatními programy antivirového balíku AVAST! instalačním programem, který je součástí dodávky. Instalaci pro Windows provede program AVINST, který vytvoří skupinu AVAST!, z níž je možno program spustit.

Pro svoji práci program používá stejný datový soubor (LGUARD.VPS) s definicemi virů, stejně jako program LGUARD pro DOS. Tento soubor musí být umístěn ve stejném adresáři, jako vlastní výkonný program. Program se spouští stejným způsobem, jako všechny ostatní programy pro Windows. Program nerozeznává žádné parametry příkazové řádky. Pro uchovávání pracovních parametrů používá stejný konfigurační soubor (AVAST!.INI) jako ostatní programy pro Windows firmy ALWIL Software. Pokud tento soubor neexistuje, program ho při prvním spuštění vytvoří v tom adresáři, ze kterého byl spuštěn.

V závislosti na nastavených parametrech může program startovat ve dvou režimech: v popředí (v normálním okénkovém režimu) nebo v pozadí (jako ikona). Podrobnější vysvětlení obou režimů naleznete v popisu parametrů programu.

LGW může být spuštěn jenom v jedné kopii. Při pokusu o spuštění druhé kopie programu se ozve varovný tón a na obrazovce se rozvine hlavní okno první kopie.

Co je možné programem LGW testovat

Program LGW umožňuje otestovat všechny části vašeho systému jednu za druhou nebo samostatně podle zvolených parametrů. Pro účely testování program rozeznává čtyři oblasti:

- **operační paměť systému**,
- **sektor s tabulkou rozdělení (DPT) pevných disků**,

– **zaváděcí (BOOT) sektor jednotlivého disku**,
– **soubory na jednotlivém disku**.

Každou z uvedených částí je možné testovat jednotlivě, nebo je možné určit, že program bude opakovaně testovat všechny části za sebou. Pokud si zvolíte první možnost, program otestuje vámi vybranou oblast systému a testování ukončí. Pokud si zvolíte druhou možnost, bude testování probíhat cyklicky přes všechny části systému. Navíc je možno určit, od které oblasti testování začne. Vlastní průběh bude následující:

– paměť
– DPT
– disk C:
– BOOT sektor
– soubory
– disk D:
– BOOT sektor
– soubory
– ...
– paměť

a tak stále dokola. Kromě toho je možno určit, že program otestuje všechny podadresáře daného adresáře.

Paměť systému

LGW testuje 1024+64 KB operační paměti, která začíná na lineární adrese 0. Je to paměť, ve které se nachází operační systém DOS, všechny paměťově rezidentní programy a kam se ukládají kritická data systému Windows, která musí být z DOSu přístupná. Pokud máte (a určitě máte) víc paměti, tato není programem testována. Tuto paměť nedokáže žádný známý virus použít ani se v ní šířit.

Pokud používáte okno DOSu, je jeho paměť emulována ve dvou hlavních částech. Oblast společná všem oknům DOSu ve Windows je oblast, která obsahuje DOS a rezidentní programy instalované před spuštěním Windows. Druhá oblast je vyčleněna z adresového prostoru Windows a obecně se nenachází v prostoru lineárních adres pod 1 MB. Tuto druhou část paměti okna DOSu program netestuje. Proto pokud v ní spustíte zavirovaný program, LGW nemusí zjistit virus v paměti.

DPT pevných disků

Program je schopen testovat pouze dva lokální pevné disky připojené k systému standardním způsobem. Pokud ve vašem systému nejsou instalovány dva pevné disky, program to rozezná, a sleduje pouze jeden pevný disk. LGW testuje DPT maximálně dvou pevných disků najednou před testováním BOOT sektoru disku C:.

BOOT sektor jednotlivých disků

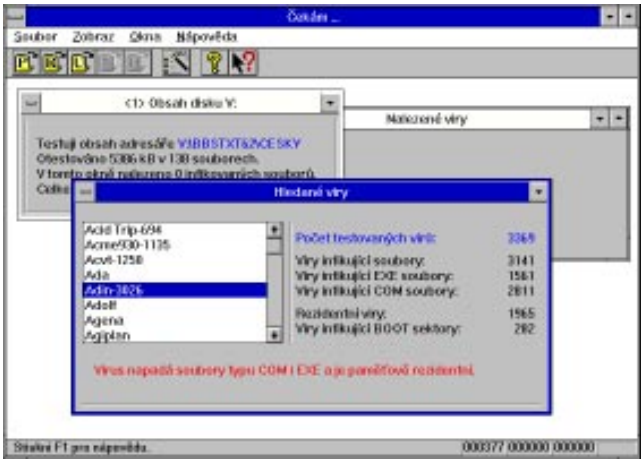
LGW testuje zaváděcí (BOOT) sektor každého lokálního disku před testováním souborů na tomto disku umístěných. Program netestuje BOOT sektor pro RAM disky.

Soubory na jednotlivých discích

LGW testuje soubory na každém disku podle nastavení jednotlivých parametrů. Program je schopen testovat soubory na všech discích, které rozezná operační systém, to znamená i na vzdálených discích (Novell, ...). Program normálně netestuje soubory na lokálních discích CD–ROM, ale uživatel může o jeho testování požádat.

Okna programu

LGW je tzv. MDI aplikace, to znamená, že v hlavním okně může být zobrazeno více dceřiných oken s různým účelem nebo různým obsahem, která jsou naprosto nezávislá. Program LGW umožňuje otevřít libovolný počet samostatných oken (je zde zajisté omezení volnou lokální pamětí programu, ve které se uchovávají datové struktury pro jednotlivá okna) různých druhů. Jednotlivé druhy oken jsou následující:



Pracovní okno
okno, ve kterém probíhá testování vybrané části systému,

REPORT okno
okno, které zobrazuje výsledkový (REPORT) soubor,

Uživatelské definice
okno, ve kterém můžete editovat definice uživatelských virů,

Nalezené viry
okno se seznamem nalezených virů,

Hledané viry
okno se seznamem virů, které program rozeznává.

Z těchto pěti druhů mohou být některá otevřena pouze v jedné kopii. Počet pracovních oken je omezen pouze množstvím právě volné **lokální paměti** (ne celkové paměti systému) a při normálním používání systému se tento počet pohy–

buje v rozsahu 3–5 oken. Každé okno je možné zmenšit do tvaru ikony bez jakéhokoli vlivu na jeho činnost.

Pracovní okno

Pracovní okno slouží ke znázornění průběhu testování systému. V okně jsou vypisovány adresáře, které byly otestovány. Je tam též uveden počet virů, který byl v daném okně nalezen, stejně jako celkový počet virů, nalezený během daného spuštění programu ve všech oknech.

Pracovní okno je základní částí programu. První pracovní okno je otevřeno ihned při startu programu a má číslo 1. Každé z pracovních oken zobrazuje vlastní nezávislý postup testování určených částí systému. Jednotlivá okna mohou testovat zároveň různé i stejné oblasti (i když testování stejných částí ve stejném okamžiku má smysl jenom pokud chcete zdržovat procesor).

Postup otevírání pracovního okna

Pracovní okno se otevírá na požadavek uživatele, který ho vyjádří vybráním příslušné položky menu nebo stlačením tlačítka v pracovní liště. Při vytváření pracovního okna musí program vytvořit nezávislou pracovní oblast ve svých lokálních datech. Může se stát, že program v daném okamžiku nemá k dispozici dostatek prostoru a tyto data nevytvoří. V tom případě program oznámí uvedenou skutečnost a požadavek uživatele zruší.

Otevírání dalších oken

Pokud program zjistí požadavek na otevření druhého nebo dalšího pracovního okna, je toto okno označeno prvním volným číslem, které program zjistí. Toto číslo program určí tak, že projde seznam všech pracovních oken a oknu přiřadí první volné číslo. Pokud program používá například tři pracovní okna, vytvořená jedno za druhým, přiřadí jim čísla 1, 2 a 3. V případě, že je okno číslo 2 zrušeno (pracují pouze okna 1 a 3), je nově vytvářenému oknu přiřazeno číslo 2. Všechna pracovní okna jsou na sobě absolutně nezávislá, i když používají stejná referenční data pro testování, stejná konfigurační data pro výběr položek pro testování a stejné rutiny pro práci. Program nemá žádné prostředky pro zásah jednoho okna do interních dat jiného okna.

Význam okna číslo 1

Okno číslo 1 je vytvořeno zcela automaticky při startu programu bez nutnosti zásahu uživatele. Je to také jediný okamžik, kdy je pracovní okno vytvářeno bez požadavků na vstup informací od uživatele, a tyto data si převezme z konfiguračního souboru (například typy testovaných souborů, možné atributy, atd.).

Pokud program uzavírá okno číslo 1, zapisuje stav testování v něm do konfiguračního souboru. Tuto operaci program dělá pro každé okno číslo 1 (i pokud je uzavřené a opakovaně vytvořené). Žádné jiné okno při svém ukončování svůj stav testování nezapisuje. Zde je důležité si uvědomit, že pokud uzavřete první pracovní okno, nově ho pak vytvoříte s požadavkem na samostatné otestování některé části systému a program ukončíte, bude při dalším spuštění programu otestována jenom tato část a program nebude testovat cyklicky celý systém.

Jedině okno automaticky vytvořené při startu programu je schopno pokračovat v práci podle konfiguračních dat uložených při posledním ukončení programu.

Uživatelsky definované viry

AVAST! je dodáván včetně souboru LGUARD.VPS, který popisuje jednotlivé viry. Tento soubor je velice často aktualizován, ale i tak program obsahuje možnost definovat vlastní soubor uživatelských charakteristik virů. Okno uživatelsky definovaných charakteristik virů umožňuje zobrazit a editovat tento soubor.

Soubor s uživatelskými charakteristikami může obsahovat libovolné množství definic virů. Jeho obsah se řídí pravidly uvedenými v kapitole o programu LGUARD.

Pokud není nějaký řetězec platný, program pokračuje v interpretaci souboru do té doby, než nalezne řetězec, který by mohl být na uvedeném místě platný. Tato vlastnost programu může za určitých okolností způsobit, že se několik definic rozličných virů smíchá dohromady. Doporučujeme věnovat definičnímu souboru virů velkou pozornost! Příklady takových definic jsou uvedeny v popisu programu LGUARD.

Okno nalezených virů

V průběhu testování systému se mohou objevit některé viry (to je ostatně smyslem celého programu). Program LGW

hlásí každý virus nalezený v paměti a první virus nalezený v souborech. Seznam virů, které systém nalezl, je možné prohlížet v okně nalezených virů, kde se zobrazují všechny objevené viry společně s místem jejich nálezu. Obsah okna na rozdíl od zobrazování REPORT souboru je průběžně obnovován podle toho, kolik a jakých virů program zjistí v testovaných částech systému. Obsah okna není možné jakýmkoli způsobem editovat nebo měnit.

Okno hledaných virů

V tomto okně zobrazuje program seznam všech virů, které je schopen odhalit. Skutečný počet je ovšem vyšší, protože v seznamu není zahrnuta spousta modifikací. V okně jsou také zobrazeny některé statistické údaje o složení databáze virů a pomocí něho můžete získat některé základní informace o každém viru vybráním jeho jména. Obsah okna není možné jakýmkoli způsobem editovat nebo měnit a není možné měnit jeho velikost.

Stavová lišta

Pro průběžné zobrazování některých důležitých informací slouží stavová lišta, která je zobrazena ve spodní části hlavního okna. Její zobrazování je možné vypnout vybráním příslušné položky menu.

Levá strana stavové lišty stručně popisuje operaci položky menu, která je právě zvýrazněna. Při pohybu v systému menu je tento popis průběžně aktualizován. Tato oblast také popisuje akce, které mohou být vyvolány stisknutím některého z tlačítek v pracovní liště v okamžiku, když některé tlačítko stlačíte. Popis pro tlačítko zůstane aktivní až do okamžiku, než pustíte tlačítko myši. Pokud chcete zrušit operaci, kterou by vyvolalo puštění myši ukazující na některé tlačítko, pusťte myš v okamžiku, když nebude ukazovat na pracovní lištu.

Indikátor	Vysvětlení
1	počet otestovaných souborů celkem,
2	počet napadených souborů celkem,
3	počet nalezených druhů virů celkem,
4	procento otestování vybraného média.

Ovládání programu

Obsluha programu se od normální obsluhy programu pro Windows prakticky vůbec neliší. Všechny standardní akce, které je možné vykonávat pomocí myši nebo klávesnice je možné použít i v programu LGW.

Jako doplnění rychlé nápovědy pro jednotlivé ovládací prvky programu byla implementována tzv. bublinová nápověda (Tool Tips), která popisuje pracovní lištu programu. Bublinovou nápovědu můžete vyvolat pravým tlačítkem myši, pokud její ukazatel ukazuje na některou část lišty. Nápověda se zobrazí v bublině, která je kontextově citlivá, tj. pro různé prvky lišty se zobrazí vysvětlení jejich funkce.

Všechny schopnosti programu je možné obsluhovat z menu programu, které se mění podle toho, zda je otevřeno některé z oken a podle toho, které z otevřených oken je aktivní. Hlavní funkce je možné obsluhovat z pracovní lišty, která je zobrazena bezprostředně pod menu programu. Jednotlivá tlačítka mají stejný význam, jako odpovídající položky menu. Pokud je některé tlačítko neaktivní, je zobrazeno v šedivé barvě a není možné jej použít.

Jednotlivá tlačítka pracovní lišty mají následující význam:

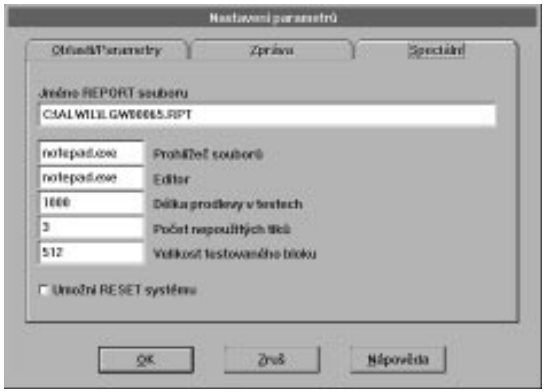
- otevření nového pracovního okna; LGW zobrazí dialog pro určení parametrů pro toto okno,
- otevření REPORT okna,
- otevření okna s uživatelskými charakteristikami virů,
- otevření okna se seznamem nalezených virů,
- otevření okna se seznamem hledaných virů,
- konfigurace programu; LGW zobrazí dialog, kterým se konfigurují všechny parametry programu,
- otevření informace o copyrightu a verzi definičního souboru charakteristik virů,
- změna kurzoru pro kontextovou nápovědu o jednotlivých prvcích programu.

Nastavování parametrů programu

LGW nerozeznává žádné parametry na příkazové řádce. Všechny potřebné parametry program načítá z konfiguračního souboru AVAST!.INI. Pokud tento soubor neexistuje, nebo pokud není některý z parametrů v souboru uveden, je použito standardní nastavení, které zaručuje optimální činnost programu v naprosté většině případů.

LGW má dvě místa, kde je možné zadat pracovní parametry. Jsou to **konfigurační dialog** a spouštění druhého a všech dalších pracovních oken.

Konfigurační dialog



Konfigurační dialog slouží k nastavení parametrů práce programu. Parametry jsou rozděleny do několika tématických skupin. Nesprávné nastavení ovládacích prvků může znehodnotit celou práci programu, proto je nutné všem změnám nastavení věnovat velkou pozornost.

Dialogový box podporuje všechny standardní postupy vkládání informací klávesnicí nebo myší. Pro jeho ovládání je možné použít tlačítka **OK** nebo **Zruš**.

Stlačení tlačítka **OK** má za následek uložení všech parametrů do konfiguračního dialogu a okamžité nastavení těch parametrů, pro které je to možné. Dialogový box je smazán z obrazovky. Stlačení tlačítka **Zruš** způsobí zrušení všech provedených změn konfiguračních parametrů a smazání dialogového boxu z obrazovky. Stlačení tlačítka **Nápověda** způ–

sobí vyvolání nápovědy ke konfiguračnímu dialogu. Stlačení klávesy Esc má stejný účinek jako stlačení tlačítka Zruš.

Pro konfiguraci programu můžete použít následující parametry.

Testuj paměť

Označení tlačítka znamená, že se bude testovat paměť v rozsahu lineárních adres 0 až 0x10FFFF, což představuje paměť reálného módu (DOS – 1MB) a HMA (64 KB). Pokud program dostane požadavek na otestování paměti a toto tlačítko není označeno, paměť se nebude testovat. Program automaticky generuje požadavek na otestování paměti vždy před testováním disku C:. Při startu programu se paměť otestuje i v případě, že toto tlačítko není označeno.

Standardní hodnota: Označeno

Testuj DPT

Označení tlačítka znamená, že se bude testovat sektor s tabulkou rozdělení pevných disků (DPT). Protože velikost tabulky pro jeden pevný disk je 512 bytů, testují se tabulky pro oba pevné disky systému najednou. Pokud má systém k dispozici pouze jeden pevný disk, program tuto skutečnost zjistí a pracuje pouze s jeho tabulkou. Pokud program dostane požadavek na otestování tabulky rozdělení pevných disků a toto tlačítko není označeno, tabulka se nebude testovat. Program automaticky generuje požadavek na otestování tabulek rozdělení pevných disků vždy po otestování paměti, a to i v případě, že paměť není testována. V případě nemožnosti přečíst DPT program zobrazí chybové hlášení a pokračuje v práci dále.

Standardní hodnota: Označeno

Testuj BOOT sektory

Označení tlačítka znamená, že se bude testovat BOOT sektor každého disku. Pokud program dos–

tane požadavek na otestování BOOT sektoru a toto tlačítko není označeno, sektor se nebude testovat. Program automaticky generuje požadavek na otestování BOOT sektoru vždy před testováním souborů na daném pevném disku. V případě nemožnosti přečíst BOOT sektor program zobrazí chybové hlášení a pokračuje v práci dále. Program netestuje BOOT sektor RAM disku.
Standardní hodnota: Označeno

Testuj soubory

Označení tlačítka znamená, že se budou testovat soubory na přístupných pevných discích systému. Pokud program dostane požadavek na otestování souborů a toto tlačítko není označeno, soubory se nebudou testovat. Program testuje soubory na lokálních i vzdálených discích, na které má uživatel v daném okamžiku přístup, přičemž rozeznává jména disků C: až Z:. Program při cyklickém testování ignoruje CD–ROM disky, které bez upozornění přeskakuje. Pokud při startu nového okna uživatel zadá na místo jména disku hodnotu A: nebo B: program otestuje i disketu v příslušné jednotce.
Standardní hodnota: Označeno

Testuj síťové soubory

Tlačítko slouží k rychlému přepínání stavu testování síťových disků, přičemž program automaticky rozeznává typ disku. Označení tlačítka znamená, že pokud se budou testovat soubory na lokálních discích, budou se testovat i na vzdálených discích. Pokud toto tlačítko není označeno, soubory na vzdálených discích se nebudou testovat.
Standardní hodnota Označeno.

Testuj SYS Soubory

Označení tlačítka znamená, že se budou testovat i soubory s nastaveným atributem SYSTEM. Pokud

není toto tlačítko označeno, soubory s nastaveným atributem SYSTEM budou ignorovány.
Standardní hodnota: Označeno

Testuj HID soubory

Označení tlačítka znamená, že se budou testovat i soubory s nastaveným atributem HIDDEN. Pokud není toto tlačítko označeno, soubory s nastaveným atributem HIDDEN budou ignorovány.
Standardní hodnota: Označeno

Testuj všechny soubory

Označení tlačítka znamená, že se budou testovat všechny soubory bez ohledu na to, jakou mají příponu. Pokud toto tlačítko není označeno, budou testovány pouze binární soubory s příponami: COM, EXE, SYS, BIN, OV?.
Standardní hodnota: Neoznačeno

Testuj celé soubory

Označení tlačítka znamená, že se budou testovat celé soubory. Pokud toto tlačítko není označeno, bude se testovat pouze začátek a konec souborů v délce 8191 slabik.
Standardní hodnota: Neoznačeno

Ignoruj specifikace virů

Označení tlačítka znamená, že se budou testovat všechny viry ve všech souborech bez ohledu na typ souboru a parametry viru. Pokud toto tlačítko není označeno, soubory typu COM (EXE) se testují jenom na viry, které mohou napadat soubory typu COM (EXE). Soubory jiných typů než COM a EXE jsou testovány na oba druhy virů.
Standardní hodnota Neoznačeno.

Zapisuj REPORT soubor

Označení tlačítka znamená, že se budou zapisovat některé informace do REPORT souboru. V tom pří–

padě se v souboru objevují informace o nalezených virech a o jiných důležitých informacích včetně statistik testování systému. Pokud toto tlačítko není označeno, žádné informace se do REPORT souboru nezapisují.
Standardní hodnota: Neoznačeno

Vytvoř pokaždé nový REPORT
Označení tlačítka znamená, že se při začátku zápisu do REPORT souboru při startu programu nebo při změně konfiguračních dat vytvoří nový soubor. Program automaticky generuje jeho jméno podle jména posledního zapisovaného souboru. Pokud toto tlačítko není označeno, zapisovaná data jsou ukládána v již existujícím souboru.
Standardní hodnota Neoznačeno.

Zapisuj i nenakažené soubory
Označení tlačítka znamená, že program bude zapisovat do REPORT souboru i soubory, ve kterých nenalezne známku přítomnosti známého viru. Pokud toto tlačítko není označeno, program nenakažené soubory nezapisuje.
Standardní hodnota Neoznačeno.

Pracuj v pozadí
Označení tlačítka znamená, že program se při spuštění automaticky změní na ikonu. Pokud toto tlačítko není označeno, bude program pracovat v popředí jako standardní okno. Označení tlačítka má vliv na spuštění programu. V čase jeho běhu je možné přepínat mezi ikonou a normálním oknem bez jakéhokoli omezení.
Standardní hodnota: Neoznačeno

Zpráva o nalezení viru
Editační okno obsahuje informaci, která se vypíše na obrazovku, pokud je nalezen virus. Zpráva se vypisuje v případě, že se jedná o virus v paměti, nebo

jde o první virus v jiné testované oblasti systému. Tuto zprávu je možno editovat a na její místo vložit libovolný text. Text je zobrazován v okně Zprávy o nalezení viru společně se jménem oblasti, kde byl virus nalezen a jménem viru. Text je zobrazován stejným způsobem, jakým je do tohoto okna zadán. Zpráva o nalezení viru může být poskytnuta také hlasovým výstupem, pokud jej aktuální instalace Windows podporuje. Konfiguraci zvukového hlášení je možno nastavit standardním způsobem v kontrolním panelu.
Standardní hodnota: „Nalezen virus!!!“

Umožni RESET

Označení tlačítka znamená, že uživatel může vynulova počítač. Pokud toto tlačítko není označeno, uživatel programu nemá právo vynulovat počítač použitím tlačítka pro RESET v dialogu „Zpráva o nalezení viru“ a po pokusu o RESET se zobrazí varovné hlášení. Samozřejmě, že program nijak nemůže ovlivnit činnost hardwarového RESETu nebo síťového vypínače.
Standardní hodnota: Neoznačeno

Jméno REPORT souboru

Editační okno umožňuje určit základ jména REPORT souboru. Program automaticky generuje nové jména podle dalších konfiguračních parametrů. Z uvedené hodnoty jsou platné cesta pro vytváření, první tři znaky jména a typ (extension) souboru. Zbylých pět znaků jména je rezervováno pro nahrazení programem.
Standardní hodnota „lgw.rpt“

Prohlížeč souborů

Editační okno, které umožňuje určit jméno programu společně se seznamem jeho parametrů, který se spustí v případě, že chcete zobrazit REPORT

soubor. Jméno REPORT souboru se neuvádí, program použije aktuální jméno.
Standardní hodnota „notepad.exe“

Editor

Editační okno, které umožňuje určit jméno programu společně se seznamem jeho parametrů, který se spustí v případě, že chcete zobrazit nebo editovat soubor uživatelem definovaných virů. Jméno souboru se neuvádí, program použije aktuální jméno.
Standardní hodnota „notepad.exe“

Délka prodlevy v testech

Editační okno umožňuje zadat, jak dlouho bude program čekat po každém pohybu myší. Program sleduje intenzitu práce uživatele a tomu přizpůsobuje svou vlastní práci tak, aby co nejméně rušil. Délka prodlevy se zadává v milisekundách.
Standardní hodnota 1000

Počet nepoužitých tiků

Editační okno umožňuje zadat četnost generování zprávy pro testování v případě, že systém Windows čeká na uživatelský vstup. Pokud Windows čekají na vstup od uživatele a neprovádí žádné operace (ani vlastní režii), je pravidelně volána systémová událost se stále se zvyšujícím číslem. Pokud v některém okamžiku systém Windows zpracuje nějakou událost, je toto číslování znovu generováno od čísla 0.

Vkládané číslo představuje počet volání události, která se ignorují. Pokud je zde uvedeno číslo 0, program pokaždé, když systém Windows nemá co dělat, generuje zprávu pro testování.
Standardní hodnota 3

Velikost testovaného bloku

Editační okno umožňuje zadat maximální velikost bloku v bytech, který se otestuje bez jakéhokoli

přerušení. Tento parametr slouží k odstranění problémů s prodlevami, kdy počítač nereaguje na žádný podnět uživatele. Hodnoty kolem 16 by měly vyhovovat i těm nejpomalejším systémům a hodnota 512 a výše je vhodná pro systémy osazené procesorem 486/66 a lepším. Zmenšování tohoto parametru způsobí zpomalení rychlosti testování.
Hodnota 0 znamená, že se celý přečtený blok testuje najednou. Hodnota různá od nuly znamená, že se přečtený blok dat testuje po částech s maximální velikostí udanou v tomto editačním boxu.
Standardní hodnota 512.

Nové pracovní okno

Dialog pro výběr oblasti pro testování je vyvolán vždy, když uživatel programu požaduje vytvoření nového pracovního okna. Slouží pro nastavení základních parametrů pro toto okno a jenom v případě jeho úspěšného vyplnění je možné vytvoření nového pracovního okna. Dialogový box podporuje všechny standardní postupy vkládání informací klávesnicí nebo myší. Stlačení klávesy Esc má stejný účinek jako stlačení tlačítka Zruš. Pro jeho ovládání můžete použít následující prvky.

Stlačení tlačítka **OK** má za následek uložení všech parametrů do interních dat programu a jejich předání nově se vytvářejícímu pracovnímu oknu. Dialogový box je smazán z obrazovky. Stlačení tlačítka **Zruš** způsobí zrušení všech

provedených změn parametrů a potlačení dalšího vytváření pracovního okna. Dialogový box je smazán z obrazovky.

Začni s pamětí, Začni s DPT, Začni s BOOT sektorem a Začni se soubory

Tlačítka pro test paměti, DPT, BOOT sektoru a souborů slouží pro výběr jedné z oblastí systému, která bude jako první nebo jako jediná testována na přítomnost virů v novém pracovním okně. Pro položky Test BOOT sektoru a Test souborů se bližší specifikace oblasti vybírá z editačního boxu se jménem disku a adresáře.

Standardní hodnota: Test souborů

Testuj cyklicky dále

Označení tohoto tlačítka způsobí, že se budou testovat i jiné oblasti systému, než právě vybrané. Program zaručuje, že vybraná část se bude testovat jako první. Pokud si uživatel vybere test adresáře, bude testován obsah disku od tohoto adresáře dále tak, jak program načte adresářovou strukturu daného pevného disku (jaké informace dostane od systému DOS). Všechny adresáře, které jsou umístěny před vybraným adresářem nebudou testovány a o této skutečnosti nebude podána žádná zpráva. Pokud zůstane toto tlačítko neoznačeno, bude pracovní okno testovat pouze vybranou část systému a po ukončení testů se automaticky uzavře. Automatické uzavírání nepotřebných oken urychluje činnost programu a poskytuje dalším oknům více dostupné paměti.

Standardní hodnota: Neoznačeno

Testuj jenom podadresáře

Tlačítko umožňuje otestovat jenom část adresářového stromu od vybraného adresáře. Po ukončení testů této oblasti bude pracovní okno zrušeno podobně, jako tomu je v případě testů jenom jedné oblasti.

Standardní hodnota: Neoznačeno

Nápověda

Program LGW poskytuje kontextově citlivou nápovědou, která reaguje na standardní klávesu F1.

Pokud potřebujete získat nápovědu k některému zobrazenému prvku použijte klávesu Shift–F1 nebo příslušné tlačítko z příkazové lišty, které změní tvar kurzoru. Dokud je kurzor změněn stačí kliknout levým tlačítkem myši v okamžiku, když se její kurzor nachází na příslušném prvku a program k němu vyvolá příslušnou nápovědu.

Seznam zpráv, varování chyb a dotazů.

Pracovní okno číslo X bylo uzavřené pro chybu v programu. Chyba byla specifikována předchozím hlášením.

Jedno z pracovních oken bylo uzavřeno pro zde nespecifikovanou chybu. Jde o informační hlášení, které bylo uvedeno jiným hlášením s přesnějším vymezením chyby.

Nemáte právo resetovat počítač. Pokud toto právo potřebujete, musíte manuálně nastavit příslušné tlačítko v dialogu pro nastavování parametrů.

RESETovat počítač je činnost, která musí být povolena v konfiguračních datech programu. Pokud je zobrazeno toto hlášení, uživatel v daném okamžiku toto právo nemá.

REPORT soubor JMÉNO neexistuje. Nemohu otevřít jeho okno. Pokud chcete, aby program zapisoval REPORT soubor, musíte nastavit příslušné tlačítka a jméno souboru v dialogu pro nastavování parametrů.

Program nemůže zobrazit neexistující soubor.

Váš definiční soubor virů je příliš starý. Informujte se na možnost upgrade u Vašeho dodavatele.

Pokud používáte program LGW dlouho, může se stát, že definiční soubor virů není na úrovni doby. V případě, že je starší než 6 měsíců, LGW zobrazí toto hlášení. Informujte se na možnost získání nejnovější verze u vašeho dodavatele.

Není co testovat. Nastavení programu indikuje, že program nemá co testovat. Pokud potřebujete otestovat některou část systému, změňte nastavení programu.

Nastavení konfiguračních dat ukazuje, že program nemá co na práci. V tomto stavu pouze zabírá paměť a jinak je k nepotřebě. Změňte nastavení konfiguračních dat nebo ukončete program.

Definiční soubor není použit. Uživatelské definice se specifikují v souboru SYSTEM.INI a v současné době nejsou použity. Použiji JMÉNO.

V okamžiku vyvolání editace souboru uživatelsky definovaných virů není žádný soubor definován. Je vytvořen nový soubor.

Konfigurační soubor není uložen. Program detekoval chybu při ukládání změněných parametrů na disk. Změny nejsou uloženy a nejsou akceptovány.

Změněná data nejsou uložena v konfiguračním souboru. Chyba nebyla způsobena programem LGW.

Přepisování obsahu REPORT souboru. V případě, že místo prohlížeče používáte editor, nepřepisujte obsah REPORT souboru z důvodů možných kolizí s následnými zápisy Lguardu.

Toto upozornění je vypsáno při pokusu o zobrazení REPORT souboru. V případě, že pro zobrazení používáte editor, manuální vepsání dat může porušit strukturu souboru a způsobit ztrátu dat.

Chyba při zápisu do REPORT souboru. Program detekoval chybu při zápisu do REPORT souboru, kterou není schopen opravit. Zaznamenáváni dat je vypnuto. Můžete ho opakovaně zapnout nastavením příslušného tlačítka v konfiguračním dialogu.

Pokud při zápisu dat do REPORT souboru dojde k chybě, je jeho aktualizace okamžitě vypnuta, ale program pokračuje nadále v testování. Nejpravděpodobnější příčinou je nedostatek místa na disku.

Testování souboru na síti. Soubory na síti tvoří podmnožinu přístupných souborů. Není možné testovat soubory na síťových discích a mít vypnut požadavek testování souborů obecně.

Pokud požádáte o testování souborů na síti, musíte mít zapnut požadavek na otestování souborů obecně. Změňte nastavení konfiguračních dat.

Soubor JMÉNO je již smazán. Nemůžete pracovat se souborem, který již neexistuje. Pokud jste ho smazali omylem, je nám velice líto, ale soubor je nenávratně ztracen.

Opravdu práce se smazanými soubory není snadná a v programu LGW ani možná.

Chyba přejmenování souboru. Nemohu přejmenovat soubor na stejné jméno. Operace nemá žádný smysl.

Opravdu existence dvou souborů s úplně stejným jménem není možná.

Program nemůže vytvořit interní data. Pro práci programu jsou nutná některá další data, která zabírají místo v lokální paměti. Program nemá dostatek místa pro jejich vytvoření. Váš požadavek není akceptován.

Toto hlášení je zobrazeno jako reakce na požadavek na otevření dalšího pracovního okna. Požadavek nemůže být splněn.

Nedostatek paměti. Program nemá dostatek místa v paměti. Požadovaná akce nemůže být uskutečněna a je zrušena. Pokud trváte na jejím provedení, uzavřete některé okno programu a zkuste znovu.

Pokud opravdu trváte na svém požadavku, řiďte se radou hlášení.

Chyba při pokusu o zobrazení dat. Program z neznámého důvodu nemůže zobrazit potřebná data. Okno, které způsobilo chybu, bude uzavřeno.

Zdroj chyby nemůže být přesně určen. V každém případě se nepovedlo přistoupit k datům a ta zobrazit.

Chyba otevírání REPORT souboru. Soubor JMÉNO neexistuje nebo není přístupný. Není ho možné zobrazit.

Není možné zobrazit REPORT soubor. Buď neexistuje nebo jiné programové vybavení k němu neuvolňuje přístup.

Nemohu alokovat časovač, což je nutné pro práci programu. Ukončete některý program a zkuste znovu.

Program potřebuje pro svou práci časovač, kterých není mnoho. Pokud opravdu chcete spustit LGW, musíte uzavřít některý ze spuštěných programů.

Chyba čtení DPT. Za běžných okolností můžete volně číst DPT, ale na síťových nebo CD–ROM discích tuto možnost nemáte. Existuje také hardware nebo software, který zabraňuje čtení těchto oblastí disků. DPT nebude testována.

Přístup k DPT může být velice obtížný.

Chyba čtení BOOT sektoru disku X. Za běžných okolností můžete volně číst BOOT sektor, ale existuje

hardware nebo software, který zabraňuje čtení těchto oblastí disků. BOOT sektor nebude testován.

Přístup k BOOT sektoru disků může být obtížný.

Chyba otevírání souboru JMÉNO. Program zjistil chybu při pokusu otevřít soubor. Tento soubor nebude testován. Pokračovat v práci ?

Pokud je soubor nalezen ale není ho možné otevřít, program reaguje tímto hlášením. Je na uživateli, aby rozhodl, zda pokračovat s testováním dalších souborů nebo ne.

Chyba zápisu do souboru JMÉNO.

Při zápisu do souboru může dojít k množství chyb, kterých přesný zdroj může být obtížné identifikovat. V každém případě zkontrolujte velikost volného místa na disku.

Zakázán přístup k souboru JMÉNO.

Existuje programové vybavení, které znemožňuje přístup k zvoleným souborům. Pokud podobné programové vybavení nepoužíváte, zkontrolujte integritu disku.

Chyba čtení souboru JMÉNO. Program zjistil chybu při čtení ze souboru.

Při čtení souborů může dojít k množství chyb, kterých přesný zdroj může být obtížné identifikovat. Zkontrolujte integritu disku.

Nedostatek paměti pro požadovanou operaci. Program nemá dostatek lokální paměti pro splnění požadované operace.

Operační paměť není v 16–ti bitových Windows rovnocenná. Dělí se na lokální a globální. Velikost lokální paměti nemůžete ovlivnit.

Nedostatek paměti. Program nemá dostatek paměti pro pokračování v práci za dané konfigurace. S poli–

továním Vám oznamuje, že jedno z pracovních oken bylo uzavřeno.

Operační paměť není v 16–ti bitových Windows rovnocenná. Dělí se na lokální a globální. Velikost globální paměti můžete ovlivnit uzavřením některých běžících programů, zvětšením virtuální paměti nebo vlastním přidáním RAM.

Chyba vytváření souboru JMÉNO. Program zjistil chybu při pokusu vytvořit požadovaný soubor.

Program LGW potřebuje občas vytvořit soubor. Pokud se mu to nepovede, znamená to chybu přístupu k disku. Zkontrolujte jeho integritu.

Chyba spuštění programu. Nemohu spustit JMÉNO. Je pravděpodobné, že tento program neexistuje nebo k němu nemáte přístup.

Právo ke spuštění programu může být odebráno jiným programovým vybavením (např. SUP) nebo síťovým operačním systémem. Zkontrolujte však, zda daný program existuje a je přístupný.

Chyba čtení BOOT diskety X. Za běžných okolností můžete volně číst BOOT sektor disket. Ujistěte, zda máte disketu v jednotce a zkuste opakovat operaci znova.

Právo čtení BOOT sektoru může být odebráno jiným programovým vybavením (např. SUP). Zeptejte se správce systému, zda tomu tak není.

Chybný výběr oblasti. Není možno testovat BOOT sektor disku X:. Vyberte si jinou oblast, kterou chcete otestovat, nebo kterou chcete testování začít.

Není možné testovat BOOT sektor všech typů záznamových médií. Pokud program neumí příslušný BOOT sektor přečíst, uvidíte toto hlášení.

Chyba při uzamykání globální paměti. Alokovaná globální paměť nemůže být uzamčena pro program.

Toto je vážná chyba, která může způsobit zhroucení systému Windows.

Toto je opravdu vážná chyba systému Windows, která může způsobit zablokování počítače a ztrátu dat. Hlášení není možné ignorovat.

Program nemůže použít globální paměť. Při inicializaci dat nutných pro alokaci globální paměti došlo k chybě. Toto je vážná chyba, která může zhroutit systém Windows.

Toto je opravdu vážná chyba systému Windows, která může způsobit zablokování počítače a ztrátu dat. Hlášení není možné ignorovat.

Program nemůže použít časovač. Tato chyba nastala až po uvolnění původního časovače, takže program nemůže dále pokračovat v práci. Tato chyba nemůže destabilizovat systém Windows, ale program je ukončen.

Pokud požadujete změnu časových konstant programu může dojít k chybě realokace časovače. Chyba má za následek okamžité ukončení programu, ale není potřeba se obávat dalších následků. Veškerá paměť byla uvolněna a můžete se pokusit spustit LGW znova.

Definiční soubor virů není v paměti. Pro práci programu je nutno při startu systému Windows zavést knihovnu AWANTI.386 do paměti.

Knihovna AWANTI.386 obsahuje vlastní jádro antivirového testování všech dat systému AVAST!. Pokud není zavedena do paměti, nemá smysl, aby LGW nadále pracoval.

Chyba VxD číslo X. Při testování dat se vyskytla chyba. Místo jejího vzniku je v kritické oblasti, takže doporučujeme program ukončit a spustit znovu.

Chyba vznikla opravdu v kritické oblasti programu. Je s podivem, že systém stále pracuje. V každém

případě uzavřete program a zkuste testování znova.

Chyba testování polymorfních virů. Program nemůže otestovat soubor JMÉNO na přítomnost polymorfních virů z neznámých důvodů. Soubor nebude testován.

Není vůbec jasné, proč nemůže být příslušný soubor otestován na přítomnost polymorfních virů. Pokud je toto hlášení zobrazeno, kontaktujte svého dodavatele nebo přímo firmu ALWIL Software.

Chyba detekce rozšířeného módu. Program není schopen pracovat v jiném módu. Ukončete Windows a použijte příkaz 'WIN /3'.

Program LGW vyžaduje rozšířený režim práce systému Windows.

Opravdu? Jste si zcela jisti, že chcete testovat soubory na CD–ROM disku? Samozřejmě je to možné, ale jistě uznáte, že to není zcela běžný požadavek. Testování může trvat velice dlouho.

Otestovat CD–ROM disk může trvat dlouho, ale je pravda, že se virus občas na CD–ROM vyskytuje.

Smazat soubor JMÉNO? Pokud odpovíte ANO, soubor bude smazán bez možnosti jakékoli obnovy. Pokud si nejste jisti, operaci neprovádějte.

Smazání souboru programem LGW je zcela nevratné. Ani odborník na operační systém nepomůže, protože je použit zcela destruktivní způsob mazání.

Vytvářený soubor JMÉNO již existuje. Pokud si zvolíte odpověď ANO, bude existující soubor nenávratně přepsán.

Vytvoření souboru stejného jména zcela nevratně likviduje původní soubor.

Sum–GUARD pro Windows

SGW je jeden program, který je určen pro rychlý test změn jednotlivých souborů. Jeho základní určení je v rychlé kontrole základních (hlavně systémových) souborů, např: msdos.sys, io.sys, command.com nebo win.com). Program není samozřejmě omezen jenom na vyjmenované soubory, ale je do něj možno zařadit libovolný soubor, který je v okamžiku spuštění programu dosažitelný.

Instalace programu

Program SGW se instaluje v průběhu instalace systému AVAST!. Instalace samotná probíhá ve dvou krocích. Základní instalační program se zeptá, zda chcete nainstalovat i programy pro Windows. Po kladné odpovědi se instalují i soubory, které jsou nutné pro práci v systému Windows.

Vlastní instalace v systému Windows spočívá ve spuštění instalačního programu AVINST, který je standardní součástí dodávky a je připraven po instalaci systému AVAST! pro DOS.

Princip práce

Princip práce programu je velice jednoduchý. Program si přečte soubory uvedené na příkazové řádce nebo v konfiguračním souboru systému AVAST!, spočte si jejich kontrolní součty a zkontroluje s údaji zjištěnými dříve nebo uvedenými na příkazové řádce společně se jmény souborů.

Program je schopen zpracovat soubory uvedená na příkazové řádce, nebo je schopen práce v interaktivním režimu, kdy je možné zadat jména kontrolovaných souborů v přehledném dialogu.

Parametry programu

Program SGW je schopen zpracovat několik různých parametrů na příkazové řádce a jeden speciální parametr. Parametry, které program nezná, jednoduše ignoruje bez jakýchkoli chybových hlášení. V případě, že program nenajde soubor uvedený na příkazové řádce, ignoruje jej také.

Obecný tvar příkazové řádky programu SGW je:

```
SGW [soubor [suma] [soubor [suma] ...][[/|-][A|a]]
   [[/|-][D|d]] [[/|-][M|m]]]
```

kde soubor představuje plné jméno souboru pro kontrolu, suma jeho kontrolní sumu zapsanou v desítkové soustavě. Kontrolní sumu je nutné zadat v případě, že ji znáte. Pokud ji neznáte a zapíšete příkazovou řádku například ve tvaru:

```
SGW c:\command.com c:\io.sys c:\msdos.sys
```

program SGW vypočte kontrolní sumu pro každý soubor a ohlásí chybu, protože nenašel žádné číslo, se kterým by spočtenou kontrolní sumu porovnal. Výše uvedený zápis má smysl pouze v případě, že do příkazové řádky zařadíte jeden z přepínačů /A nebo /D. Pokud znáte kontrolní součet jednotlivých souborů, můžete zadat stejný příkazový řádek ve tvaru:

```
SGW c:\command.com 12345 c:\io.sys 23456
```

Význam jednotlivých přepínačů je následující:

přepínač /A

přidá všechny soubory nalezené na příkazové řádce do konfiguračního souboru. Pokud je na příkazové řádce uvedena taky kontrolní suma, přidá ji do konfiguračního souboru také.

přepínač /D

smaže soubory nalezené na příkazové řádce z konfiguračního souboru. Uvedení kontrolní sumy nemá žádný vliv na další práci.

přepínač /M

přepne program do interaktivního režimu práce, přičemž nejprve zpracuje všechny ostatní parametry příkazové řádky a po jejich zpracování zobrazí konfigurační dialog.

Parametry /A a /D nemohou být na příkazové řádce uvedeny najednou. Pokud se tak stane, program ohlásí chybu a ukončí práci programu.

Pokud při použití parametru /A není uvedena kontrolní suma pro některý nebo všechny soubory, jsou tyto přidány do konfiguračního souboru a kontrolní suma je spočtena při prvním

dalším spuštění programu. Tato skutečnost není žádným způsobem ohlášena a probíhá plně bez zásahů uživatele.

Všechny přepínače příkazové řádky mohou být uvedeny znaky '/' nebo '–' a mohou být napsány velkým nebo malým písmenem.

Program akceptuje jeden parametr, který se nezadává z příkazové řádky, ale z vlastností ikony spouštěného programu, který určuje, zda spustit program v minimalizované formě nebo ne. Pokud je program spuštěn s označením tlačítka **Run Minimized**, zkontroluje stav souborů uvedených na příkazové řádce a uvedených v konfiguračním souboru v tomto pořadí. Pokud toto tlačítko není označeno, program tento stav považuje za stejný, jako by byl na příkazové řádce uveden parametr /M a je spuštěn v interaktivním režimu. Při instalaci se vytvoří dvě kopie ikony programu SGW. Jedna z nich, uložená ve skupině AVAST! nemá tento parametr onzačen a spuštění tohoto programu má za následek vyvolání konfiguračního dialogu. Ve startovací skupině je tento parametr zaškrtnut a program při startu Windows zkontroluje nastavené soubory a konfigurační dialog nezobrazuje.

Pracovní soubory

Program SGW potřebuje pro svou práci několik souborů. Některé z nich potřebuje, aby se vůbec spustil (dynamické knihovny) a konfigurační soubor, který si čte i zapisuje. V případě, že tento soubor neexistuje, program si ho vytvoří v adresáři, ze kterého byl spuštěn.

Program používá soubor AVAST!.INI k ukládání potřebných údajů. Tento soubor má standardní formát všech konfiguračních souborů systému Windows a je umístěn v adresáři, odkud byl program spuštěn. Pro svou práci program používá skupinu [SGUARD].

Parametr FileXXX

Parametr FileXXX je určen pro uložení jména testovaného souboru a jeho kontrolní sumy. Soubor znaků 'XXX' je v reálném konfiguračním souboru nahrazen číslem. Například:

```
File1=c:\command.com,12345
```

Z ukázky je zřejmé, že číslo nahrazující znaky 'XXX' není uvedeno žádnými nulami nebo prázdnými znaky. Kontrolní suma je uvedena ihned za jménem souboru a je od něj oddělena čárkou.

Číslování jednotlivých položek není důležité, je dokonce možné některé z nich vynechat. Při používání interaktivního nastavení program SGW automaticky vzestupně čísluje jednotlivé položky. V případě, že jsou některé z nich smazány, program automaticky použije volné čísla.

Pokud manuálně editujete obsah kontrolního souboru, je nutno přesně dodržet formát parametru. Program nepředpokládá žádné odchylky od zde popsaných pravidel. Položky, které program není schopen identifikovat, ignoruje bez jakýchkoli hlášení.

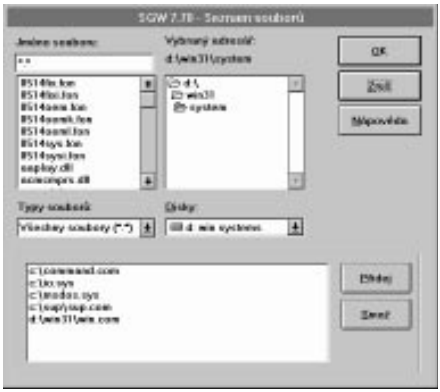
Parametr NumberFiles

Parametr NumberFiles je určen pro uložení počtu souborů, které má kontrolovat. Počet je uložen jako standardní číslo v desítkové soustavě.

Pokud používáte interaktivní nastavení, program SGW automaticky udržuje hodnotu parametru. Pokud manuálně editujete konfigurační soubor, je potřebné mít na vědomí následující fakta.

Program otestuje jenom ten počet souborů, který je uveden v parametru NumberFiles, přičemž tyto soubory zpracovává v číselném pořadí. Všechny ostatní soubory ignoruje.

Pokud je v parametru NumberFiles uvedeno vyšší číslo, než kolik je uvedeno souborů v konfiguračním souboru, program ohlásí chybu a nabídne opravu parametru.



Ovládání programu

Ovládání programu SGW je stejné, jako ovládání ostatních programu pracujících v systému Windows. Program nepoužívá žádné speciální způsoby obsluhy a nevyžaduje žádné speciální nebo nezvyklé znalosti.

Práce s dialogem pro interaktivní nastavení

Pokud je při spuštění programu použit parametr /M nebo speciální parametr, je zobrazen dialog pro interaktivní nastavení testovaných programů.

Dialog je modifikovanou verzí standardního dialogu systému Windows pro otevírání souborů. Jeho modifikace spočívá v přidání spodní části, ve které se nachází seznam se jmény souborů, které se při spuštění SGW testují a dvě tlačítka pro práci s tímto seznamem.

Do seznamu je možno přidat prakticky neomezené množství souborů. Jediné omezení je způsobeno systémem Windows, který neumožňuje libovolné množství prvků v seznamu.

Práce s dialogem chybových hlášení a zpráv

Chybová hlášení nebo zprávy jsou programem generovány na podnět událostí, které mají vážný vliv na práci programu nebo jsou důležité pro uživatele.

Tento typ dialogu umožňuje pouze jednu odpověď a program čeká do okamžiku, než uživatel tuto odpověď zadá. Ostatní

pracující programy systému Windows nejsou tímto čekání žádným způsobem ovlivněny a pracují normálně dále.

Práce s dialogem pro dotazy

Dotazy jsou programem generovány v případě, že program potřebuje znát odpověď jak pokračovat dále v práci.

Tento typ dialogu umožňuje odpovědět kladně nebo záporně na otázku, která je zobrazena. Program čeká do okamžiku, než si uživatel vybere jednu z nabízených odpovědí. Ostatní pracující programy systému Windows nejsou tímto čekání žádným způsobem ovlivněny a pracují normálně dále.

Původ programu

Program SGW ve své verzi 7.0 je první implementací pro systém Windows. Je součástí systému AVAST! od verze 7.0 a číslování jeho verzí je stejné jako číslování verzí AVASTu.

Program SGW odvozuje svůj původ od programu SGUARD pro DOS, který je součástí systému AVAST! již od verze 3.0. Při své práci používá stejné interní algoritmy pro zjišťování kontrolních sum souborů, takže čísla, které při práci s programem nebo jeho pracovními soubory spatříte jsou stejná, jako ty, která produkuje program SGUARD pro DOS.

Program má téměř stejné schopnosti, jako jeho DOSový protějšek s několika změnami.

1. Program pracuje výhradně v systému Windows.
2. Program obsahuje interaktivní nastavování testovaných souborů.
3. Program neobsahuje možnost testování kontrolní sumy paměti, protože tato schopnost je v systému Windows zbytečná.
4. Program ve své současné verzi neobsahuje možnost testování systémových oblastí jednotlivých disků.

Požadavky pro práci a spouštění programu

Program SGW pro svou práci požaduje:

1. Microsoft Windows 3.1 nebo novější operační systém.
2. Systém s procesorem minimálně 80386sx nebo kompatibilním.

Program ve standardním režimu nevytváří žádné okno, ale přes to všechno zjišťuje, zda je spouštěn s požadavkem na

zobrazení ve standardním tvaru s rozvinutým oknem, nebo má být spuštěn ve tvaru ikony.

Program je možné spustit všemi způsoby, které akceptují všechny normální 16–ti bitové EXE programy ve Windows.

Seznam zpráv, varování, chyb a dotazů

SGW je schopen zobrazit několik různých druhů varování a chybových hlášení, která zobrazuje v různé formě. Jejich seznam a bližší informace o možných variantách jsou uvedeny níže.

Špatný kontrolní součet. Soubor 'ANYFILE' má kontrolní součet 99998. Kontrolní součet v konfiguračním souboru je 99999. Je tato změna v pořádku ?

Toto varování je zobrazeno v případě, že kontrolní součet souboru nesouhlasí s daty uvedenými na příkazové řádce nebo v konfiguračním souboru. Varování má dvě podoby. V případě kontroly souboru z příkazové řádky je zobrazeno ve formě varování. V případě kontroly souboru z konfiguračního souboru má formu dotazu, kde můžete určit, zda je nová kontrolní suma v pořádku (změna souboru je legální) nebo ne. Zpráva o nesprávném kontrolním součtu může být poskytnuta také hlasovým výstupem, pokud jej aktuální instalace Windows podporuje. Konfiguraci zvukového hlášení je možno nastavit standardním způsobem v kontrolním panelu. Pokud je změna v pořádku, je nová hodnota kontrolní sumy zaznamenána do konfiguračního souboru.

Smazat soubor 'ANYFILE' z konfiguračního souboru ? Pokud tento soubor smažete, nebude se vícekrát testovat.

Toto varování je zobrazeno v okamžiku, kdy je požadováno smazání některého souboru ze seznamu uvedeného v konfiguračním souboru. Toto varování je zobrazeno ve formě dotazu, zda tento soubor chcete opravdu trvale smazat. Pokud odpovíte kladně,

soubor bude smazán se seznamu a až do opětovného zařazení nebude testován.

Nedostatek paměti. Lituji, ale program nemá k dispozici dostatek paměti. Požadovaná služba nemůže být provedena.

Tato chyba se zobrazí v okamžiku, když program narazí na nedostatek paměti pro svou práci. SGW používá pro svou práci jenom naprosté minimum paměti (asi 10 kB), které by měly být k dispozici v každém případě. Pokud Vám program zobrazí tuto chybu, spojte se s vaším dodavatelem systému AVAST! nebo přímo s firmou ALWIL Software a informujte jej o této skutečnosti.

Chyba otevření souboru. Program není schopen otevřít soubor ANYFILE. Soubor bude vyřazen ze seznamu.

SGW potřebuje otevřít každý testovaný soubor. Program jej otevírá pouze pro čtení a zároveň nastavuje příznak, že soubor může být jinými procesy čten, ale ne zapisován. V případě, že je testovaný soubor již otevřen exkluzivním způsobem nebo operační systém nemůže tento soubor zpřístupnit z jakýchkoli jiných důvodů, je ohlášena tato chyba. Jako reakci na tento typ chyby doporučujeme zkontrolovat, zda testovaný soubor skutečně existuje a zda jej právě nepoužívá jiná spuštěná aplikace.

Soubory pro kontrolu nenalezeny. Parametry souboru AVAST!.INI nejsou správné. Opravit konfigurační soubor ?

Program zobrazí tuto chybu jako reakci na špatný obsah konfiguračního souboru. Jedná se o případ, že proměnná NumberFiles obsahuje větší počet souborů pro testování než se v konfiguračním souboru skutečně nachází (proměnné FileXXX). Tato chyba je zobrazena ve formě dotazu, zda chcete op–

ravit konfigurační soubor. Před zobrazením této chyby může dojít k poměrně značné prodlevě v práci programu, která je uvedena změnou kurzoru na tvar přesýpacích hodin. Tato prodleva je způsobena intenzivním prohledáváním konfiguračního souboru a hledáním chybějících souborů pro testování.

Špatná struktura příkazové řádky. Příkazová řádka nemůže obsahovat přepínače '/A' a '/D' najednou.

Tato chyba je zobrazena jako reakce programu na špatnou strukturu příkazové řádky.

Alter–GUARD pro Windows

AGW je určen pro testování integrity obsahu všech dostupných disků. Program představuje základní článek ochrany systému před napadení viry. Pokud pravidelně a správně používáte tento program, máte vysokou pravděpodobnost, že se Vám povede zachránit většinu napadených souborů.

Instalace programu

Program AGW se instaluje v průběhu instalace systému AVAST!. Instalace samotná probíhá ve dvou krocích. Základní instalační program se zeptá, zda chcete nainstalovat i programy pro Windows. Po kladné odpovědi se instalují i soubory, které jsou nutné pro práci v systému Windows.

Vlastní instalace v systému Windows spočívá ve spuštění instalačního programu AVINST, který je standardní součástí dodávky a je připraven po instalaci systému AVAST! pro DOS.

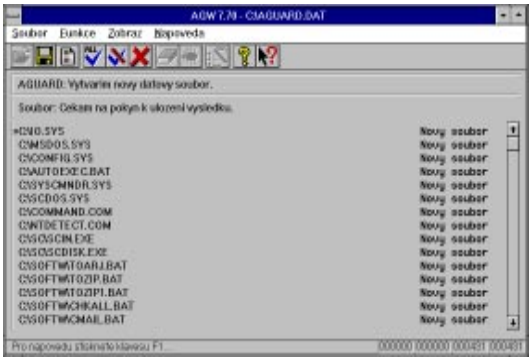
Principy práce

AGW je určen pro sledování změn obsahu jednotlivých souborů na discích, které jsou v daném okamžiku přístupné. Program sleduje změny všech parametrů, které jsou pro daný soubor charakteristické a je schopen zachytit jakoukoli jejich změnu.

Program při svém startu přečte konfigurační soubor a zjistí, zda v něm nenajde určení oblastí, které je nutno otestovat. Pokud tomu tak je, program zcela automaticky začne testovat

první z nalezených oblastí. Pokud tomu tak není, program očekává zadání pro testování pomocí mírně modifikovaného dialogu pro otevírání souborů.

Pro každou testovanou oblast si AGW načte soubor s již uloženými daty. Vlastní práce spočívá v přečtení každého souboru v testované oblasti a porovnání aktuálně zjištěných dat s daty, které byly uloženy při posledním běhu programu. Pokud se data rovnají, je zaručeno, že soubor zůstal nezměněn. Uživatel si může vybrat několik oblastí pro testování najednou, přičemž jejich počet je omezen pouze systémovými prostředky Windows.



Pokud je některý z parametrů změněn, program ho vypíše do hlavní oblasti svého pracovního okna společně s určením typu změny. Změněné soubory je možné dále zpracovávat prostředky programu, které jsou blíže popsány v kapitole Ovládání programu.

Po ukončení testování některé z oblastí, je možno změněná data pro vybrané (nebo všechny) soubory prohlásit za správná a uložit je do datového souboru. Data o nevybraných souborech zůstanou nezměněna.

Program pracuje v prodlevách práce systému a jeho návrh prakticky vylučuje jakýkoli vliv na rychlost práce ostatních programů. Jediné a v praxi velice malé zdržení může vyplynout z přístupu k souborům a obsazení velké části diskové vyrovnávací paměti, která tak nemůže být využita jinými programy.

Parametry programu

Program AGW ve své verzi 7.0 nerozeznává žádné parametry předané pomocí příkazové řádky. Všechny parametry, které zde nalezne, ignoruje bez jakéhokoli varování.

Všechny parametry, které program potřebuje uchovat v období mezi dvěma spuštěními programu si program uchovává v konfiguračním souboru AVAST!.INI. Program AGW používá jenom část z parametrů, které jsou zapsány v tomto konfiguračním souboru. Jedná se o data ve skupinách [AGUARD] a [AGW–Param].

Skupina (AGUARD)

Skupina AGUARD obsahuje základní parametry pro práci programu, které neurčují jeho konfiguraci. Jedná se zejména o parametry nevyhnutelné pro komunikaci dvou instancí programu.

Ve skupině [AGUARD] můžete nalézt tyto parametry:

Temp

Proměnná TEMP slouží pro účely komunikace jednotlivých instancí programu. Její hodnota se mezi jednotlivými běhy programu mění. Je důležité, abyste její obsah za běhu programu neměnili jiným programem (editorem), protože může dojít ke ztrátě důležitých dat.

Skupina (AGW–Param)

Skupina [AGW–Param] obsahuje parametry, které jsou důležité pro uchovávaní konfigurace programu mezi jeho dvěma spuštěními. Nedoporučujeme manuální změny jednotlivých parametrů z důvodů možnosti jejich nesprávné kombinace a z toho vyplývající možnosti ztráty dat.

Ve skupině [AGW–Param] můžete nalézt tyto parametry:

Extension1 – Extension10

Tyto parametry slouží pro uchování testovaných typů souborů. Jsou v nich uchovány textové řetězce o délce 1 – 3 znaky ve formátu, který odpovídá formátu typu souboru v DOSu. Z důvodů zachování

kompatibility s verzí AGUARDu pro DOS můžete uchovat pouze deset typů souborů. Pokud potřebujete testovat více typů, musíte použít znaky pro zadání více typů najednou („*“ nebo „?“) podle pravidel DOSu.

TestingAreas

Parametr „TestingAreas“ slouží pro uložení oblastí pro testování, které chcete pravidelně automaticky testovat. Tyto oblasti budou při každém spuštění programu. Hodnotu parametru představuje řetězec znaků.

AutomaticStart

Parametr „AutomaticStart“ obsahuje logickou hodnotu 0 nebo 1, která určuje, zda program automaticky otestuje oblasti pro testování, které jsou vyjmenovány v parametru „TestingAreas„ bez výzvy uživateli. Pokud má tento parametr hodnotu 0, je uživatel vyzván na zadání oblastí pro testování. Pokud má parametr hodnotu 1 a parametr „TestingAreas„ obsahuje platnou oblast pro testování, program automaticky začne s testováním.

FastCheck

Parametr „FastCheck“ obsahuje logickou hodnotu 0 nebo 1, která určuje, zda bude program testovat i obsahy jednotlivých souborů. Pokud má parametr hodnotu 0, obsahy souborů budou testovány, Pokud má parametr hodnotu 1, obsahy souborů testovány nebudou. V tomto případě program slouží pro velice rychlou kontrolu vymazaných souborů nebo změn atributů. Program i v případě netestování obsahu jednotlivých souborů povolí uložení změněných dat do souboru.

IgnoreArchive

Parametr „IgnoreArchive“ obsahuje logickou hodnotu 0 nebo 1, která určuje, zda bude program brát

v úvahu změnu archivního bitu souboru. Pokud má parametr hodnotu 0, změna archivního bitu bude hodnocena jako změna souboru. Pokud má parametr hodnotu 1, změna archivního bitu nebude hodnocena. Pokud se některému souboru změní více parametrů, než pouze hodnota archivního bitu, bude jeho změna zobrazena.

NoSubdirs

Parametr „NoSubdirs“ obsahuje logickou hodnotu 0 nebo 1, která určuje, zda bude program zpracovávat i soubory v podadresářích vybrané oblasti pro testování. Pokud má parametr hodnotu 1, nebudou zpracovávány soubory v žádném podadresáři. Hodnota 0 znamená, že soubory v podadresářích budou testovány.

ReportMode

Parametr „ReportMode“ obsahuje logickou hodnotu 0 nebo 1, která určuje, zda bude program schopen změněná data zapsat do datového souboru. Pokud má hodnotu 0, program pracuje ve standardním režimu. Pokud má hodnotu 1, program pracuje v tzv. REPORT módu, ve kterém není schopen udělat žádnou změnu v již existujícím datovém souboru.

Ovládání programu

Ovládání programu neobsahuje žádné zvláštní postupy nebo prvky, které by se lišily od ovládání většiny standardních programů pro systému. Program je možno ovládat klávesnicí a myší, přičemž postupy a ovládací prvky jsou naprosto standardní.

Menu programu

Menu AGW sdružuje všechny funkce programu. Je jej možné ovládat klávesnicí i myší bez jakýchkoli problémů.

Nepřístupné položky menu jsou zobrazeny pomocí šedivé barvy. Přístupnost jednotlivých položek se řídí aktuálním stavem programu.

Menu Soubor

Menu Soubor obsahuje následující položky:

Vyber oblasti...

Položka „Vyber oblasti...“ slouží pro vyvolání dialogu, ve kterém je možné vybrat oblasti pro testování. Bližší popis dialogu naleznete v příslušné kapitole. Přímý výběr položky je možný klávesnicovou zkratkou „Ctrl–O“.

Ulož data

Položka „Ulož data“ slouží pro uložení změněných a vybraných dat do datového souboru AGUARD.DAT. Je důležité si uvědomit, že do datového souboru se uloží jenom vybrané položky. Přímý výběr položky je možný klávesnicovou zkratkou „Ctrl–S“.

Smaž soubor

Položka „Smaž soubor“ slouží pro smazání vybraných souborů na pevných discích. Je důležité si uvědomit, že smazání souborů je ve velké většině případů nevratné. Jejich obnovení si může vyžádat přítomnost odborníka na operační systém. Přímý výběr položky je možný klávesnicovou zkratkou „Del“.

Nastavení

Položka „Nastavení“ slouží pro vyvolání dialogu, ve kterém je možné nastavit jednotlivé pracovní parametry programu. Nastavené parametry jsou ukládány v konfiguračním souboru AVAST!.INI.

Konec

Položka „Konec“ slouží pro ukončení programu. Přímý výběr položky je možný klávesnicovou zkratkou „Alt–F4“.

Menu Funkce

Menu Funkce obsahuje následující položky:

Vyber všechny

Položka menu „Vyber všechny“ slouží pro výběr všech souborů, které jsou v okamžiku vybrání této funkce zobrazeny v hlavní části okna programu. Jsou vybrány i položky, které nejsou aktuálně vidět a jsou přístupné pomocí posuvných lišt. Vybrané položky jsou zobrazeny v inverzních barvách. Jednotlivé soubory je možné vybrat pomocí dvojitého kliku levého tlačítka myši.

Zruš výběr

Položka menu „Zruš výběr“ slouží pro zrušení vybrání všech položek, které jsou v okamžiku použití této funkce vybrány jakýmkoli způsobem. Zrušit vybrání jednotlivých souborů je možné pomocí dvojitého kliku levého tlačítka myši.

Test na viry

Položka menu „Test na viry“ slouží pro otestování vybraných souborů na viry. Testované jsou jenom existující soubory, které nebyly dosud testovány. Výsledek testů se zobrazí přímo vizuálně a v informacích o souboru, které jsou přístupné pomocí pravého tlačítka myši. Infikované soubory jsou zobrazeny pomocí červené barvy.

Vytvoř report

Položka menu „Vytvoř report“ slouží pro vytvoření tzv. Report souborů, které obsahují informace o aktuálním stavu dat pro aktuální testovanou oblast. Soubory jsou vytvořeny v adresáři, odkud byl program AGW spuštěn. Bližší informace o Report souborech naleznete v příslušné kapitole.

Menu Zobraz

Menu Zobraz obsahuje položky, které zapínají a vypínají zobrazování jednotlivých lišt programu. V případě, že je příslušná položka označena, je odpovídající lišta zobrazena. Program obsahuje Stavovou lištu a Pracovní lištu, někdy nazývanou Nástrojová lišta.

Menu Nápověda

Menu Nápověda obsahuje následující položky:

Index

Položka menu „Index“ umožňuje vyvolat soubor s nápovědou. Přímý výběr položky je možný klávesnicovou zkratkou „F1“.

Copyright

Položka menu „Copyright“ umožňuje zobrazit dialog Dialog Copyright se stručnými informacemi o programu.

Pracovní lišta

Pracovní nebo nástrojová lišta slouží k rychlému přístupu k nabízeným funkcím programu. Jednotlivá tlačítka zobrazená na pracovní liště vizuálně zobrazují funkce, které reprezentují. Jejich funkce je stejná jako funkce odpovídajících položek menu. Některá tlačítka nemají svůj přímý ekvivalent položek menu a slouží ke zjednodušenému ovládání programu pomocí myši.

Klávesa ESC

Klávesa ESC slouží pro přerušení delší nepřerušované činnosti programu, na kterou nemůže uživatel z nějakých důvodů čekat. Uživatel může přerušit testování jednotlivé oblasti, hledání smazaných souborů nebo čekání na uložení do datového souboru.

Pro přerušení některé činnosti je možné použít přímo klávesu ESC nebo příslušné tlačítko pracovní lišty.

Kontextová nápověda

Kontextová nápověda slouží k rychlému získání informací o programu AGW. Použití myši velice zjednodušuje výběr části programu, o které můžete získat nápovědu. Stačí myší kliknout na příslušné tlačítko pracovní lišty a pak kliknout na vybranou oblast programu. Pokud existuje nápověda o dané oblasti, bude bez odkladu zobrazena.

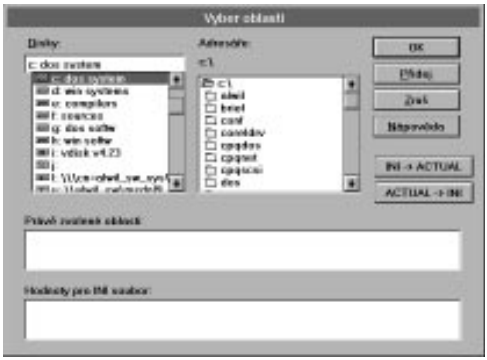
Stavová lišta

Stavová lišta programu slouží k zobrazení stavových informací o stavu programu a testované oblasti. Celá stavová lišta je rozdělena na dvě hlavní části. V levé z nich se zobrazují informace o vybraných položkách myši nebo tlačítkách pracovní lišty.

V pravé části pracovní lišty jsou 4 indikátory počtu, které zobrazují počet zavirovaných souborů, počet vybraných souborů, počet zpracovaných souborů a počet všech souborů.

Dialogy programu

Dialogy programu AGW představují samostatná okna, která zobrazují nebo požadují výběr nějaké informace. Jejich určení je různé a tomu odpovídá i jejich podoba.



Dialog Vyber oblasti

Dialog pro výběr oblastí pro testování je jedním z hlavních prvků programu.

Dialog představuje modifikovanou verzi standardního dialogu pro otevírání souborů. Oproti standardnímu dialogu je zde vypuštěn seznam souborů ve vybraném adresáři a navíc jsou zařazeny dvě editační okna, ve kterých se zobrazují vybrané oblasti pro testování a dvě tlačítka, která slouží pro práci s obsahem těchto editačních oken.

Disky

V seznamu jsou zobrazeny aktuálně přístupné lokální i vzdálené disky, ze kterých je možno vybírat testované oblasti.

Adresáře

V seznamu jsou zobrazeny aktuálně přístupné adresáře, které je možno vybírat pro testování. Těsně nad seznamem je zobrazen aktuálně vybraný adresář.

Právě zvolené

Editační okno „Právě zvolené“ obsahuje seznam oblastí, které se po stisknutí tlačítka OK otestují. Do seznamu je možno přidat některou oblast (adresář) pomocí tlačítka Přidej nebo přímým napsáním textu.

Hodnoty pro INI soubor

Editační okno „Hodnoty pro INI soubor“ obsahuje seznam oblastí, které se automaticky otestují při startu programu v případě, že máte nastaven příslušný přepínač v dialogu Nastavení. Editační okno můžete přímo editovat nebo jej zpracovávat k tomu určenými tlačítky.

OK

Tlačítko „OK“ informuje program o tom, že máte nastaveny oblasti pro testování a program může začít svou práci. V případě, že je editační okno „Právě zvolené“ prázdné, otestuje se adresář, který je aktuálně vybrán a jeho jméno je zobrazeno těsně nad seznamem aktuálně přístupných adresářů.

Přidej

Tlačítko „Přidej“ slouží pro přidání vybraného adresáře do editačního okna „Právě zvolené“. Při přidávání do editačního okna se kontroluje, zda je přidávaná oblast již popsána předchozími oblastmi nebo ne. Pokud je, nová oblast není přidána a uživatel je informován.

Zruš

Tlačítko „Zruš“ informuje program o tom, že se uživatel rozmyslel a nechce dále pokračovat v práci. Tlačítko smaže okno a veškeré změny v editačních oknech nebudou brány na zřetel.

Nápověda

Tlačítko „Nápověda“ slouží k vyvolání nápovědy o programu AGW. Při vyvolání nápovědy se zobrazí tato stránka.

INI–>Actual

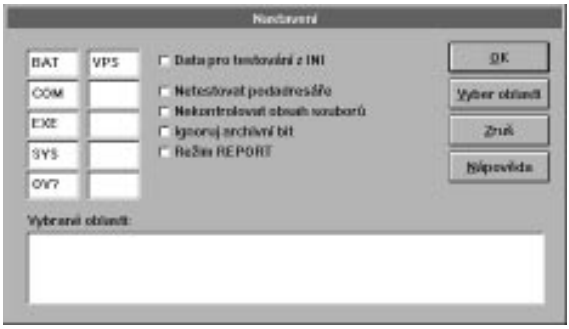
Tlačítko „INI–>Actual“ slouží k zkopírování obsahu editačního okna „Hodnoty pro INI soubor“ do okna „Právě zvolené“.

Actual–>INI

Tlačítko „Actual–>INI“ slouží k zkopírování obsahu editačního okna „Právě zvolené“ do okna „Hodnoty pro INI soubor“.

Dialog Nastavení

Dialog „Nastavení“ slouží k nastavení parametrů programu, které mohou modifikovat jeho chování. Nastavené parametry se ukládají do konfiguračního souboru AVAST!.INI.



Typy souborů

Program AGW umožňuje testovat až deset typů různých souborů. Pokud chcete testovat více typů, můžete použít speciální znaky (wildchars), například typ „*“ znamená, že program bude testovat všechny soubory. Typ souborů může být dlouhý maximálně 3 znaky. V případě, že napíšete více znaků, program na to upozorní.

Vybrané oblasti

Editační okno „Vybrané oblasti“ obsahuje seznam adresářů, které jsou automaticky testovány při startu programu v případě, že máte označen přepínač „Data pro testování z INI“. Obsah editačního okna se zobrazuje v dialogu pro výběr oblastí pro testování v editačním okně „Hodnoty pro INI soubor“. Editační okno je možné přímo editovat nebo je možné určit jednotlivé oblasti pomocí dialogu pro výběr oblastí pro testování.

Data pro testování z INI

Přepínač určuje, zda se při startu programu AGW automaticky otestují oblasti uložené v konfiguračním souboru AVAST!.INI nebo bude program čekat na manuální určení testovaných oblastí.

Netestovat podadresáře

Přepínač určuje, zda bude program AGW testovat i podadresáře vybraných adresářů. V případě, že chcete otestovat kompletně celý disk, je nutné ponechat tento přepínač označen a vybrat si ROOT adresář jako testovanou oblast.

Nekontrolovat obsah souborů

Přepínač určuje, zda bude program kontrolovat změny obsahu souborů. Při testování jednotlivých souborů se pokaždé testuje změna času a data vytvoření, délky a atributů. Obsah souboru může a nemusí být testován. V případě, že není testován, je rychlost programu značně větší, ale nezískáte kompletní informaci. Zároveň, pokud netestujete obsah souborů, přijdete o možnost restaurování původního obsahu souboru.

Ignoruj archivní bit

Přepínač určuje, zda bude program brát do úvahy i změnu archivního bitu v atributech souborů. Pokud je přepínač označen, je změna obsahu archivního bitu ignorována. V případě změny několika parametrů souboru je změna archivního bitu vypsána společně s ostatními změnami.

Režim Report

Přepínač určuje, zda bude program schopen zapisovat výsledky práce do datového souboru. Pokud je přepínač označen, program nebude schopen změnit datový soubor a výsledky testování si můžete jenom prohlédnout na obrazovce.

OK

Tlačítko informuje program, že nastavené parametry jsou správné a mají se použít při další práci programu. Okno dialogu je smazáno z obrazovky a parametry jsou uloženy do konfiguračního souboru.

Vyber oblasti

Tlačítko vyvolá dialog pro výběr oblastí a po jejich výběru nastaví vybrané oblasti do editačního okna.

Zruš

Tlačítko informuje program o tom, že nastavené parametry nejsou správné a nemají se dále používat. Okno dialogu je smazáno z obrazovky a změny parametrů nejsou zapsány.

Nápověda

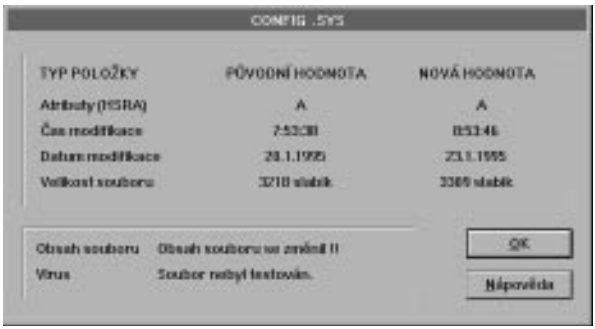
Tlačítko vyvolá soubor nápovědy o programu AGW a zobrazí tuto stránku.

Dialog Copyright

Dialog Copyright slouží pro zobrazení velice stručných informací o verzi programu a autorských právech, které jsou k programu vázány.

Dialog Stav souboru

Dialog Stav souborů je určen pro zobrazení popisu změn souborů, které jsou zobrazeny v hlavní části pracovního okna. Dialog zobrazuje přehlednou tabulku se seznamem změn, které průběhem času nastaly. V případě, že byl soubor smazán nebo naopak vytvořen je příslušný sloupec tabulky prázdný.



Dialog Zprávy, Varování nebo Chyby

Dialog pro zprávu, varování nebo chybu je určen pro jednoduché zobrazení příslušné informace. V záhlaví okna je zobrazen text, který určuje program a typ zprávy, která je zobrazena. Navíc je text zprávy zobrazen v různých barvách, které dále upozorňují na závažnost sdělení.

Normální zpráva je napsána standardní černou barvou, varování je světle modré, chyba je fialová a závažná chyba je světle červená.

Dialog tohoto typu nabízí jenom jednu variantu odpovědi, což je odpověď „OK“, kterou uživatel dá najevo, že si informaci přečetl a bere ji na vědomí.

Program je po dobu zobrazení dialogu pozastaven. Ostatní programu systému Windows nejsou nijak ovlivněny. Dialog tohoto typu používají všechny programy systému AVAST!

Dialog Dotazu

Dialog pro dotaz je určen pro zobrazení nějakého dotazu a získání odpovědi od uživatele. V záhlaví okna je zobrazen text, který určuje program a typ zprávy, která je zobrazena, což je v tomto případě pokaždé dotaz. Navíc je text zprávy zobrazen v různých barvách, které dále upozorňují na závažnost sdělení.

Normální zpráva je napsána standardní černou barvou, varování je světle modré, chyba je fialová a závažná chyba je světle červená.

Dialog tohoto typu nabízí jenom dvě varianty odpovědi. Kladnou odpověď je možné zadat tlačítkem „ANO“, zápornou tlačítkem „NE“.

Program je po dobu zobrazení dialogu pozastaven. Ostatní programu systému Windows nejsou nijak ovlivněny. Dialog tohoto typu používají všechny programy systému AVAST!

Tlačítka myši

Myš se v program AGW používá stejným způsobem jako ve většině ostatních programů určených pro Systém Windows. Pro zjednodušení ovládání programu však byly implementovány některé postupy, které práci urychlují nebo zjednodušují.

Levé tlačítko

Levé tlačítko má zvláštní význam pouze v hlavní části pracovního okna. Na této ploše je možné použít jednoduchý klik myši na nastavení klávesnicového kurzoru na položku, na kterou ukazuje kurzor myši. Dvojitý klik levého tlačítka označí danou položku za vybranou nebo toto označení smaže.

Střední tlačítko

Střední tlačítko není součástí všech typů myši a také jeho simulace není standardizováva, takže obsluha středního tlačítka není v programu AGW implementována žádným způsobem.

Pravé tlačítko

Pravé tlačítko myši se používá pro zobrazení dialogu o stavu souboru. Dialog je zobrazen ihned po jednoduchém kliku pravého tlačítka. Pravé tlačítko ve aktivní jenom v případě, že kurzor myši ukazuje na některý rádek s popisem změny souboru.

Hlavní část okna

Hlavní část okna je oblast, ve které se zobrazují změněné soubory. Těchto souborů může být více, než pojme okno najednou. V tom případě je při pravém okraji okna zobrazí posuvná lišta, kterou je možné seznam souborů posouvat.

Každá zobrazená položka se skládá z několika částí. Na levé straně je jméno souboru s plnou cestou. Na pravé straně je zobrazen stav souboru, jak se soubor změnil od posledního spuštění programu.

Hlavní část okna je možno obsluhovat myší nebo klávesnicí. Popis obsluhy myší si můžete přečíst v příslušné kapitole. Pokud dáváte přednost obsluze klávesnicí, můžete ji také používat. Pro tyto potřeby je implementován kurzor klávesnice, který je zobrazen jako znak „»“ těsně vedle jmen souborů. Kurzor můžete obsluhovat standardními klávesami.

Report soubory

Report soubory je možné vytvořit pomocí tlačítka. Program AGW podobně jako AGUARD pro DOS vytváří dva soubory, se jménem AGW–[jméno disku].ALL a AGW–[jméno disku].DIF. Soubory jsou vytvořeny v adresáři, odkud byl program spuštěn a jejich obsah je tvořen pouze textem v kódové stránce 1250 česky nebo česky bez diakritiky v závislosti na módu práce programu.

Formát souborů je pokaždé stejný a v budoucnu se pravděpodobně nebude měnit, takže výstup je možné zpracovávat dalším programem.

Po dobu vytváření report souborů je pozastavena práce programu AGW a vzhledem k návrhu systému Windows také práce všech ostatních programů.

Původ programu

Program AGW ve své verzi 7.0 j první implementací pro systém Windows. Je součástí systému AVAST! od verze 7.0 a jeho číslování je stejné jako číslování verzí systému AVAST!.

Program AGW odvozuje svůj původ od programu AGUARD pro DOS, který je součástí systému AVAST! již od verze 1.0. Při své práci používá stejné interní algoritmy pro zjišťování změn souborů, takže výsledky, které můžete při práci s programem nebo jeho pracovními soubory spatřit jsou stejná, jako ty, která produkuje program AGUARD pro DOS.

Program má téměř stejné schopnosti, jako jeho DOSový protějšek s několika změnami.

1. Program pracuje výhradně v systému Windows.
2. Program umožňuje interaktivní nastavení testovaných oblastí.
3. Program neumožňuje obnovování změněných souborů.

Požadavky pro práci

Program AGW pro svou práci požaduje:

1. Microsoft Windows 3.1 nebo novější 16–ti bitový operační systém
2. Počítač s procesorem minimálně 80386sx nebo plně kompatibilním.
3. Pro testování souborů je nutná správná instalace knihovny AWANTI.386.

Seznam zpráv, varování, chyb a dotazů

AGW je schopen zobrazit několik různých druhů varování a chybových hlášení, která zobrazuje v různé formě. Jejich seznam a bližší informace o možných variantách jsou uvedeny níže.

Opakovaný test oblasti. Oblast „ANYAREA“ je již pokrytá a není ji zapotřebí přidávat. Opakované testování stejných dat pouze zatěžuje procesor a nemá další význam. Položka nepřidána.

Při výběru další oblasti pro testování program AGW zjistil, že tato oblast je již zařazena do testování. Takto nastavená data nemají smysl a nová oblast nebude zařazena.

Vybraný disk je CD–ROM disk. Program není možné použít na otestování tohoto média. Požadavek zrušen.

AGW potřebuje uchovávat datový soubor v ROOT adresáři testovaného disku. Zápis na médium v mechanice CD–ROM není možný a proto AGW odmítne pracovat s tímto diskem.

Konfigurační soubor není uložen. Program detekoval chybu při ukládání změněných parametrů na disk. Změny nejsou uloženy a nejsou akceptovány.

Program detekoval chyb při ukládání konfiguračního souboru na disk. Chyba není způsobena programem, ale operačním systémem nebo chybou na disku. V každém případě nejsou změněná data uložena na disk.

Vybraný adresář je příliš velký. Oblast paměti, která udržuje seznam vybraných oblastí pro testování není neomezená. Vybraný adresář již přesahuje danou oblast. Požadavek zrušen.

AGW má jenom omezené možnosti co se týče uchovávaní pracovních dat v paměti. Tyto možnosti sice nejsou omezeny 16–ti bitovou strukturou systému Windows (segmentací paměti), ale přesto všechno

vybraná oblast pro testování přesahuje možnosti programu.

Chyba čtení disku. Program nemůže přečíst systémovou oblast disku X. Systémová oblast není testována.

AGW nemohl přečíst systémovou oblast nějakého disku. Tato skutečnost je z největší pravděpodobností způsobena jiným programem, který přístup do těchto oblastí zakazuje.

Výjimka testování. Disk X je obsluhován STACKERem. Jeho systémová oblast je neustále modifikována. Systémová oblast disku není testována.

Program STACKER při své práci neustále zaznamenává své interní data do BOOT sektoru disku, který obsluhuje. AGW tyto změny samozřejmě zjistí a změnu ohlásí. Protože tyto změny jsou legální a hlavně neustálé, program zjišťuje přítomnost STACKERu na testovaném disku a v případě jeho přítomnosti netestuje BOOT sektor.

Smazat označené soubory ? Pokud odpovíte ANO, budou všechny označené soubory nenávratně smazány z pevného disku. Opravdu je chcete smazat ?

AGW umožňuje smazat označené soubory. Smazání je ovšem často nevratná funkce a proto AGW vypisuje toto hlášení.

Nedostatek paměti. Program nemá dostatek místa, pravděpodobně v lokální paměti. Požadovaná akce nemůže být vykonána a je zrušena.

AGW je limitován systémem Windows a velikost lokální paměti je velice malá. Operace, kterou si zvolil uživatel, přesahuje možnosti systému.

Nedostatek globální paměti. Program nemá dostatek místa v globální paměti. Ukončete některý program a zkuste znovu. Požadovaná akce je zrušena.

AGW pro paměťově náročné operace používá hlavní paměť systému Windows. Její nedostatek znemožňuje provedení vybrané operace.

Chyba přístupu k testovanému souboru. Program zjistil chybu při práci s některým souborem. Testování oblasti není úplné !

AGW z nějakého důvodu nemůže přečíst část testovaného souboru. Tato chyba byla způsobena systémem Windows nebo chybou na disku.

Špatná verze otevíraného souboru. Program není schopen zpracovat informace uložené v souboru z důvodu nekompatibility verze. Smažte soubor AGUARD.DAT a zkuste znova.

AGW si do datového souboru ukládá číslo verze programu, který tento datový soubor vytvořil. S postupem času se struktura souboru mění a program je schopen rozhodnout, zda datový soubor je s programem kompatibilní nebo ne.

Špatný obsah otevíraného souboru. Program není schopen zpracovat informace uložené v souboru z důvodu jejich neautorizované změny. Obnovte soubor AGUARD.DAT ze záložní kopie a opakujte znova.

AGW si do datového souboru zaznamenává informace, které později slouží pro ověření jeho konzistence. Pokud jiný program změní obsah tohoto souboru, nemůže ho AGW použít.

Chyba otevírání souboru. Nemohu otevřít soubor ANYFILE. Soubor nebude testován.

AGW nemůže otevřít soubor pro testování. Soubor existuje, ale jiný program brání jeho otevření tím, že

ho má otevřený sám nebo brání k přístupu k němu jiným způsobem.

Chyba hledání souboru. Při hledání souboru byla zjištěna obecná chyba. Program nemůže pokračovat v testování této oblasti.

AGW zjistil obecnou chybu při hledání souboru. Tato chyba je způsobena systémem Windows nebo chybou na pevném disku.

Chyba přístupu k paměti. Program nemůže přistoupit k dříve alokované paměti. Požadovaná akce nemůže být uskutečněna.

AGW nemůže přistoupit k dříve alokované paměti. Tato paměť by měla být přístupná ale z neznámého důvodu není. Tato chyba vznikla v programu AGW nebo v jádře systému Windows.

Chyba při obnovování dat v databázi. Tato chyba vznikla při interním zpracovávání změn, která jste si přál uložit na disk. Pokud se vyskytne častěji, volejte ALWIL Software a žádejte nápravu.

Při ukládání dat na disk je potřeba změnit formát dat tak, aby byly kompatibilní s programem Aguard pro DOS. Tato změna formátu by pokaždé měla proběhnout bez problémů. Pokud tomu tak není, spojte se přímo s firmou ALWIL Software a konzultujte problém s odpovědným pracovníkem.

Změněná data nebyla uložena na disk. V průběhu ukládáni dat došlo k chybě a data nemohla být uložena. Původní soubor zůstal nezměněn.

AGW zjistil chybu při ukládání datového suboru na disk. Chyba vznikla v systému Windows nebo na pevném disku. Nejčastější příčinou může být nedostatek místa na cílovém disku.

Nemohu smazat požadované soubory. Váš požadavek nemůže být vykonán z důvodu chyby v přístupu k paměti.

AGW při požadavku na mazání souborů zjistil chybu v přístupu k databázi umístěné v paměti. Tato chyba vznikla v programu AGW.

Nemohu smazat soubor. Váš požadavek na smazání souborů nemůže být plně vykonán z důvodu chyby v přístupu k souboru „ANYFILE“.

AGW nemůže smazat vybraný soubor. Tato chyba vznikla v systému Windows nebo na pevném disku. Nejpravděpodobnější příčina je to, že soubor byl smazán jiným programem, nebo jiný program brání k přístupu k tomuto souboru.

Chyba při antivirovém testu. Soubor ANYFILE nebude testován na přítomnost virů z důvodů nedostatku paměti nebo chyby v přístupu k souboru.

AGW nemůže otestovat vybraný soubor na přítomnost virů. Pro otestování souboru je potřeba ho celý načíst do operační paměti. Pokud tedy není tato paměť k dispozici nebo soubor není přístupný, otestování nemůže být provedeno.

Chyba vytváření REPORT souboru. Program zjistil chybu při práci se souborem ANYFILE. Report soubory nejsou kompletní.

AGW zjistil chybu při vytváření REPORT souboru. Tato chyba vznikla v operačním systému Windows nebo na disku. Nepravděpodobnější příčinou vzniku je nedostatek místa na disku.

Změna obsahu systémové oblasti. Systémová oblast disku X se změnila. Je tato změna v pořádku ?

Tento dotaz je zobrazen jako důsledek změny obsahu systémové oblasti testovaného disku. Její změna, pokud nemá legální vysvětlení, téměř pokaždé

znamená napadení systému virem nebo jinou, stejně závažnou poruchu práce počítače.

Uložit změny na disk ? Po potvrzení tohoto příkazu budou označené soubory prohlášeny za správné a změněná databáze bude uložena na disk. Pokud odpovíte NE, program se Vás zeptá na možnost zrušení načtených dat.

AGW uloží do datového souboru jenom ty změny, které uživatel označí.

Zrušit načtená data ? Pokud odpovíte ANO, budou zjištěná data smazána a databáze na disku zůstane beze změny. Pokud odpovíte NE, program se vrátí k zpracovávání seznamu změněných souborů.

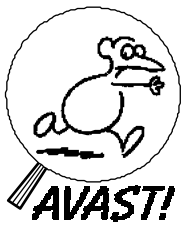
Načtení dat o testované oblasti může být déletrvající procedura. AGW vás varuje před neuváženým zrušením získaných výsledků.

Ukončit aplikaci v průběhu práce ? Požadavek ukončit program uprostřed práce není obvyklý. Pokud Vás okno programu obtěžuje, zmenšete ho do tvaru ikony.

Ukončení programu uprostřed práce opravdu není obvyklým požadavkem.

Ukončit aplikaci bez uložení dat ? Váš požadavek není obvyklý. Pokud opravdu chcete ukončit program bez uložení dat, stiskněte tlačítko ANO.

Ukončení programu uprostřed práce opravdu není obvyklým požadavkem.



Tato stránka je úmyslně prázdná

Viry a počítačové sítě

Počítačové viry a sítě jsou kapitolou samy pro sebe. Ne snad proto, že by viry nějak speciálně síť využívaly či narušovaly, ale prostě proto, že v prostředí, sdíleném mnoha uživateli, může dojít k daleko rychlejší nákaze viry a její odstranění je mnohem komplikovanější než u samostatných počítačů. Také možnost reinfekce – opětovného napadení sítě – je mnohem větší.

Koncepce ochrany v počítačové síti je založena na ověření totožnosti uživatele (definovaného například pomocí jména a hesla) a na tom, že tomuto uživateli jsou přiděleny určité pravomoci. Problém, před kterým ovšem taková síť stojí, je v tom, že je sice prověřen (a předpokládejme, že správně) uživatel, ovšem zdaleka nemusí být prověřeny programy, které spouští. Přitom tyto programy automaticky získávají všechna přístupová práva daného uživatele. Pokud například uživatel s minimálními pravomocemi nahraje do jediného adresáře, který má přístupný, nějaký program a spustí ho, pak tento program nemá přístup do jiných oblastí, spravovaných sítí. Jestliže ale tentýž program později spustí uživatel s právy Supervisora, má tentýž program rázem obrovské pravomoci.

V praxi je proto nutné důsledně využívat ty typy ochran, které síť nabízí. Které to jsou? Soubory mohou mít například nastaveny (podobně jako v DOSu) určité atributy. Rozdíl je v tom, že atributů je více, a není zdaleka tak jednoduché je změnit. Navíc oproti DOSu existuje například atribut „pouze pro spuštění“ (execute only), který umožňuje takto chráněné programy spouštět, ale již ne číst, kopírovat či modifikovat. Podobné atributy mohou být specifikovány pro přístup uživatele k adresářům či souborům. Tato koncepce však pro některé programy bohužel nevyhovuje. Řada programů nemůže být chráněna proti zápisu, protože například zapisuje svoji konfiguraci sama do sebe, a toho není v uvedeném případě schopna. I atribut „pouze pro spuštění“ je potřeba používat uváženě. Může totiž být dvousečný: je pravda, že takto

chráněné programy nemohou být viry napadeny, nemohou však být ani kontrolovány antivirovými prostředky, a pokud by byly infikovány již při své instalaci, virus by se poměrně špatně hledal. Navíc jsou zde často opět problémy s určitými programy: pokud takový program obsahuje overlay, kterou sám načítá, nebude fungovat. A takové programy skutečně existují – zářným příkladem může být T602. S tím souvisí i další věci: například nastavení proměnné PATH. Ta určuje adresáře, ve kterých se hledají spouštěné programy. Síť by v žádném případě neměla obsahovat „veřejné“ adresáře, do kterých může nahrávat kdokoli cokoli.Na druhou stranu doporučujeme správci sítě, aby zřídil uživatele s právy super–vizora bez práva zápisu. Tohoto uživatele může správce využít pro testování bez nebezpečí infekce dalších souborů. V kaž–dém případě musí správce sítě této problematice věnovat dostatečnou pozornost.

Jak se viry po sítích vůbec šíří? Ve světě jsou čas od času prováděny experimenty, které zkoumají, jak jsou konkrétní viry schopny se šířit v prostředí sítí a do jaké míry jsou sítě proti nim odolné. Ukazuje se, že často záleží na tom, v jakém okamžiku zavádění sítě je virus aktivován (např. pro Novell před, po či mezi programy IPX, NETx a LOGIN).

V zásadě je možno viry rozdělit podle jejich vztahu k sítím do čtyř skupin:

- na viry, které pracují celkem normálně,
- na viry, které nepracují v síti vůbec,
- na viry, které jsou se sítí v konfliktu,
- na viry, které jsou speciálně pro sítě vytvořeny.

První skupinu tvoří většina virů. Právě pro ně je důležité správná konfigurace všech ochran sítě.

Do druhé skupiny patří bezesporu všechny klasické boot viry. Ty sice mohou napadat jednotlivé stanice sítě, za určitých podmínek dokonce i server, ale nejsou schopny se šířit po síti z jednoho počítače na druhý, jednoduše proto, že síť služby tak nízké úrovně (BIOS) neposkytuje. Dále je možno sem zařadit i některé další viry, které jsou příliš spjaty s DOSem, takže opět nejsou schopny pracovat se vzdálenými zařízeními. To je i případ virů, které používají „tunelování“, tj. techniku, pomocí které hledají vstupní bod pro svoji činnost hluboko

v operačním systému, aby tak obešly použité antivirové ochrany. Často však současně obejdou i síťový software.

Do třetí skupiny patří viry, které jsou s počítačovou sítí v konfliktu. Pokud jsou aktivovány, buď nepracují ony nebo síť. Nejčastějším případem je to, že virus pro svoje rozpoznání v paměti volá nějakou nepoužívanou funkci operačního systému, kterou však ve skutečnosti používá právě síť.

Do čtvrté skupiny můžeme zařadit viry, které přímo obsahují prostředky, využívající možnosti sítě. Vytvoření takového viru je nepoměrně těžší než vytvoření viru pro DOS. Do dneška jsou známy pouze dva druhy virů, jež něco podobného používají. První z nich je virus GP1. Ten monitoruje funkci pro LOGIN a pak se snaží použité jméno a heslo odeslat na předem určené místo. Druhý je virus Yankee.Login, poprvé zachycený a analyzovaný právě u nás, který dělá něco podobného, ale trochu jiným způsobem. Monitoruje, zda náhodou není spuštěn program LOGIN.EXE, a pokud ano, ukládá zjištěné a zakódované jméno a heslo do těla viru v infikovaném souboru.

Zatím není znám virus, který by využíval prostředky sítě hlouběji. Odborníci se již více než dva roky dohadují, zda může existovat hypotetický virus, který by byl schopen šířit se po síti, která má správně nastavené ochrany, tj. obejít ochranné prostředky sítě. Firma Novell tvrdí, že něco takového není v principu možné. Fakt, že se takový virus dosud neobjevil, jí zatím dává za pravdu. Ovšem v počítačové bezpečnosti platí, že 100% ochrana nikdy neexistuje...

AVAST! a podpora sítě

AVAST! samozřejmě práci v síti podporuje. Je zaměřen (vyvíjen a testován) zejména pro síť Novell, v praxi však pracuje i na řadě dalších typů sítí. Všechny programy na síti pracují. Síť Novell je například automaticky rozpoznána paměťově rezidentními programy FGUARD a RGUARD, vyhledávací programy umožňují odeslat v případě výskytu známého druhu viru zprávu vybranému uživateli a podobně.

Je důležité používat AVAST! v souladu s licenčním ujednáním. Počet stanic v síti, které AVAST! využívají, musí od-

povídat počtu licencí. Naše firma nabízí výhodné slevy pro vícenásobné použití programu a určitě je mezi nimi typ, odpovídající vašim potřebám.

Pro správce sítě je nesmírně důležité správně navrhnout a pak udržovat dohodnuté bezpečnostní schéma, které by mělo zahrnovat i ochranu proti virům. U toho je kritické zejména to, jak zabezpečit, že uživatelé antivirové programy vůbec používají, a pak to, aby vždy používali poslední, aktuální verzi, která je k dispozici.

Program CHKAVAST

První problém může být vyřešen pomocí velmi jednoduchého programu CHKAVAST, který je schopen zjistit, zda je v paměti instalován program FGUARD či RGUARD a pomocí návratového kódu ohlásit výsledek. Program funguje samozřejmě úplně obecně, ale je vhodné ho využívat při přihlášení uživatelů do sítě. Uživatele, kteří jeden nebo oba programy nemají v paměti instalovány, je možno jednoduchým způsobem do sítě vůbec nevpustit.

Parametry programu CHKAVAST

Program CHKAVAST může mít dvě skupiny parametrů. První z nich (/F a /R) testuje přítomnopst rezidentních programů v paměti pracovní stanice. Druhá skupina parametrů je určena pro porovnávání systémového data a času s uloženou hodnotou a tak umožnit spouštění sprogramů LGUARD či AGUARD pouze jednou denně, týdně atp.

Parametr F

Tento parametr určuje, že se testuje přítomnost programu FGUARD v paměti pracovní stanice.

Parametr R

Tento parametr určuje, že se testuje přítomnost programu RGUARD v paměti pracovní stanice.

Pokud jsou uvedeny oba parametry nebo ani jeden z nich, testuje se přítomnost obou paměťově rezidentních programů FGUARD a RGUARD.

Návratové kódy

Program CHKAVAST nastaví operačnímu systému návratový kód. Tento kód může být později testován buď jiným (rodičovským) programem nebo v příkazové dávce pomocí příkazu IF ERRORLEVEL, popřípadě v LOGIN scriptu sítě. Návratový kód programu CHKAVAST může nabývat pouze následujících hodnot, které mají tento význam:

0 příslušný program/programy nejsou v paměti pracovní stanice instalovány,

1 příslušný program/programy jsou v paměti pracovní stanice instalovány.

Příklad použití CHKAVAST v LOGIN Scriptu

Pro testování přítomnosti rezidentních programů nejprve vytvořte zvláštní příkazovou dávku TSTAVAST.BAT, která bude mít např. následující obsah:

```
@echo off
rem dávka TSTAVAST.BAT volaná z Login Scriptu
chkavast
if errorlevel 1 goto konec
echo Nemáte nainstalován RGUARD a FGUARD, nemůžete
  být připojen!!
logout
:konec
```

Na konci Login Scriptu uživatele pak musí být řádek:

```
#TSTAVAST
```

Soubory CHKAVAST.COM a TSTAVAST.BAT musí být umístěny v adresáři LOGIN. Pokud program LOGOUT.EXE není umístěn na cestě, je nutno specifikovat jeho přesné umístění.

Testování času a data

CHKAVAST ISTIME hh:mm

Slouží pro zjišťování času; vrací návratový kód 1, pokud je systémový čas vyšší než čas zadaný a 0, pokud je nižší nebo stejný.

CHKAVAST ISDAY [NEW] [OLD] [<den>] [<datum>]

Slouží ke zjištění údajů o nastaveném systémovém datu a dnu a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný den, parametr OLD má opačný význam.

Kromě těchto parametrů je možno použít i anglickou zkratku dne v týdnu a nebo datum, zadané pomocí dvou dvoucifer–ných čísel, udávajících den a měsíc. Pokud je některé z těchto čísel nulové, jedná se o libovolnou hodnotu (00–08 znamená celý srpen, 15–00 je patnáctého v libovolném měsíci). Pro zadání data se bere v úvahu nastavení kódu země (tj. buď evropská nebo americká konvence zadání).

Jednotlivé parametry je možno kombinovat (například pro pátek třináctého), výsledek je správně pouze tehdy, jestliže jsou splněny všechny dílčí podmínky.

Příklad:

```
chkavast isday mon new
if errorlevel 1 goto label1
echo Na začátku týdne provedeme důkladné testy!!
lguard c:\*.* /s /e*
:label1
...
isday 13-00 fri
if errorlevel 1 goto label2
pause Dnes je pátek 13. Přeji vám hodně štěstí...
:label2
```

CHKAVAST ISMONTH [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém měsíci a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný měsíc, parametr OLD má opačný význam.

Příklad:

```
chkavast ismonth new
if errorlevel 1 goto label1
echo Dnes je třeba udělat záložní kopie!!
:label1
...
```

CHKAVAST ISWEEK [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém týdnu a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný týden, parametr OLD má opačný význam.

Příklad (stejná činnost jako u ISDAY ale spolehlivější, protože funguje i v případě svátků či pokud je počítač zapnut například až v úterý):

```
chkavast isweek new
if errorlevel 1 goto label1
echo Na začátku týdne provedeme důkladné testy!!
lguard c:\*.* /s /e*
:label1
...
```

CHKAVAST ISYEAR [NEW] [OLD]

Slouží ke zjištění údaje o tom, zda je počítač spuštěn poprvé v novém roce a k případnému větvení příkazů v dávce. Příkaz nastavuje návratový kód na nulu, pokud je podmínka splněna, či na jedničku, pokud splněna není.

Parametr NEW slouží ke zjištění, zda je počítač spuštěn poprvé v daný rok, parametr OLD má opačný význam.

Příklad:

```
isyear new
if errorlevel 1 goto label1
echo Hodně štěstí v novém roce!!
:label1
...
```

CHKAVAST pro svoji činnost používá soubor AVAST.DAT ve stejném adresáři pro ukládání dat, pokud je použit příkaz NEW či OLD. Parametry ISDAY, ISWEEK, ISMONTH a ISYEAR jsou na sobě nezávislé, tj. pokud například zapnete počítač v pondělí ráno, podmínky ISDAY NEW a ISWEEK new ve dvou po sobě následujících příkazech jsou obě splněny.

Aktualizace programů AVAST! na síti

Velmi důležité je zabezpečit distribuci nové (aktualizované) verze antivirových programů. Ve větších organizacích mají často vypracován celý (např. stromový) postup, jakým se aktualizace dostane až ke každému uživateli. Na počítačové síti to může být poměrně jednoduchá záležitost, a to i tehdy, je-li vhodné, aby se programy nenacházely pouze na serveru, ale i na všech stanicích (například pro testy ještě před přihlášením do sítě). Takovou rychlou distribuci je možno zařídit například takto:

Na serveru je potřeba zřídit veřejný adresář pojmenovaný např. \AVASTNEW\ . Do tohoto adresáře je možno umístit novou verzi souboru AVAST! nebo jeho části (například nový VPS soubor).

Na pracovní stanici je pak možno vždy po přihlášení uživatele vykonat následující příkaz:

```
replace X:\AVASTNEW\*.* C:\AVAST! /U /R
```

„REPLACE“ je standardní součást MS-DOSu. Je to program, který zkopíruje soubory zadané v prvním parametru pouze tehdy, pokud jsou novější než soubory, které odpovídají druhému parametru. Písmeno X odpovídá písmenu, přiřazenému disku počítačové sítě.

Tímto jednoduchým způsobem je možno zajistit, že programové vybavení na všech stanicích je aktualizováno v okamžiku, kdy se z nich někdo poprvé přihlásí. Podrobnosti o systémovém programu Replace je možno najít v dokumentaci MS-DOSu.

Charakteristika některých počítačových virů

V několika dalších odstavcích se můžete seznámit s popisem několika počítačových virů. Doplňky této uživatelské příručky mohou být případně obsaženy v souboru READ.ME na distribuční disketě.

Virus 534 (W–13)

Virus 534 je velmi jednoduchý virus, který se u nás objevil v roce 1990. K šíření viru dochází v okamžiku spuštění infikovaného programu. Napadené programy jsou o 534 slabik delší než původní. Virus napadá soubory typu COM, které se nacházejí v právě platném adresáři, a pokud tam není žádný takový soubor nalezen, v hlavním (kořenovém) adresáři právě platného disku.

Virus 534 neobsahuje žádnou manipulační činnost.

Příznakem viru 534 je změněné datum poslední modifikace souboru, nastavené na nesmyslnou hodnotu 13. měsíc.

Virus 648 (Vienna)

Virus 648 (Vienna, PC–Boot) byl snad prvním počítačovým virem, který se v roce 1988 v Československu objevil. Patřil ve své době určitě k nejrozšířenějším. K šíření tohoto viru dochází v okamžiku spuštění infikovaného programu. Tento virus napadá soubory typu COM a zvětšuje jejich velikost o 648 slabik. Pro svoji činnost využívá systémovou proměnnou PATH, takže se velmi rychle rozšíří po celém systému (díky znalosti PATH napadá nejvíce používané programy).

Jeho destruktivní činnost spočívá v tom, že přibližně každý osmý program, který nalezne, nerozšíří o virus, ale zničí ho (na jeho začátek napíše instrukci pro zavedení systému, původní obsah této části programu je zničen). Velikost zničeného programu se nezvětší.

Příznakem viru 648 je změněný čas poslední modifikace souboru, nastavený na nesmyslnou hodnotu 62 sekund (tato hodnota se nevypisuje příkazy DIR atd.).

Přítomnost viru v systému se projeví tím, že po spuštění některých programů dojde k zavedení systému (popř. k „zamrznutí počítače“).

Virus 744

Virus 744 se u nás objevil v roce 1990. Jedná se o modifikaci viru 648. K šíření viru dochází v okamžiku spuštění infikovaného programu. Tento virus napadá soubory typu COM a zvětšuje jejich velikost o 744 slabik. Pro svoji činnost využívá systémovou proměnnou PATH, takže se velmi rychle rozšíří po celém systému (díky znalosti PATH napadá nejvíce používané programy).

Jeho destruktivní činnost spočívá v tom, že přibližně každý osmý program, který nalezne, nerozšíří o virus, ale zničí ho (na jeho začátek napíše nesmyslnou instrukci, původní obsah této části programu je zničen). Velikost zničeného programu se nezvětší.

Příznakem viru 744 je změněný čas poslední modifikace souboru, nastavený na hodnotu 30 sekund.

Přítomnost viru v systému se projeví tím, že po spuštění některých programů dojde k „zamrznutí počítače“.

Virus 897 (April 1st)

Virus 897 (April 1st, SURIV 1.01) se u nás objevil v roce 1990. Je to paměťově rezidentní virus, který napadá soubory typu COM kromě systémového programu COMMAND.COM. K šíření viru dochází v okamžiku spuštění programu. Virus se šíří tak, že na stejném disku, na kterém je napadený program,

vytvoří pracovní soubor s názvem TMP$$TMP.COM, do kterého zapíše nejprve virus a pak napadený program.

Jeho manipulační činnost spočívá v tom, že 1. dubna vypíše po napadení souboru na obrazovku zprávu „APRIL 1ST HA HA HA YOU HAVE A VIRUS“ a zastaví počítač. Ve dnech 2. dubna až 31. prosince vypíše po napadení souboru zprávu „YOU HAVE A VIRUS !!!“.

Příznakem viru 897 je řetězec „sURIV“ (pozpátku virus) v napadených COM souborech.

Přítomnost viru v systému se projeví tím, že po spuštění některých programů dojde k vypsání zprávy, popřípadě k „zamrznutí počítače“.

Virus 1339 (Vacsina)

Virus 1339 (VACSINA) se v Československu objevil v roce 1989. Jedná se o paměťově rezidentní virus, u něhož je šíření odděleno od okamžiku spuštění infikovaného programu. Virus se instaluje do paměti a poté monitoruje spouštění programů v systému. Napadá soubory typu COM, které zvětšuje o 1339 slabik, některé EXE soubory modifikuje tak, že se stanou programy typu COM (i když mají rozšíření EXE!!), modifikací se prodlouží o 132 slabik a při příštím spuštění mohou být virem napadeny. Virus 1339 je jedním ze skupiny virů, které se mohou navzájem modifikovat, odstraňovat či vzájemně spolupracovat.

Virus 1339 neobsahuje žádnou destruktivní činnost.

Příznakem viru 1339 je určitý kód jak v operační paměti tak na konci napadeného souboru.

Virus 1560 (Alabama)

Virus 1560 (Alabama) se u nás objevil na podzim roku 1990. Je to paměťově rezidentní virus, který napadá soubory typu EXE kromě programů DEBUG a SYMDEB. Šíří se při spouštění programů či otevírání souborů. Nenapadá však program, který je právě spoušten či otevírán, ale jiný EXE program v právě platném adresáři. Jeho zvláštností je i to, že dokáže v paměti „přežít“ reset počítače pomocí stisknutí kombinace kláves „Ctrl Alt Del“.

Manipulační část viru spočívá v tom, že po 674 generacích viru vypíše v rámečku zprávu na obrazovku a zastaví počítač. Zpráva obsahuje text:

„SOFTWARE COPIES ARE PROHIBITED BY INTER–NATIONAL LAW“ a „Box 1055 Tuscambia ALABAMA USA“.

Příznakem viru 1560 je stejně jako u viru 648 změněný čas poslední modifikace souboru, nastavený na nesmyslnou hod–notu 62 sekund.

Virus 1618 (Mixer 1A)

Virus 1618 (MIXER 1A) se u nás se objevil v roce 1990. Je to paměťově rezidentní virus, který napadá soubory typu EXE o délce větší než 8192 slabik. Šíří se v okamžiku spouštění pro–gramů.

Manipulační část viru spočívá v tom, že překódovává znaky odeslané na sériový či paralelní port počítače. Kromě toho po určitém počtu generací a po 50 minutách od nainstalování znemožní reset počítače pomocí klávesnice a po 60 minutách se aktivuje běhání míčku, které je podobné jako u viru Ping–Pong.

Příznakem viru 1618 je řetězec „MIX1“ na konci napadeného programu.

Přítomnost viru se projeví zejména tím, že tiskárna se chová podivně a vypisuje nesmyslné znaky.

Virus 1701 (Cascade)

Virus 1701 se objevil v Československu v roce 1989 a je velmi rozšířen. Napadá soubory s rozšířením COM, zvětšuje jejich velikost o 1701 slabik. V napadeném systému se šíří velice ry–chle. Při prvním spuštění systému se totiž virus umístí v ope–rační paměti počítače a monitoruje veškeré spouštění pro–gramů. Při spuštění programu typu COM virus testuje, zda je tento program virem již napaden a pokud ne, infikuje ho. Šíření tohoto viru je tedy časově oddělené od spuštění napadeného programu.

Jeho manipulační část je poměrně neškodná – v období od října 1988 do konce roku 1988 způsobí to, že na monitoru

náhodně „padají“ znaky shora dolů. Nejprve jich padá pouze několik, postupně se aktivita viru stupňuje, až není takřka možno provádět žádnou jinou činnost. Je–li systémové datum jiné (tj. menší než 1.10.1988 nebo větší než 31.12.1988), virus žádnou manipulační činnost neprovádí.

Příznakem viru 1701 je délka kódu viru. Virus zjišťuje, zda program začíná instrukcí skoku a zda má skok určitou délku od konce souboru (jedná se o skok na začátek viru).

Přítomnost viru v systému se mimo výše zmíněné období (tj. i v současné době) bez speciálních prostředků dá odhalit velmi těžko. Virus neničí data, programy fungují.

Virus 1800 (Dark Avenger)

Virus 1800 (Dark Avenger, Bulharský, Sofijský) k nám přišel v roce 1989. Je to velmi nebezpečný paměťově rezidentní virus, který napadá programy typu COM i EXE. Šíří se velmi rychle, protože programy nenapadá pouze v okamžiku jejich spuštění jako většina ostatních virů, ale i při dalších operacích s nimi (vytvoření, uzavření, zjištění atributů, přejmenování atd.). Napadené programy obsahují texty: „Eddie lives...somewhere in time!“ a „This program was written in the city of Sofia (C) 1988–89 Dark Avenger“. Virus modifikuje zaváděcí sektor disků.

Destruktivní činnost viru 1800 spočívá v tom, že po každých šestnácti programech spuštěných z daného disku přepíše náhodný cluster na disku svým kódem, čímž jeho původní obsah zničí. To je velmi zákeřné, protože zničená data mohou být velmi důležitá a jejich rekonstrukce obtížná.

Virus 1800 nemá svůj vlastní příznak, testuje přítomnost celého svého kódu v testovaném souboru.

Virus 1813 (Friday 13th)

Virus 1813 (Pátek 13.) je snad nejpopulárnějším virem vůbec. U nás se objevil na podzim roku 1989. Je to paměťově rezidentní virus, který napadá soubory typu COM a EXE. Soubory typu EXE napadá díky chybě, kterou v sobě obsahuje, vícenásobně. Bývá označován jako politický virus, protože poprvé se

měl projevit v Izraeli v květnu 1988 v předvečer 40. výročí jeho založení. Virus nenapadá program COMMAND.COM.

Manipulační část viru spočívá v tom, že zhruba po půl hodině od instalování do paměti vytvoří na obrazovce okénko a od tohoto okamžiku začne zpomalovat chod počítače. Každý pátek 13. maže všechny soubory, které byly spuštěny.

Příznakem viru 1813 je řetězec „MsDos“ v napadených COM souborech.

Přítomnost viru v systému se mimo pátek 13. projeví zpomaleným chodem počítače.

Virus 2881 (Yankee Doodle)

Virus 2881 (Yankee Doodle) je virem, který se u nás objevil na podzim 1989. Je to nebezpečný, paměťově rezidentní virus, který obsahuje velké množství mechanismů pro své maskování a obranu. Umožňuje například korekci vlastního kódu, umí sám sebe za jistých podmínek z napadeného programu odstranit apod. Patří do stejné skupiny virů jako virus 1339. Napadá soubory typu COM i EXE v okamžiku jejich spuštění.

Manipulační část viru spočívá v tom, že modifikuje Ping–Pong virus, pokud ho v daném počítači nalezne, a dále v tom, že za určitých podmínek zahraje v 17 hodin písničku Yankee Doodle.

Příznakem viru 2881 je určitý kód na konci napadeného programu.

Virus 2928 (Yankee Doodle)

Virus 2928 (Yankee Doodle) je starší verzí předchozího viru. Je o 47 slabik delší a jediný rozdíl v jeho činnosti je ten, že písničku Yankee Doodle zahraje v 17 hodin pokaždé.

Ping–Pong virus

Ping–pong virus se u nás objevil v červenci 1989. Šíří se velmi rychle. Tento virus vůbec nenapadá soubory, pouze systémovou oblast disku, nazývanou zaváděcí sektor (boot sektor). Při napadení disku přepíše zaváděcí sektor disku vlastním

kódem, kromě toho najde na disku volný cluster, který označí za vadný, a do tohoto clusteru zapíše druhou část svého kódu a původní obsah zaváděcího sektoru. Při pokusu o zavedení systému z infikovaného disku se instaluje do paměti (zmenší paměť o 2KB) a hlídá přístup k diskům. Při pokusu o čtení z dosud neinfikovaného disku tento disk napadne výše popsaným způsobem. Na pevný disk se rozšíří při pokusu o zavedení systému z infikované diskety, což se může stát i omylem, pokud zapomenete v jednotce A disketu a stisknete Ctrl+Alt+Del. Pokud tato situace nastane, doporučujeme vyjmout disketu a stisknout „Ctrl Alt Del". V tomto případě k infikaci pevného disku nedojde!

Manipulační činnost viru spočívá v tom, že za určitých podmínek se začne po obrazovce pohybovat „míček" (znak s kódem 07).

Virus může být modifikován viry 2881 a 2928, takže po 255 zavedeních systému přestane být funkční.

Stoned virus

Stoned virus je boot virus, který nenapadá soubory, ale systémovou část disku, konkrétně zaváděcí sektor disket či tabulku rozdělení disků (DPT) pevných disků. Stoned virus je možno přímo rozpoznat podle toho, že zmenší velikost operační paměti o 2 KB (lze zjistit například pomocí PCTOOLS), v napadených sektorech (tj. v zaváděcím sektoru disket a v DPT u pevných disků) se objevují texty: „Your PC is now Stoned" a „LEGALISE MARIJUANA", přičemž první text se s určitou pravděpodobností objeví na obrazovce při zavedení systému z infikované diskety. Stoned virus přepisuje jeden sektor (stopa 0, hlava 0, sektor 7 na pevném disku a stopa 0, hlava 1, sektor 3 na disketách) na infikovaném médiu. Původní obsah těchto sektorů je přepsán, což může za určitých podmínek vést k porušení a ztrátě dat.

Stoned virus v paměti napadá již jen diskety v jednotce A:. Každá operace s nechráněnou disketou může vést k rozšíření viru! Z infikované diskety se může dostat na pevný disk přes natažení systému z této diskety (tato disketa nemusí být systémová). Stoned virus nerespektuje formát BPB (BIOS Pa–

rameter Block) v boot sektoru disket, proto jsou údaje v tomto bloku nesmyslné, což může opět vést k poškození či ztrátě obsahu diskety.

Virus 2967 (Yankee Doodle)

Virus 2967 je modifikací známého viru 2881 (Yankee Doodle). Jedná se o paměťově rezidentní virus, který napadá soubory typu COM i EXE v okamžiku jejich spuštění. Oproti viru 2881 chybí většina mechanismů pro maskování a obranu. Navíc je však rutina, která monitoruje spuštění programu LOGIN.EXE (součást sítě Novell) a poté shromažďuje kódovaná jména uživatelů sítě Novell a jejich hesla. Virus se objevil v Československu na jaře 1991.

Virus 1575 (Caterpillar)

Virus 1575 je paměťově rezidentní virus, který napadá programy typu COM i EXE v okamžiku jejich vyhledávání (např. při příkazech DIR či COPY). Dva měsíce po napadení programu se na obrazovce objeví „virus“ v podobě „housenky“, která se pohybuje zleva doprava a shora dolů a posunuje znaky na obrazovce.

Bloody! virus

Bloody! je paměťově rezidentní virus, který napadá systémovou oblast disků: boot sektor disket a tabulku rozdělení pevných disků. Po 128. zavedení systému z infikovaného pevného disku vypíše zprávu „Bloody! Jun. 4, 1989“. V uvedený den došlo v Pekingu k masakru na náměstí Nebeského klidu. Na discích typu IDE může dojít ke ztrátě dat na pevném disku!!

Virus Michelangelo

V září 1991 se v Československu objevil nový, dosud neznámý druh počítačového viru, nazvaný Michelangelo. Tento virus napadá systémovou oblast disků, konkrétně zaváděcí sektor disket a sektor s tabulkou rozdělení disků u pevných

disků. Je odvozen z již dříve známého viru Stoned a není nijak zvlášť pozoruhodný. S jedinou výjimkou, a tou je jeho manipulační část. Virus totiž může být velmi nebezpečný. Při každém spuštění testuje datum v počítači a dne 6. března přepíše obsah disku, ze kterého byl spuštěn! Virus Michelangelo čte datum přímo ze zálohovaných hodin počítače (v okamžiku jeho spuštění není totiž ještě DOS aktivní a datum nastavené v operačním systému není možno jistit), proto se přepsání disků nikdy neprovede na počítačích bez baterií zálohovaných hodin (klasický IBM PC/XT).

Virus Stoned (2)

Stoned (2) virus (NoInt, Arc Hub) je boot virus, který nenapadá soubory, ale systémovou část disku, konkrétně zaváděcí sektor disket či DPT pevných disků. Je odvozen z viru Stoned a je možno jej přímo rozpoznat podle toho, že zmenší velikost operační paměti o 2 KB. Stoned (2) virus přepisuje jeden sektor (stopa 0, hlava 0, sektor 7 na pevném disku a stopa 0, hlava 1, sektor 3 na disketách) na infikovaném médiu. Původní obsah těchto sektorů je přepsán, což může za určitých podmínek vést k porušení a ztrátě dat. Virus obsahuje textový řetězec „ARC HUB 8A“.

Stoned (2) virus používá techniku stealth: v případě čtení/zápisu infikovaného sektoru je místo něho přečten/zapsán originální sektor. Pokud je tedy virus aktivní, nemohou některé antivirové programy jeho přítomnost na disku detekovat.

Stoned (2) virus v paměti napadá již jen diskety v jednotce A:. Každá operace s nechráněnou disketou může vést k rozšíření viru! Z infikované diskety se může dostat na pevný disk přes natažení systému z této diskety (tato disketa nemusí být systémová). Stoned virus nerespektuje formát BPB (BIOS Parameter Block) v boot sektoru disket, proto jsou údaje v tomto bloku nesmyslné, což může opět vést k poškození či ztrátě obsahu diskety.

Virus 1376 (Helloween)

Začátkem roku 1992 se v Československu objevil nový druh počítačového viru, který byl prokazatelně vytvořen u nás. Jde o virus 1376 (Helloween). Tento paměťově rezidentní virus napadá soubory typu COM i EXE, neinfikuje některé antivirové programy, a to i československého původu. Testuje datum v počítači a dne 1. listopadu napíše na obrazovku zprávu:

```
Nesedte porad u pocitace a zkuste jednou delat
   neco rozumneho!
******************
!! Poslouchejte HELLOWEEN - nejlepsi metalovou
   skupinu !!
```

a poté provede reset počítače. Jinou manipulační činnost tento virus neobsahuje.

Virus DIR II

Virus DIR II se liší od všech ostatních druhů virů. Je dlouhý 1024 slabik a je zvláštní v tom, že sice napadá programy typu COM a EXE, ale soubory, ve kterých jsou tyto programy uloženy, vůbec nemodifikuje. Na infikovaném disku se vyskytuje pouze jedenkrát. Pochází z Bulharska a v poslední době je u nás poměrně značně rozšířen.

Po svém spuštění se virus instaluje do paměti a pak prochází zřetězené ovladače zařízení (device drivers) a připojí se k nim tak, že je při každém volání diskových operací aktivován. Používá funkce Strategy a Interrupt. Po instalaci spustí hostitelský program a normálním způsobem se ukončí. Paměťově rezidentní virus pak monitoruje přístup na disk a jednak hlídá funkce Build BPB (kvůli správné funkci programu typu CHKDSK) a jednak napadá disky a adresáře.

Infekční rutinu viru je možno rozdělit do dvou částí. První souvisí s napadením celého disku. Virus zjistí poslední cluster na disku, zapíše do něho sebe sama a v tabulce FAT jej zvláštním způsobem označí jako obsazený. Pokud tento cluster náležel nějakému souboru, je tento soubor virem přepsán a zničen.

Je to však jediná škoda, kterou virus může trvale způsobit. Druhá část infekční rutiny souvisí s modifikací adresářů. Virus totiž manipuluje s položkou v adresáři, ve které je uloženo místo na disku, na kterém soubor začíná (First Cluster Pointer, FCP). Virus změní tento parametr u všech souborů typu EXE a COM tak, že všechny programy začínají kódem viru. Originální hodnota je zakódována a uložena na volné (rezervované) místo v položce adresáře. Virus tímto způsobem najednou napadá všechny soubory v daném adresáři a proto se velmi rychle šíří. Virus kontroluje pouze rozšíření a ne jméno souboru, a proto napadá i smazané soubory (!!!). Virus neustále při práci s adresářem přepíná položky FCP mezi původními a modifikovanými hodnotami, aby mohl operační systém vůbec pracovat. Jako vedlejší efekt z toho vyplývají i určité vlastnosti typu Stealth (skrývání).

Pokud je virus aktivní v paměti, chová se počítač celkem normálně. Když je však zaveden systém z čisté diskety, jsou všechny napadené soubory pouze 1024 slabik dlouhé a program CHKDSK hlásí miliony chyb (všechny programy začínají na stejném místě). Stejným způsobem se chová infikovaná disketa v nezavirovaném počítači.

Po zjištění viru v počítači lze jen těžko napadené soubory zálohovat. Pokud je virus v paměti, jsou na záložní média přeneseny infikované programy, pokud není virus aktivní, je na disku pouze velký zmatek. Existuje velmi jednoduchý způsob, jak může bez zvláštních prostředků virus z disku odstranit i naprostý laik. Stačí totiž v okamžiku, kdy je virus aktivní, přejmenovat ve všech adresářích všechny soubory typu COM (například na *.CO) a EXE (například na *.EX). Virus sám uvede příslušné položky adresáře do původního stavu. Pokud chcete zachránit i programy na disketách, je nutno provést stejný úkon i na nich. Poté je nutno zavést systém z originální diskety a všechny soubory přejmenovat zpět. Programem CHKDSK je možno odstranit cluster obsazený virem. Program, který i po tomto kroku virus obsahuje, je pravděpodobným zdrojem celé nákazy.

Virus Jack Ripper

Tento boot virus se po své aktivaci instaluje pod hranici 640KB operační paměti, zmenší zbývající velikost volné paměti o 2KB, přesměruje vektor přerušení 13h a otestuje, zda je již napaden pevný disk počítače. Pokud ne, virus provede zápis svého kódu do tabulky rozdělení disku (DPT). Svou druhou část uloží do sektoru 8, hlava 0, stopa 0. Originální DTP je umístěna v sektoru 9, hlava 0, stopa 0. Virus pak zavede do paměti originální DPT sektor a předá mu řízení.

Virus sleduje při zápisu či čtení diskety, zda je již napadena. Pokud není, tak se zapíše do jejího boot sektoru a do předposledního sektoru v základním adresáři. Do následujícího sektoru uloží původní boot sektor.Každá operace s nechráněnou disketou tak vede k jejímu napadení a dalšímu šíření viru.

Jack Ripper používá techniky stealth. Pokud je virus aktivní, monitoruje požadavky na čtení a zápis sektoru. Při pokusu číst DPT předloží originální DPT, při pokusu o zápis DPT se operace neprovede. Při čtení sektorů 8 nebo 9 se přečtou samé nuly.

Virus v sobě obsahuje znakový řetězec „(C) 1992 Jack Ripper“. Tento řetězec, je jak na pevném disku, tak i na disketách kódován.

Škodlivá činnost tohoto viru je velmi zákeřná. Virus při zápisu sektoru prohodí s pravděpodobností asi 1:1024 dvě náhodně vybraná slova v zapisovaném sektoru. A protože se nejčastěji zapisují data, může to vést k hromadění nevysvětlitelných chyb.

Tento virus je detekován programy LGUARD, RGUARD i AGUARD. Odstraněn může být jak programem FDISK /MBR (od verze DOSu 5.0), tak i programem BGUARD (pokud ovšem máte předem uložený původní stav disku). Z disket se odstraní pomocí programu BGUARD.

Virus J&M (JiMi)

Virus J&M (Hasita) je boot virus. Po své aktivaci se instaluje na konec operační paměti a zmenší zbývající část o 2KB. Otestuje, zda je pevný disk počítače již napaden. Není–li, virus uloží svůj kód do DPT a originální DPT do sektoru 6, hlava 0, stopa 0. Virus přesměruje vektor přerušení 13h, načte do paměti originální boot sektor a předá mu řízení.

Virus testuje operace s disketou a pokud není ještě napadena, zapíše svůj kód do jejího boot sektoru. Originální boot sektor přesune do sektoru 14, hlava 1, stopa 0.

Virus v sobě obsahuje znakový řetězec J&M. Tento řetězec není nijak kodován a virus ho používá ke své identifikaci.

Virus po své aktivaci testuje aktuální datum. Pokud je 15. listopadu, pokusí se formátovat stopu 0, hlavu 0 prvého pevného disku. Pokud mu tuto činnost řadič disku povolí, virus přepíše sám sebe spolu s originální DPT.

Tento virus je detekován programy LGUARD, RGUARD i AGUARD. Odstraněn může být jak programem FDISK/MBR (od verze DOSu 5.0), tak i programem BGUARD (pokud ovšem máte předem uložený původní stav disku). Z disket se odstraní pomocí programu BGUARD.

Virus One Half

Tento virus je paměťově rezidentní, multipartitní, tunelující, stealth a polymorfní. Virus po své aktivaci nejprve krokuje přerušení 13h až do segmentu DOSu. Pak se pokusí infikovat tabulku rozdělení pevného disku (DPT). Pokud se mu to povede, uloží své tělo do posledních 7 sektorů nulté stopy, původní DPT do osmého sektoru od konce stopy a ukončí svou činnost. V případě, že se mu infekce pevného disku nezdaří, stane se okamžitě rezidentním a napadá soubory typu COM i EXE delší než 1000 slabik. Soubory napadá při jejich spuštění, otevření či přejmenování, a to jak na pevném disku tak i na disketách nebo síťových discích. Virus testuje jména souborů a nenapadá soubory SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV A CHKDSK.

Po zavedení systému z napadeného pevného disku si virus vyhradí poslední 4KB paměti RAM, instaluje se do vyhrazené paměti a stane se rezidentním. Nyní napadá soubory pouze na disketách či na síťových discích. Napadené soubory prodlužuje o 3544 nebo 3577 slabik. Příznakem napadení souboru je určitá závislost mezi datem a časem vzniku souboru.

Autor viru One Half se nejspíše nechal inspirovat bulharským virem Commander Bomber. Podobně jako v tomto viru i zde je dekódovací smyčka rozprostřena v deseti úsecích náhodně rozmístěných po původním souboru. Jednotlivé úseky jsou navzájem provázány dvěma typy skoků a jsou doplněny náhodnými jednoslabikovými instrukcemi. Celá tato konstrukce dekodovací smyčky má dvojí účel. Jednak jsou napadené soubory bez dekodování virem v paměti nefunkční a běžnými metodami z nich nelze virus odstranit, jednak nelze tento virus vyhledávat pomocí textového řetězce.

Škody, které může tento virus napáchat, mohou být značné. Po každém zavedení systému virus zaxoruje poslední dvě stopy každého povrchu pevného disku s náhodným číslem, které si vygeneruje při instalaci do DPT. Číslo poslední kodované stopy si uchovává ve svém zavaděči v DPT. Po zakódování poloviny disku se v zavislosti na datu může zobrazit hlášení:

```
"DIS IS ONE HALF ... PRESS ANY KEY TO CONTINUE".
```

Virus pak pokračuje v kódování. První třetinu disku virus ponechá nezakódovanou.

One Half používá techniky stealth. Pokud je virus v paměti aktivní, není xorování disku ani prodloužení napadených souboru patrné.

Virus může být z DPT odstraněn jak systémovým programem FDISK /MBR (od verze DOSu 5.0), tak i programem BGUARD. Napadené soubory je nejlepší smazat a nahradit ze záložních kopii. Před odstraněním viru z disku, doporučuji zazálohovat důležitá data, ještě pokud je virus aktivní v paměti. Jinak se totiž může stát že budou umístěny v již zakódované části disku a odstraněním viru z DPT o ně nenávratně přijdete.

Virus Tremor

Tremor je polymorfní virus, který napadá programy typu COM (o délce 8192 až 55039 slabik) a EXE (o délce 8192 až 1048576 slabik) a je paměťově rezidentní. Při spuštění napadeného programu se virus nejprve dekóduje, a pak testuje aktuální datum. Pokud od data napadení dosud neuplynuly alespoň 3 měsíce, případně je soubor v jiném adresáři než byl napaden, virus modifikuje vlastní kód a neprojevuje se žádnými zvukovými ani obrazovými efekty. Dále virus testuje svou přítomnost v operační paměti pomocí přerušení 21h funkce 0F1E9h. Pokud je virus již v paměti aktivní nebo je verze DOSu menší než 3.30, je řízení předáno napadenému programu. V případě, že virus dosud v paměti není, instaluje se do paměti XMS nebo do UMB. Pokud se nepovede ani jedna z těchto variant, instaluje se na vrchol základní operační paměti. Přitom si v paměti alokuje 4288 slabik. Virus pomocí prerušení 01h testuje jednak možnou přítomnost debuggerů, jednak si zjistí adresu přerušení 21h, kterou pak používá k přímému volání jádra systému. Adresy přerušení 21h a 15h přesměruje do nepoužité oblasti MCB hostitelského programu a odtud pak skáče přímo do své rezidentní části. Infikuje program specifikovaný proměnnou 'COMSPEC=', nejčastěji COMMAND.COM a spustí původní program.

Tremor používá techniky stealth. Pokud je virus aktivní, monitoruje činnost systému a informace, které by mohli vést k jeho odhalení, předává systému ve zkreslené formě. Např. při dotazu na délku souboru předá původní délku napadených souborů atd. Při spuštění programu, virus testuje, zda jméno souboru nezačíná CH, ME, MI, F2, F–, SY, SI a PM. Pokud ano, provede změny v alokaci paměti, takže např. CHKDSK vrací jakoby správné hodnoty velikosti volné paměti. Virus nenapadá programy začínající znaky SC, CL nebo HB. Virus také testuje, zda druhý a třetí znak jména programu je RJ. V takovém případě začne dávat systému pravdivé informace o souborech. Znamená to, že archivy ARJ budou obsahovat virus, kdežto např. v ZIPech virus nebude. Podobně kopie zdravého i napadeného souboru vytvořené pomocí systémového COPY virus neobsahují, zatímco obě kopie udělané pomocí Nortona jsou

infikovány. Zjistí–li virus přítomnost antivirového programu FLU–SHOT+, soubor nenapadne a přestane se jakkoliv projevovat. Tremor také testuje přítomnost antivirového programu VSAFE z DOSu 6.00. Pomocí speciálních funkcí přerušení 13h umí virus uvést VSAFE do neaktivního stavu a po napadení souboru zase zaktivovat.

Virus otevře soubor a přečte si posledních dvacet slabik. Vcelku jednoduše je dekóduje a pokud obsahují slovo „DEAD“ a datum souboru je zvětšené o 100 let předpokládá, že je soubor již napaden. V opačném případě virus přihraje svou zakódovanou kopii na konec napadeného programu, přesměruje počáteční skok nebo změní hodnotu v hlavičce EXE souboru a spustí původní program.

Napadené soubory prodlužuje o 4000 slabik, datum napadených souboru zvětšuje o 100 let. Při volání přerušení 15h vypisuje uvedenou zprávu. Při volání přerušení 21h posouvá celou obrazovku doleva a doprava o jeden znak.

```
-=> T×R×E×M×O×R was done by NEUROBASHER / May-
   June'92, Germany <=-
-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-
```

Virus může být odstraněn buď zrušením napadených souborů a jejich nahražením z originálních disket, nebo pomocí programu AGUARD (pokud ho ovšem pravidelně používáte).

17.11.1989 (Pojer)

Tento virus je domácího původu. Po svém spuštění se nejprve dekóduje a zjišťuje svoji přítomnost v operační paměti. Pokud v paměti není, instaluje se poměrně standardním způsobem na její konec. Přesměrovává vektor přerušení 21h (služby DOSu) a v únoru, červenci, září a v prosinci v liché dny také časovač (vektor 1Ch). Nakonec spustí hostitelský program.

Paměťově rezidentní virus pak monitoruje funkci spouštění programů a napadá spouštěné COM a EXE soubory. Obsahuje v sobě tabulku se jmény programů, které nenapadá. Jedná se o programy SCAN, CLEAN a podobně, celkem jde o 8 antivirových programů. V okamžiku infikování přesměrovává vektor přerušení 24h (kritická chyba), takže nedochází k systémovým chybovým hlášením při neúspěšných pokusech o napadení

programu. Infikované soubory jsou delší o 1919 slabik, virus je velmi jednoduchým způsobem kódován.

Pokud je napadený program spuštěn 17. listopadu nebo 6. února (proč?), virus vypíše za doprovodných zvukových efektů uvedenou zprávu a pak pokračuje ve své normální činnosti. Kromě toho ve dnech, kdy instaluje vlastní rutinu pro časovač (viz výše), vykresluje v levém horním rohu obrazovky střídavě mezeru a „obdélník“.

```
  **  B R A I N  2  v1.40  **
WARNING ! Your PC has been WANKed !
>> 17.11.1989 <<
Viruses against political extremes , for freedom and parliamentary democracy
>> STOP LENINISM , STOP KLAUSISM , STOP BLOODY DOGMATIC IDEOLOGY !! <<

Remarks:
 - for John McAfee: John,your SCAN = good program.
 - for CN and his company:
   Boys,the best ANTI-VIRUSES are Zeryk,Saryk and Vorisek !
 - for F : Girls are better than computers and programming !

This program is copyright by  SB SOFTWARE  All rights reserved.
O.K. Your PC is now ready !
```

Jde o velmi primitivní virus, jehož autor nemá příliš jasno jak v politice, tak v angličtině a nakonec i v programování a morálce. Virus obsahuje řadu základních omylů ve všech zmíněných oblastech.

Civil Defense

Jedná se o virus, který evidentně pochází z Ruska. Je napsán tak, že pracuje pouze na počítačích třídy 286 a vyšších. Typ počítače však také testuje.

Virus napadá sektor s tabulkou rozdělení disku a soubory typu EXE. Při zapnutí infikovaného počítače zmenší velikost paměti o 7 KB a instaluje vektory přerušení pro časovač, klávesnici, tiskárnu a později pro DOS. Neinstaluje vektor přerušení 13h tak, jako většina ostatních boot virů. Pak monitoruje funkce DOSu a při vyhledávání souborů (Find First a Find Next) napadá programy typu EXE, které jsou na disketě A nebo B. Na disketě nejprve čte a pak zpět zapíše zaváděcí sektor. To slouží jako test na disketu chráněnou proti zápisu. Infikovanými programy je zabezpečen přenos viru z jednoho počítače na druhý. Po spuštění napadeného programu se testuje, zda je napaden pevný disk počítače, a pokud ne, provede se zápis zaváděcího sektoru viru, originálního DPT sektoru a dalších 12

sektorů s virem. Virus se nakonec v každém případě sám z napadeného a spuštěného programu odstraní. Příznakem viru v napadeném souboru je čas poslední modifikace nastavený na hodnotu 54 sekund.

Paměťově rezidentní virus provádí poměrně složitou činnost. Ta je založena na ,,věku" viru v rozmezí od nuly do pěti. Věku 2 odpovídá zhruba 275 hodin aktivního viru v počítači, věku 5 více než 375 hodin. Virus počítá délku své aktivity v minutách, přičemž toto číslo ukládá v rezervované části paměti CMOS. S přibývajícím věkem se zitenzivňuje rušivá činnost viru. Popišme si, jakou činnost virus vykonává v 5. věku. Střídavě bliká se třemi LED světly na klávesnici, simuluje velkou spoustu poruch klávesnice či překlepů. Někdy se znaky prostě nenapíší, jindy se jich vygeneruje několik, někdy se napíší jiné. Při stisknutí funkčních kláves hraje sovětské písně, při kláv–ese Scroll Lock virus zbarví obrazovku do červena, napíše v azbuce ,,Cha cha cha, Sláva KPSS, Naród i pártija jedíny, Privjet ot GKČP", přehraje bývalou sovětskou hymnu a pro–vede reset. Při resetu (Ctrl Alt Del) napíše za zvukových efektů žlutě na modrém pozadí dlouhou ruskou báseň, podepsanou jménem E. Letov (a ,,Graždanskaja oborona", odtud je odvozeno i jméno viru Civil Defense, které je v kódu spolu s verzí 1.1 též uvedeno).

Virus též začne vracet verzi DOSu 2.00, takže řada pro–gramů nepracuje korektně. Při spouštění programů vypíše s pravděpodobností 1 : 15 zprávu ,,Formatting disc c: complete. Format another ? (y/n) " a čeká na odpověď. Pokud zní odpověď Yes, virus oznámí, že je pevný disk zformátován, a pak chvíli čte sektory na disku. Neformátuje!! Pokud zní odpověď No, virus napíše ,,Ech, kak žal, veď mě tak chatělos eto sdělat" a pokračuje normálně v činnosti. Po dvaceti minutách od akti–vování počítače se zprava objeví žlutý ,,píst", který vytlačí za zvuků písně text vlevo. Na jeho ose je nápis ,,Vas privětstvujet virus CDV ver. 1.1 ..." Kromě těchto efektů virus též monitoruje, co se tiskne na tiskárně, a určitá ruská slova nahrazuje jinými.

V–Sign

Tento boot virus se podle své manipulační rutiny nazývá V–Sign a má několik zajímavých vlastností. Virus zabírá dva sektory na disku a neuchovává původní sektor. Do něho totiž zapisuje jen svůj vlastní krátký *loader*, který po aktivaci přepíše v paměti původním obsahem. Navíc virus obsahuje (jako jeden z mála boot virů) lehce polymorfní rysy. Cyklicky totiž přehazuje některé instrukce loaderu tak, že mají pokaždé jiné pořadí.

Při zavedení systému z infikovaného média loader viru nejprve načte dva sektory s tělem viru do paměti, alokuje si 2 KB paměti těsně pod hranicí 640 KB a zkopíruje se do ní. Modifikuje vektor přerušení 13h (práce s diskem), obnoví původní obsah zaváděcího sektoru a předá mu řízení.

Virus pak monitoruje přerušení 13h a při operacích čtení a zápis je schopen se šířit. Pokud je na pevném disku čten libovolný sektor na stopě 0, hlavě 0, je při následující operaci testována přítomnost viru na disku. U disket virus testuje první slabiku tabulky FAT a podle něj rozpoznává typ diskety, což potřebuje pro určení pozice, na kterou uloží sám sebe.

Virus V–Sign má ještě jednu pozoruhodnou vlastnost. Při své instalaci do paměti totiž testuje přítomnost boot viru Stoned v paměti a dokáže si z něho *ukradnout* původní hodnotu přerušení 13h a přepsat ho v paměti. Navíc, pokud zjistí, že daný disk je jím samým již napaden, zkouší napadnout i sektor, do kterého virus Stoned ukládá původní zaváděcí sektor. Je tak možné, že odstraněním viru Stoned některými antivirovými programy dojde k následné reinfekci virem V–Sign. V oblasti virů sice odstranění jednoho viru druhým není novinkou, ale metoda viru V–Sign je dost unikátní.

Manipulační rutina viru spočívá v tom, že na obrazovce je vypsáno veliké písmeno V, složené ze semigrafických znaků. Výpis je *zpožďován*, takže se celý obrázek objevuje postupně. Poté je program zacyklen tak, že nemůže pokračovat a je nutno znovu počítač spustit.

Manipulační rutina nastane velmi zřídka, a sice pouze tehdy, je–li úspěšně napadeno 64 disket. Protože je však čítač vynulován při každé instalaci viru do paměti, musí se jednat o

napadení v rámci jednoho *sezení*, což asi nebude příliš obvyklé. Podobná situace snad může nastat pouze při velkoobjemovém formátování či při zálohování velkých disků na diskety.

Základní informace o makrovirech

Makroviry tvoří poměrně novou skupinou virů. První makrovirus se objevil v létě 1995. Od té doby se jejich počet zvyšuje a zejména ve velkých firmách představuje zcela nové nebezpečí. Ačkoli jejich základní princip je stejný jako u „normálních" virů, představují úplně novou koncepci. Napadají totiž „dokumenty", které již nejsou pouhými datovými soubory, ale obsahují i celou řadu dalších věcí, jako jsou například makra. Tyto makra jsou součástí dokumentu a představují plnohodnotné programy, vytvářené ve vyšším programovacím jazyce (Word Basic, Visual Basic). Řada produktů pak provádí tyto krátké programy, a to i zcela automaticky (například při spuštění programu, při otevření dokumentu, při skončení práce s dokumentem a podobně). Tyto programy umožňují také předefinovat menu, význam kláves a podobně. A to jsou všechno oblasti, ve které bohužel makroviry mají šanci se uplatnit.

Základní princip, že virus musí být aktivován, aby mohl provádět svoji činnost, zůstává tedy nezměněn. Přesto má existence makrovirů velký dopad na náš přístup k virové problematice. Je potřeba prohledávat i „datové" soubory, viry se mohou šířit na různé platformy počítačů či operačních systémů (ve skutečnosti je platformou samotný aplikační program, např. MS–Word) a viry se mohou velmi rychle šířit elektronickou poštou, ať už v rámci jedné firmy či třeba přes Internet. S tímto novým fenoménem se uživatelé musí vypořádat zejména tím, že si uvědomí existující nebezpečí a přijmou odpovídající organizační opatření.

Další viry

Nové viry se objevují zcela pravidelně. Jejich popis můžete najít v souboru READ.ME na distribuční disketě.

Likvidace virů v systému

V této kapitole bychom vás rádi seznámili s tím, jak se zachovat v okamžiku, kdy zjistíte napadení vašeho systému počítačovými viry. Podle mnoha průzkumů se to stalo již miliónům uživatelů výpočetní techniky po celém světě, a tak je bohužel vysoká pravděpodobnost, že přes veškerá preventivní opatření se to může jednou přihodit i vám.

Nejdůležitější je v takovém okamžiku nepropadnout panice a zachovat klid. Neuvážená akce může totiž způsobit mnohem větší škody než virus samotný.

Jelikož jste uživatel, který nerad riskuje, máte jistě všechna důležitá data a programy zálohovány, takže ani kompletní zničení obsahu vašeho disku by vás nezaskočilo. Navíc jste určitě uživatel pozorný a pečlivý, takže přítomnost viru jste odhalil poměrně včas, tedy dříve, než mohl napáchat velké škody. Aktivní virus je možno zjistit například pozorováním neobvyklého chování systému, jako jsou grafické a zvukové efekty, neobvyklá chybová hlášení, neznámá aktivita disků, chyby dosud bezvadně fungujících programů apod. nebo pomocí programového vybavení AVAST!. Z tohoto důvodu je nesmírně důležité pravidelně používat program AGUARD a při každé změně konfigurace pevného disku uložit nová data programem BGUARD!!!

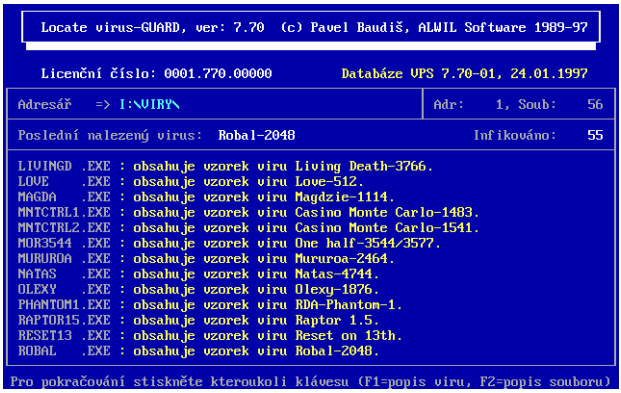
Pokud tedy zjistíte (například pomocí programů SGUARD, AGUARD nebo FGUARD) nesrovnalosti, které nelze nějakým racionálním způsobem vysvětlit (změna délky či obsahu souborů, nepovolená manipulace se soubory, podivné diskové operace, změny v operační paměti atd.), je třeba nejprve pomocí programu LGUARD zjistit, zda v systému není přítomen některý ze známých virů, které umí tento program odhalit. Program LGUARD by si měl poradit s naprostou většinou dnešních virů.

Pokud zjistíte na svém počítači virus, je potřeba zavést operační systém z originální systémové diskety, kterou jste dostali s počítačem nebo ze systémové diskety, která byla vytvořena při instalaci AVAST!. Tato disketa musí být chráněna proti zápisu!!! Tak je zajištěno, že virus není v paměti aktivní. Pak je důležité nespouštět žádný program z pevného disku, ale pouze z prověřených disket.

Nejlepším způsobem odstranění viru je smazání infikovaných programů a jejich nová instalace z originálních distribučních disket. To však bohužel není vždy možné. Druhou nejlepší metodou je přepsání napadených programů ze záložních kopií. Je však důležité uchovat alespoň jeden infikovaný program (například na zvláštní a výrazně označené disketě) pro pozdější prověření, o jaký druh viru se přesně jedná.

Obecné odstranění virů

Obecné odstranění počítačových virů má řadu výhod. Obecné metody fungují i na neznámé druhy virů a často jsou schopny výsledek své práce zkontrolovat a ověřit. To se může týkat virů neznámých, ale i známých, takže může nastat například následující situace:



Pokud se vám přihodí něco podobného (věříme, že ne v tomto rozsahu!), je vhodné podezřelý program zkopírovat na disketu a spojit se s pracovníky ALWIL Software a virus

bude analyzován. Stejným způsobem je třeba postupovat, pokud nebyl virus ve vašem systému nalezen programem LGUARD a vy jste přesto přesvědčeni, že se skutečně o virus jedná.

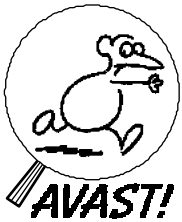
Pro obecné odstranění virů je pak potřeba nahrát systém z „čisté“ systémové diskety (nejlépe z té, která byla vytvořena při instalaci programového vybavení AVAST!). Programem AGUARD pak snadno odhalíte všechny soubory, které byly virem nelegálně modifikovány. AGUARD je schopen zkontrolovat, zda modifikované soubory obsahují některý ze známých druhů virů. Program AGUARD vám také umožňuje obnovit původní soubor a tak odstranit virus (detaily způsobu odstranění známých i neznámých druhů virů najdete v příslušné kapitole. Celou operaci doporučujeme zakončit opětovným spuštěním programu AGUARD, což vám umožní zjistit, zda jsou obnovené soubory skutečně v původním stavu. Takové ověření je velikou výhodou této metody – zda jsou obnovené soubory do posledního bitu stejné jako před napadením.

Pro obecné odstranění boot virů je možno použít program BGUARD. Ten je schopen obnovit původní obsah systémové oblasti pevného disku z diskety, a tak přepsat zde uložený boot virus. Program AGUARD je pak schopen ověřit, že systémová oblast disku je ve stejném stavu, jako byla předtím. Boot viry na disketách mohou být též programem BGUARD odstraněny.

Hlášení výskytu viru

V řadě zemí je uzákoněno, že výskyt viru na počítači je nutno hlásit policii. U nás nic takového neexistuje, přesto je ale sběr takových informací velice užitečný. Je totiž dobré (a to jak pro nás, tak pro uživatele) vědět, jaké viry a v jaké míře se u nás vyskytují. Proto jsme připravili jednoduchý dotazník, který je ve formě souboru uložen na distribuční disketě a jehož kopie je přiložena k této dokumentaci. Byli bychom vám velmi vděčni, pokud byste si v případě napadení vašeho systému našel chvilku času, vyplnil ho a odeslal na naši adresu. Údaje, které do dotazníku uvedete, budeme po–

važovat za důvěrné a použijeme je pouze pro celkový statistický přehled. Za tuto spolupráci vám předem děkujeme!



Vnitřní zabudovaná ochrana AVAST!

Programy antivirového souboru AVAST! obsahují vlastní mechanismus, který umožňuje zjistit jejich případnou modifikaci virem. Při svém spuštění nejdříve testují, zda nebyly samy změněny, a pokud ano, ohlásí tuto skutečnost uživateli, např.:

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

Press any key to continue...
```

Toto hlášení slouží jako upozornění uživateli, že byl program modifikován. Jeho hlavní význam tkví v tom, že uživatel je včas varován. Po stisknutí kterékoli klávesy program pokračuje ve své normální činnosti, je však pravděpodobné, že v tomto okamžiku byl již virus aktivován.

Přejeme vám, aby se vám počítačové viry zdaleka vyhnuly. A pokud se přece jen objeví, aby vám naše programové vybavení pomohlo překonat všechny problémy, které vám počítačové viry způsobily.

Tato stránka je úmyslně prázdná

Dodatek

UPOZORNĚNÍ:

ALWIL Software nenese **v žádném případě** odpovědnost za případné škody způsobené jakýmkoli počítačovým virem!!!

Práva uživatelů našich programů

- v případě nesprávné funkce programu, která je v rozporu s touto nebo s obsahem souboru READ.ME na distribuční disketě, možnost osobní, písemné nebo telefonické konzultace,
- uživatelé mají právo používat antivirovou službu AVS, která je finančně i technicky velmi výhodná. Služba AVS se platí vždy na jeden rok.
- v případě námětů na rozšíření možností tohoto programového vybavení se obracet písemně na níže uvedenou adresu,
- v případě napadení vašeho systému neznámým typem viru možnost osobní, písemné, E–mail nebo telefonické konzultace s pracovníky ALWIL Software.
- programové vybavení komunikuje s uživatelem česky, znaky obsahují diakritická znaménka. Standardně je dodáván s rozšířeným ASCII kódem „MJK“. Kód je možno změnit pomocí přepínače z příkazové řádky při spuštění programu. Na vyžádání je možno dodat i program, který implicitně komunikuje s uživatelem v kódu Latin 2, popřípadě bez diakritických znamének (pak není nutno spouštět s příslušným přepínačem). K dispozici je i anglická verze programů.

Naše adresa:
ALWIL Software, Lipí 1244,
193 00 Praha 9, Horní Počernice
tel: (02) 685 59 61 nebo 63, fax: (02) 685 56 24,
BBS: (02) 782 25 50

E–mail: baudis@alwil.anet.cz
WWW: http://www.anet.cz/alwil/alwil.htm

Tato stránka je úmyslně prázdná

Rejstřík

Symboly

A

B

D

F

H

Ch

I

K

L

M

N

O

P

R

S

T

V

W

Z