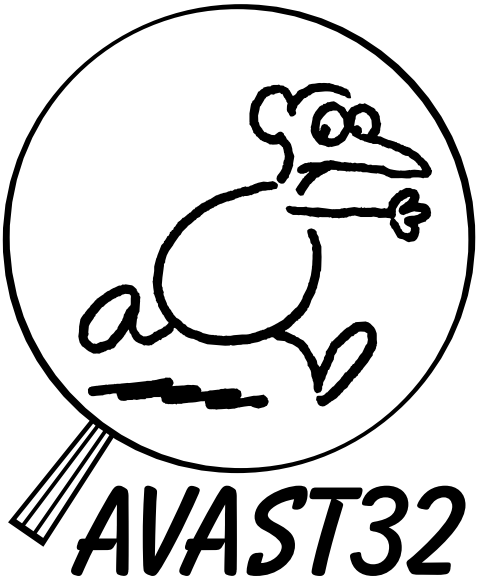


Soubor antivirových programů pro Windows 95 a Windows NT verze 1.2

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: DataLine Technology
Tisk: Tiskárna Hugo

Obsah

Tato stránka je úmyslně prázdná

Vítejte

- **Co je AVAST32?**
- **Vlastnosti a výhody AVAST32**
- **Nabídka AVAST32**
- **Program pro hledání virů – klasický scanner**
- **Program pro testování integrity dat**
- **Testování v reálném čase – permanentní testování**
- **Uživatelské rozhraní AVAST32**
- **Nároky na technické a programové vybavení**
- **Jiné nároky**
- **Podpora uživatelů**
- **Jak kontaktovat prodejce – obchodní informace**
- **Jak získat technické informace**

Co je AVAST32?

AVAST32 je soubor antivirových programů, který je schopen zjistit přítomnost viru na počítači pracujícím pod operačním systémem Microsoft Windows 95 nebo Microsoft Windows NT. AVAST32 je schopen objevit velké množství známých virů a navíc je schopen detekovat činnost nebo následky činnosti neznámých nebo modifikovaných virů, které není prozatím možné detekovat přímo.

AVAST32 omezuje na minimum jedno z velkých nebezpečí ztráty dat, hrozících převážné většině uživatelů výpočetní techniky. Správné používání antivirového systému společně s dalšími programy správy dat (například zálohování) a správnou organizací přístupu k počítači nebo počítačové síti s největší pravděpodobností zabrání infekci počítače a tím přinejmenším odboural starosti co s virem.

Že jste se ještě s virovou nákazou nesetkali? Pak patříte mezi několik málo opravdu šťastných procent populace pracující s počítačem. Nicméně **tato skutečnost ještě neznamená, že právě váš počítač není nakažen!!**

AVAST32 je přímým následníkem již dobře známého antivirového souboru AVAST!, který pracuje v systému DOS a Microsoft Windows 3.x. Jeho struktura a činnost je velice blízká jeho předchůdci, ale vlastní implementace je zcela nová, plně využívá všech vlastností nejnovějších operačních systémů pro osobní počítače. Nové vlastnosti a prostředky těchto operačních systémů dovolily změnit algoritmy systému, který tak nyní poskytuje velice kvalitní ochranu.

Vlastnosti a výhody AVAST32

1. univerzálně použitelný antivirový systém pro Microsoft Windows 95 a Microsoft Windows NT,
2. rychlé a zároveň důkladné testování systému,
3. schopnost průběžného testování v reálném čase (obdoba rezidentních programů DOSu),
4. schopnost obnovit až 95 procent nakažených souborů se stoprocentním ověřením správnosti obnovy,
5. vícevláknová (multithread) struktura všech výkonných programů,
6. kompatibilita s UNC (Universal Naming Convention, způsob zadávání jmen v sítích Microsoft Windows),
7. použití moderních prvků uživatelského rozhraní,
8. snadnost obsluhy pro začátečníky i možnost detailní konfigurace pro odborníky,
9. program je stejně úspěšný při detekci virů a změn jako jeho předchozí 16–ti bitová verze – AVAST!, která získala několik českých i mezinárodních ocenění.

Nabídka AVAST32

AVAST32 nabízí komplexní antivirovou ochranu osobního počítače pracujícího pod operačním systémem Microsoft Windows 95 nebo Microsoft Windows NT. Pojmem „komplexní“ znamená, že systém obsahuje programy pokrývající prakticky všechny oblasti toho, co se skrývá pod pojmem „antivirová ochrana“. To v praxi znamená, že se nejedná jenom o klasický program pro hledání virů, ale systém obsahuje také programy pro testování integrity dat, rezidentní programy (respektive

programy chovající se jako klasické rezidentní programy v DOSu), pomocné utility a samozřejmě také uživatelsky příjemnou nadstavbu. Schopnosti konfigurace systému umožňují práci se systémem počítačově nevzdělaným uživatelům ale i odborníkům, kteří potřebují výsledky bez zbytečných příkras.

Program pro hledání virů – klasický scanner

Jednou z hlavních součástí systému AVAST32 je vyhledávací program, tzv. scanner, který je schopen vyhledat známé viry. Nic více, ani nic méně. Jde o jednu z nejstarších metod boje s antivirovou nákazou. Programy tohoto typu jsou poměrně běžné a jistě jste se již s nimi setkali. Liší se pouze použitou technikou vyhledávaní, rychlostí a spolehlivostí detekce. Jsme hrdi na to, že naše vyhledávací algoritmy jsou opravdu rychlé, produkují velice spolehlivé výsledky a zároveň prakticky nehlásí falešné poplachy. Tuto skutečnost společně se schopností detekce virů považujeme za nejdůležitější vlastnosti dobrého programu tohoto typu.

Z vlastní praxe můžeme doložit, že hlášení falešného poplachu má často horší následky než nehlášení opravdového viru.

Program pro testování integrity dat

Již ne tak rozšířenou metodou boje proti počítačovým virům je zjišťování změn jednotlivých souborů nebo systémových oblastí disku. Je to s podivem, protože detekce změn je principiálně jediná spolehlivá metoda, jak zjistit nekalou činnost virů (ale také jiných uživatelů). Spolehlivost této metody plyne z jednoduchého faktu, že každý virus musí být uložen v permanentní paměti v době, kdy je počítač vypnut. Dnes je prakticky jedinou používanou permanentní pamětí povrch disku libovolného typu (pevný disk, disketa, optický disk, …).

Je zcela zřejmé, že na disku dochází k neustálým změnám, ale v případě, že se změní systémová oblast nebo například procesor příkazů systému DOS (soubor COMMAND.COM), jde prakticky se stoprocentní pravděpodobností o nákazu virem

(samozřejmě pouze v případě, že jste právě nenainstalovali novou verzi operačního systému).

Rychlý test integrity dat

Tento program je určen pro rychlou kontrolu změn obsahu jednotlivých vybraných souborů. Vychází ze stejné metody jako **Program pro testování integrity dat**. Údaje o souborech (kontrolní součty) se však neukládají do databáze, ale do Registru Windows 95 resp. Windows NT, kde jsou uloženy systémové informace těchto dvou prostředí. Množiny souborů, které chceme otestovat v rámci jednoho běhu, zadáváme při nastavení konfigurace programu. Počet souborů v konfiguraci není omezen, avšak velký počet souborů v jedné konfiguraci je v rozporu s filosofií tohoto testu (jednoduchý a rychlý). Při testu se vypočte kontrolní součet souboru a porovná se součtem, uloženým v Registru. Uvedený test je výhodné použít pro rychlé zjištění změn základních důležitých systémových souborů jako např. win.com (command.com), io.sys, gdi.exe, gdi32.dll apod.

Testování v reálném čase – permanentní testování

Soubor antivirových programů naší firmy již dlouho obsahuje možnost průběžného testování spouštěných programů a systémových oblastí disket, což jsou dva nejdůležitější způsoby, kterými může virus proniknout do systému. Můžeme s hrdostí říci, že v systému Microsoft Windows 3.x v současné době nemáme konkurenci. Tuto schopnost jsme implementovali i do systému AVAST32.

Vlastnosti a činnost tohoto programu vyplývají z faktu, že nejčastější způsob jak infikovat Váš počítač, je spustit některý nakažený program nebo nastartovat systém ze zavirovaného disku (nebo diskety).

V předchozím odstavci není považován za infekci proces, při kterém se dostane virus na pevný disk pasivně, například zkopírováním infikovaného souboru. V tomto případě ještě systém není ve skutečnosti napaden, ale má k tomu opravdu blízko.

V poslední době jsme se setkali s jiným způsobem šíření viru, který používá dokumenty a ne spustitelné soubory, ale i v tomto případě jde o šíření pomocí spustitelného kódu, který je v těchto dokumentech umístěn v podobě maker.

AVAST32 je schopen otestovat průběžně každý spouštěný program nebo knihovnu bez ohledu na její typ a bez ohledu na to, odkud byl daný program spuštěn. Toto testování probíhá nezávisle na uživateli **před spuštěním** příslušného souboru. V případě zjištění virové nákazy není infikovaný soubor spuštěn a uživatel je varován.

Podobně probíhají také testy disket. Pro každou disketu vloženou do mechaniky je při prvním přístupu zkontrolován zaváděcí sektor a v případě, že obsahuje virus, je uživatel informován. Samozřejmě použití takto infikované diskety automaticky nezaviruje systém, ale hrozí zde nebezpečí, že ponecháním diskety ve startovací (bootovací) mechanice dojde k infekci při dalším startu počítače. S takto infikovanou disketou lze po potvrzení varování pracovat na rozdíl od zavirovaného souboru, který není možné spustit v žádném případě.

Při testování disket rezidentním vyhledávačem není testován kompletní obsah diskety. Tato operace může trvat desítky vteřin až několik minut a žádný uživatel by nevydržel takto dlouhé testování v průběhu rutinní práce. Jiná situace je ovšem v případě spuštění programu z diskety, kde je spouštěný program samozřejmě otestován. Pokud chcete otestovat kompletní obsah diskety, použijte standardní program pro hledání virů (scanner).

Uživatelské rozhraní

Uživatelské rozhraní patří mezi nejdůležitější části návrhu každého programu. Zde jsme měli poněkud zjednodušenou pozici v tom, že způsob obsluhy programů v nových operačních systémech je z valné části standardizován. Takže můžeme s plnou odpovědností prohlásit, že ten, kdo je schopen obsluhovat operační systém Microsoft Windows 95 nebo Microsoft Windows NT, je schopen pracovat i se systémem AVAST32.

Zde bychom rádi upozornili naše uživatele, že Microsoft Windows 95 a také nové verze Microsoft Windows NT zavádějí novou koncepci práce s programy. Ta spočívá v používání pravého tlačítka myši, které slouží pro vyvolání kontextového menu. Tento způsob obsluhy jsme plně zachovali a důsledně jej dodržujeme ve všech programech, které jsou součástí AVAST32.

V praxi to znamená, že pokud nevíte co dále, použijte pravé tlačítko myši a ve většině případů uvidíte menu, které Vám umožní pokračovat v práci.

K uživatelskému rozhraní patří neoddělitelně možnost jednotné konfigurace a spouštění samostatných testů. V systému AVAST32 tento úkol plní tzv. konzole testů, která uvádí prakticky všechny činnosti spojené s obsluhou AVAST32.

Pokud používáte Microsoft Windows NT verze 3.5 nebo nižší, nemůžete použít AVAST32 z důvodů implementace ovládacích prvků nové generace. Doporučujeme vám instalovat novou verzi systému Microsoft Windows NT (3.51 nebo lepší), která podporuje nové prvky uživatelského rozhraní.

Nároky na technické a programové vybavení

AVAST32 pro svoji práci potřebuje:

1. Microsoft Windows 95 nebo Microsoft Windows NT verze 3.51 a lepší,
2. 3,5 MB volného místa na disku (plus 1 MB pro instalaci),
3. 8 MB instalované a využívané paměti RAM. V případě instalace více paměti bude systém AVAST32 přiměřeně rychlejší.

Práce AVAST32 na počítači s méně než 8 MB paměti nebyla testována. Odezva „holého" operačního systému na takovém počítači je tak pomalá, že další zátěž prakticky znemožní jakoukoli smysluplnou činnost. Nicméně je možné, že i na těchto počítačích bude možno provozovat AVAST32, což ovšem doporučujeme pouze opravdu trpělivému uživateli.

Jiné nároky

Pokud jste zatím nepochopili nebo máte problémy se základními pojmy a činnostmi potřebnými pro obsluhu operačního systému (například co je to soubor, pořadač, jak soubor uložit nebo otevřít, co je to cvaknutí myší, použití jednotlivých tlačítek myši, aktivizace okna atd.) doporučujeme podrobně prostudovat manuál operačního systému a případně spustit výukový program (samozřejmě pokud je dodáván). Je naprosto nutné, abyste znali alespoň základy práce s operačním systémem, jinak nebudete schopni sledovat výklad tohoto manuálu. Některé základní schopnosti a dovednosti jsou pro obsluhu počítače opravdu potřebné a jejich znalost vám umožní využívat Váš počítač lépe a rychleji nejenom v souvislosti s tímto souborem programů.

Podpora uživatelů

Koupí souboru antivirových programů AVAST32 a jeho registrací získáváte nárok na bezplatnou podporu ze strany firem **ALWIL Software** a **ALWIL Trade s.r.o.**, která obsahuje mimo jiné:

1. bezplatné konzultace ohledně práce AVAST32,
2. bezplatné konzultace v případě napadení systému virem týkající se vlastností viru a způsobu jeho odstranění,
3. právo na bezplatnou náhradu vadných částí AVAST32 za bezchybné (stejné nebo novější verze),
4. právo na zaslání kopie ztracené nebo poškozené diskety s produktem (zde si společnost ALWIL Trade s.r.o. vyhrazuje právo ve vybraných případech účtovat nezbytně nutné náklady spojené s tímto úkonem),

5. výhody při používání všech forem elektronické komunikace s pracovníky firem,
6. právo na bezplatné odstranění viru na určeném pracovišti firmy ALWIL Software,
7. právo na vrácení produktu v období třiceti dnů od zakoupení v případě vaší nespokojenosti.

V případě, že nejste majiteli legální kopie souboru programů AVAST32, nebo toto vlastnictví nemůžete prokázat, může vás stát odstranění viru poměrně značnou finanční částku (porovnatelnou s cenou našeho produktu) v závislosti na složitosti případu.

Koupí produktu AVAST32 vám nevzniká nárok zejména na:

1. podrobné technické informace o produktu (rozhodnutí o tom, která informace spadá do této oblasti, je plně v kompetenci pracovníků firmy ALWIL Software),
2. instalování produktu u uživatele (rozhodnutí o tom, zda pracovníci našich firem AVAST32 nainstalují na vašich počítačících je plně v jejich kompetenci),
3. technický servis u uživatele (pouze ve zcela výjimečných případech lze servis u uživatele dohodnout),
4. řešení problémů operačního systému počítače provozujícího AVAST32. V případě závad na operačním systému se obracejte na vašeho dodavatele nebo přímo na firmu Microsoft ČR s.r.o.

Jak kontaktovat prodejce – obchodní informace

Systém AVAST32 můžete získat z různých zdrojů. V případě jakýchkoli obchodních problémů, například týkajících se plnění nebo vad dodávek, chybných disket nebo nedostatku manuálů se obraťte na vašeho dodavatele. Až pokud u něj neuspějete nebo jej neznáte, obraťte se na firmu ALWIL Trade s.r.o., kterou můžete kontaktovat následujícími způsoby:

adresa:	ALWIL Trade s.r.o Průběžná 76 100 00 Praha 10 Česká Republika
telefon:	(+42 2)782 2547 (+42 2)782 2548

fax:	(+42 2)781 0548
web:	http://www.vol.cz/ALWIL
e–mail:	
obchodní ředitel:	rtrnka@alwil.cz
objednávky:	objednavky@alwil.cz
prodej, AVS:	jberankova@alwil.cz
fakturace:	pourednikova@alwil.cz

Jak získat technické informace

Doufáme, že tento manuál vám poskytne převážnou část potřebných informací ohledně systému AVAST32. Pokud tomu tak není, omlouváme se vám a doufáme, že další verze manuálu budou lépe vyhovovat vašim představám.

Pokud vám není něco zcela jasné, konzultujte tento manuál na prvním místě.

V případě, že opravdu cítíte potřebu konzultace technických informací, kontaktujte přímo firmu ALWIL Software. Pracovníci firmy výrazně preferují kontakt pomocí elektronických médií, ale pokud k nim nemáte přístup, můžete použít jiný způsob.

Firma ALWIL Software se žádným způsobem nepodílí na prodeji jakéhokoli produktu. Proto požadování obchodních informací od pracovníků této firmy je zbytečné. Tyto a mnoho dalších informací vám s radostí poskytnou pracovníci firmy **ALWIL Trade s.r.o**.

Jednotlivé informace můžete získat následujícími způsoby:

adresa:	ALWIL Software	od 1. 7. 1996
	Průběžná 76	Lipí 1244
	100 00 Praha 10	Praha 9, Horní Počernice
	Česká Republika	
telefon:	(+42 2)782 2050	(+42 2) 685 56 03
	(+42 2)782 2553	(+42 2) 685 56 24
fax:	(+42 2)782 2050	(+42 2) 685 59 61
	(+42 2)782 2553	(+42 2) 685 59 63
BBS:	(+42 2)782 2550	
web:	http://www.anet.cz/alwil/alwil.html	

e–mail:
informace o produktech pro systémy Windows:
kovacic@alwil.anet.cz
informace o produktech pro DOS:
baudis@alwil.anet.cz
informace o virech:
baudis@alwil.anet.cz
informace o ostatních produktech:
libovolná výše uvedená adresa

informace o jednotlivých produktech můžete získat u následujících pracovníků ALWIL Software:

pro Windows	Michal Kovačič
pro DOS	Pavel Baudiš
pro tiskárny	Eduard Kučera
informace o virech	Vladimír Černík
o instalaci produktů	Jindřich Kubec
obchodní informace	**ALWIL Trade s.r.o.**

Ještě jsme nezačali aneb Instalace

- **Instalace programu**
- **Příprava instalace**
- **Start instalace**
- **Průběh instalace**
- **Problémy s instalací**
- **Instalace z jiných médií**
- **Administrátorská instalace**
- **Odstranění programu ze systému**
- **Spuštění deinstalace**
- **Průběh deinstalace**

Instalace programu

AVAST32 je dodáván na několika disketách v komprimovaném stavu a tudíž není jej možné přímo použít. Pro jeho snadnou instalaci pracovníci naší firmy vyvinuli instalační program, který vykoná všechny činnosti potřebné k provozování produktu na vašem systému.

Pro přípravu instalačního programu byl použit programový balík InstallShield firmy Stirling Technologies, Inc. V současné době tento programový balík představuje standard pro instalaci v systému Microsoft Windows 95 (ale také v jiných verzích Microsoft Windows). Velice zdařilou ukázkou jeho možností je skutečnost, že vlastní instalace operačního systému probíhá plně v jeho režii.

AVAST32 je dodáván na disketách o velikosti 3,5 palce. Pouze na speciální vyžádání jej můžete obdržet na disketách jiné velikosti.

Příprava instalace

Jako vůbec první operaci před započetím instalace vám doporučujeme vytvořit si **záložní kopie** originálních disket. K tomu budete potřebovat stejný počet disket s vysokou hustotou záznamu. Pro jejich vytvoření doporučujeme použít příkaz DISKCOPY operačního systému. Při další práci používejte jenom tyto nově vytvořené diskety a originály uschovejte na bezpečném místě. Pro opravdu zřetelné označení kopií originálních disket jsou součástí dodávky AVAST32 i nálepky na tyto diskety.

V případě ztráty nebo poškození originálních disket máte samozřejmě právo na získání jejich kopií. Nicméně si v tomto případě vyhrazujeme právo požadovat za vystavení náhradních originálních disket příslušný manipulační poplatek.

Před započetím instalace se ujistěte, zda opravdu pracujete pod operačním systémem Microsoft Windows 95 nebo Microsoft Windows NT. V případě, že pod žádným z těchto systémů nepracujete (používáte například Microsoft Windows 3.x s nadstavbou Win32s), nebudete moci použít AVAST32 ani instalační program pro jeho instalaci. Nejpravděpodobnější výsledek pokusu o spuštění bude „spadnutí" počítače.

Dále se ujistěte, že již nemáte nainstalovanou předchozí verzi AVAST32. V případě, že tomu tak je, musíte jej odinstalovat. Pokud tak neučiníte, instalační program to zjistí a odmítne nainstalovat novou verzi. Instalační program také nemůže správně dokončit instalaci, pokud je některý program již spuštěn. V tomto případě instalace proběhne do konce, ale její výsledek pravděpodobně nebude pracovat správně.

*V případě, že odinstalujete předchozí verzi AVAST32 „manuálně" zjistíte, že to nestačí. AVAST32 plně podporuje nové vlastnosti Microsoft Windows 95 a tudíž také deinstalaci produktů, kterou naleznete v **„Kontrolních Panelech"**. V případě Microsoft Windows NT instalační program připraví možnost deinstalace do normální programové skupiny společně s ostatními ikonami.*

Ujistěte se, zda máte k dispozici opravdu všechny instalační diskety nebo jejich kopie. Bez nich nebudete schopni nainstalovat AVAST32 do funkčního stavu.

Pokud jste splnil všechny tyto podmínky, můžete přistoupit k instalaci produktu.

Start instalace

Pro odstartování instalace můžete použít několik způsobů. Nejjednodušší z nich je použití k tomu vyvinutého prostředku implementovaného do operačního systému. Ten naleznete ve složce „**Kontrolní panely**“ se jménem „**Přidej/Odstraň program**“. Použití tohoto prostředku je popsáno v manuálu nebo nápovědě operačního systému.

Můžete také přímo spustit program „**Setup.exe**“ na první disketě. Způsob, jak spustit program, je podrobně popsán v manuálu nebo nápovědě operačního systému. Vyberte si způsob, který vám nejlépe vyhovuje a použijte jej.

Všechny způsoby odstartování instalace jsou zcela totožné a poskytnou stejný výsledek.

Průběh instalace

Vlastní instalace probíhá formou dialogu mezi programem a uživatelem. Pro správnou instalaci je nutné vyplnit některé údaje (jméno uživatele, firmu a sériové číslo produktu). Ne všechny jsou nevyhnutelné pro její zdárný průběh. Některé z nich je možné vynechat (například identifikaci firmy v případě, že jste si AVAST32 koupil k domácímu použití). Další parametry instalace je možno modifikovat. Většina těchto údajů je přednastavena vlastním instalačním programem nebo zjištěna z prostředí operačního systému, a tak většině uživatelů stačí pouze potvrzovat jednotlivé kroky instalační programu.

Je opravdu důležité, abyste správně a úplně vyplnili položku pro sériové číslo (ve tvaru 0002.120.12345). Bez správného sériového čísla nebude program nainstalován a v případě pokusu o neoprávněnou instalaci nebude spolehlivě pracovat.

Instalace samotná je kdykoli přerušitelná. Navíc instalační program umožňuje návrat ke kterékoli části instalace pouhým

stiskem jedné klávesy. V případě jejího přerušení instalační program neodinstaluje žádné části, které do té doby instaloval a neuvede systém do původního stavu. Je proto třeba nejdříve odinstalovat i nesprávně nainstalované 'torzo' programu.

Ukončení instalačního programu se projeví jeho zmizením z obrazovky počítače. Ihned poté je možno začít AVAST32 používat. Není zapotřebí počítač restartovat nebo jinak pro další práci připravovat.

Problémy s instalací

Ano, může se stát, že došlo k problémům s instalací. Většina problémů je popsána zde:

1. Nelze nainstalovat kvůli chybě sériového čísla. Zadal jste špatně sériové číslo programu. Sériové číslo je ve formátu: 0002.120.12345. Ujistěte se, zda jste jej skutečně opsal správně. Pokud jste si stoprocentně jistý, že ano, nepletete si tečku s čárkou a písmeno o s nulou, je nejvyšší čas kontaktovat firmu **ALWIL Trade s.r.o.** a požadovat buď ústní sdělení sériového čísla nebo nově generované diskety.
2. Instalace je nekonzistentní, často „padá". Většinou je to způsobeno tím, že byl spuštěn deinstalační program s některými programy běžícími v paměti. V tomto případě se tyto programy neodstanily a ani nejdou přepsat novými verzemi. Zkuste je ukončit a znovu spusťte deinstalaci. Poté znovu instalujte. Pokud by se toto nepovedlo, jako zkušenější se zkuste poradit s přílohou D pojednávající o manuální deinstalaci. Méně zkušeným uživatelům doporučujeme kontakt se správcem sítě popř. kontaktování technické podpory.
3. Instalační program hlásí, že AVAST32 je již jednou nainstalován, ovšem vy jste jej již odstanili. Ovšem nekorektním způsobem, že ano? Pokud se AVAST32 odstraní pomocí deinstalačního programu, nemůže k tomuto problému dojít. Opět, zkušenější se poradí s přílohou D, méně zkušení se zkušenějšími.

Pokud dojde k nějaké jiné chybě instalace, je zapotřebí zapřemýšlet, zda se nejedná o vaši chybu či chybu vašeho systému. Pokud zcela vyloučíte problémy na vaší straně, kontaktujte technickou podporu.

Instalace z jiných médií

Systém AVAST32 je možné instalovat i z jiného média než z distribučních disket nebo jejich kopií. Tento postup je možné s výhodou použít pro urychlení instalace (až o několik řádů, dle typu použitého média) nebo v případě instalace na síťové stanice. V tomto případě je nutné zkopírovat všechny distribuční diskety nebo jejich kopie do adresářů DISK1, DISK2 apod. na médiu, které je v okamžiku instalace přístupné (síťový disk, Bernoulli disk, ZIP disk, …) a spustit instalaci z tohoto média způsobem uvedeným v odstavci „**Start instalace**“.

Administrátorská instalace

AVAST32 podporuje tzv. „Administrátorskou instalaci“, která spočívá v připravení vlastní klientské instalace do sdíleného adresáře na souborovém serveru. Vlastní klientská instalace pak může probíhat bez jakéhokoli zásahu uživatele zcela automaticky. Tento způsob instalace s výhodou použijí zejména správci většího množství počítačů.

Administrátorská instalace se spouští pomocí stejného programu „**setup.exe**“, jako normální klientská instalace, pouze je zapotřebí specifikovat parametr příkazové řádky „**admin**“. S výhodou můžete použít připravené dávky „**admin.bat**“, která spustí administrátorskou instalaci automaticky. Pokud chcete vědět o administátorské instalaci něco bližšího, na první instalační disketě se nachází soubor **ADMIN.TXT**, který obsahuje podrobné informace o tomto typu instalace.

Odstranění programu ze systému

AVAST32 je možné kdykoli ze systému odinstalovat. Tato operace nenávratně (jistě s výjimkou opakované instalace) odstraní AVAST32 z pevného disku počítače a uvede systém do původního stavu. Deinstalace řeší i takové problémy, jako je odinstalování sdílených knihoven a obnovení interních informací v registrech systému.

Příprava deinstalace

Před odinstalováním AVAST32 se přesvědčte, že žádný z programů není spuštěn. V opačném případě odinstalování neproběhne v pořádku a na pevném disku zůstanou zbytky AVAST32. Také obnova interních dat systému nebude moci být provedena do konce. Toto může být (a většinou bývá) příčinou **VÁŽNÝCH** problémů při instalaci dalších verzí AVAST32.

*Podívejte se na spodní okraj obrazovky. Pokud uvidíte některý z programů systému AVAST32, ukončete jej. Použijte příslušné tlačítko myši a zvolte příkaz **„Ukonči“** pro každý spuštěný program z AVAST32.*

Spuštění deinstalace

Pro odstartování deinstalace důrazně doporučujeme použít standardní prostředek implementovaný do operačního systému. Ten naleznete ve složce „**Kontrolní panely**“ se jménem „**Přidej/Odstraň program**“. Použití tohoto prostředku je popsáno v manuálu nebo nápovědě operačního systému.

Průběh deinstalace

Vlastní průběh deinstalace je plně automatický, kromě prvotního dotazu, zda odinstalování opravdu myslíte vážně. Pokud odpovíte „**Ano**“, bude AVAST32 deinstalován a systém bude uveden do původního stavu. V případě, že deinstalační program nebude schopen plně odinstalovat všechny součásti AVAST32, oznámí tuto skutečnost těsně před vlastním ukončením. Tato situace nastane poměrně často, protože při práci si AVAST32 vytváří nové soubory a zapisuje si informace do systémových proměnných („**Registry**“).

Pokud chcete opravdu dokonale odinstalovat AVAST32 prostudujte si přílohu D, kde je tato činnost podrobně popsána. Pokud si nejste jisti, nechte systém ve stavu, v jakém zůstane po standardní deinstalační proceduře. Tento stav je pro operační systém normální, nijak nebrání další instalaci produktu ani vlastní práci systému.

Začínáme s AVAST32

- **Start rychle a stručně**
- **Spuštění programu**
- **Mám zde nějaké viry?**
- **Potřebuji něco dalšího?**
- **Co mám ještě spustit?**
- **Permanentní testování**

Pokud chcete získat podrobné informace o používání AVAST32, nahlédněte prosím také do dalších kapitol tohoto manuálu. Zde naleznete informace potřebné k rychlému startu bez nutnosti číst celý manuál podrobněji.

Start rychle a stručně

Po úspěšně provedené instalaci můžete okamžitě vyzkoušet jak AVAST32 pracuje. Základní konfigurace jednotlivých části je provedena automaticky s instalací produktu a tak můžete ihned začít. Tato základní konfigurace je zvolena tak, aby optimalizovala protichůdné požadavky na rychlost testů a jejich účinnost.

Spuštění programu

Instalační program zařadil ikonu AVAST32 do standardního menu Microsoft Windows 95 do složky „**Programy**“ (v případě Microsoft Windows NT vytvořil programovou skupinu AVAST32 v Program Manageru). Podle množství instalovaných programů se asi budete muset zorientovat, ale jistě zde naleznete položku „**AVAST32**“, která představuje základní prostředek přístupu pro všechny funkce. Standardním postupem spusťte tento program.

Mám zde nějaké viry?

To bude asi zásadní otázka každého nového uživatele. Odpověď je velice snadná. Pouhým dvojitým cvaknutím levého tlačítka myši můžete získat odpověď. Tento úkon proveďte

na položce „**Standardní konfigurace**“ v oblasti „**Scanovací program**“. Výsledkem bude spuštění klasického scanneru, který zjistí, zda někde ve vašem systému je zavirovaný soubor.

Potřebuji něco dalšího?

Zcela jistě ano. Pokud si myslíte něco jiného, budete mít problémy, které se nemusí dát snadno odstranit. Pouhé používání programu pro hledání virů vám nezaručí bezpečí a v případě napadení vašeho počítače nebudete moci rekonstruovat poškozené soubory.

Používejte ještě alespoň program pro testování integrity dat. V případě nakažení počítače se alespoň budete moci pokusit viry odstranit!!

Co mám ještě spustit?

Pro začátek vám doporučujeme uložit si aktuální databázi všech souborů, které máte na pevném disku. Pokud budete tuto databázi pravidelně aktualizovat, je dosti pravděpodobné, že případná virová infekce nezpůsobí velké ztráty. Vytvoření této databáze může být časově náročné, ale podle našeho názoru se vyplatí.

Výše uvedený odstavec neříká, že žádné ztráty. Každá virová infekce i tím nejméně nebezpečným virem nese s sebou nebezpečí ztráty dat, které se výrazně zvyšuje neodborným zásahem.

Takže pokud máte stále spuštěný program AVAST32, aktivujte jej (cvakněte myší na ikonu programu ve stavové liště nebo použijte kombinace kláves Alt+TAB).

Pokud máte problémy s tím, jak aktivizovat okno programu nebo program, doporučujeme opakovaně a podrobněji prostudovat manuál operačního systému a případně opakovaně spustit výukový program (samozřejmě pokud je dodáván). Je naprosto nutné abyste znali základy práce s operačním systémem, jinak nebudete schopni sledovat výklad tohoto manuálu. Některé základní schopnosti a dovednosti jsou pro obsluhu počítače opravdu potřebné a jejich znalost vám umožní využívat váš počítač dokonaleji a rychleji.

Zvolte si oblast „**Testování integrity**“ a dvakrát cvakněte na položku „**Standardní konfigurace**“.

Program zde přečte obsah všech dostupných souborů na všech dostupných lokálních discích a pro každý disk vám zobrazí seznam souborů. Protože jde o první spuštění programu, budou v seznamu zařazeny všechny soubory jako nové. Pomocí pravého tlačítka myši vyvolejte menu a zvolte položku „**Uložit všechny položky**“. Program najednou zpracovává pouze jeden disk z důvodů paměťových nároků, které zabírají informace o jednotlivých souborech. Pokud máte více logických disků bude program automaticky pokračovat na dalším disku, ale požadavek na uložení změn nebo jejich zrušení musíte zadat pro každý disk samostatně pomocí kontextového menu, které vyvoláte pomocí pravého tlačítka myši k okně „**Detekováno**“.

Permanentní testování

Při instalaci AVAST32 do systému Microsoft Windows 95 vám instalační program nabídne automatické spuštění některých programů při startu počítače. Tyto programy jsou určeny pro běh v pozadí operačního systému a sledují jeho činnost v reálném čase. V případě zaznamenání některé sledované nebo podezřelé operace tyto programy zobrazí varování a pozastaví činnost systému do okamžiku odpovědi uživatele. Doporučujeme oba programy používat po celou dobu práce s počítačem. Jejich činnost je užitečná a může zabránit již vzniku virové nákazy.

Existují samozřejmě uživatelé, pro které nemá smysl používat programy tohoto typu. Jedním z příkladů mohou být programátoři, kteří vytvářejí spustitelné soubory. Tyto uživatele by jakýkoli program jenom zdržoval zbytečnými dotazy a častou kontrolou stále stejných modulů.

Pokud se rozhodnete pro zařazení těchto programů do startovací sekvence operačního systému, budou instalačním programem spuštěny a aktivizovány ihned po jejich nainstalování na váš pevný disk. Zda pracují nebo ne, můžete zjistit ihned při ukončování instalace, kdy zobrazí několik po sobě jdoucích varování ohledně mazání výkonných souborů. Tato varování jsou v pořádku, protože instalační program po sobě uklízí pomocné soubory, které potřeboval pro svojí práci. Potvrďte oprávněnost těchto operací stisknutím tlačítka „**Ano**“ v zobrazovaných dialozích.

AVAST32 jako celek

- **Hlavní součásti souboru antivirových programů**
- **Společné rysy AVAST32**
- **Uživatelské rozhraní**
- **Používání myši**
- **Nápověda**

Microsoft Windows 95 a také nové verze Microsoft Windows NT mají již uživatelsky velice příjemné prostředí, které by mělo být intuitivní a snadno pochopitelné. Návrh produktu AVAST32 se snaží plně respektovat všechna pravidla a zavedené postupy pro program vyhovující specifikacím těchto operačních systémů. Proto doufáme, že vám nebude dělat problémy zjistit, jak jednotlivé části AVAST32 pracují.

Dovolili bychom si vám připomenout používání pravého tlačítka myši, které slouží pro vyvolání kontextového menu. Pokud nebudete vědět, jak dále pokračovat stiskněte jej a pravděpodobně uvidíte menu, které vám to umožní.

Hlavní součásti souboru antivirových programů

AVAST32 se skládá z několika samostatných částí, které mohou být používány ze společné konzole (shellu) nebo samostatně, podle vašich aktuálních požadavků.

Instalační program zapíše na Váš pevný disk soubory různých typů, ale ne každý soubor představuje samostatný program. Protože uživatelské rozhraní Microsoft Windows 95 se snaží maximálně odstínit uživatele od podrobností o jednotlivých souborech, není třeba vědět, který soubor představuje spustitelný program a který slouží pouze jako datová podpora. Přesný seznam souborů, jejich typů a umístění je uveden v příloze G.

Soubor antivirových programů AVAST32 v současné verzi obsahuje:

1. program pro hledání virů (scanner),
2. program pro kontrolu integrity dat,
3. rezidentní scanner (pouze pro Microsoft Windows 95),
4. systémový monitor (pouze pro Microsoft Windows 95),
5. konzoli testů neboli shell.

Na disku je ovšem nenaleznete pod těmito jmény. Z důvodů kompatibility se systémem souborů operačního systému DOS a Novell Netware (hlavně z důvodu omezení délky jmen souborů) jsou zde uvedeny pod svými zkratkami, jejichž vysvětlení také naleznete v příloze G.

Společné rysy AVAST32

Při návrhu souboru antivirových programů AVAST32 jsme se snažili maximálně dodržet společný vzhled a způsob ovládání jednotlivých součástí. Doufáme, že se nám to podařilo a vám nebude obsluha AVAST32 činit žádné problémy.

Uživatelské rozhraní

AVAST32 byl navržen a vytvořen na počítači s vyšším rozlišením obrazovky a větším počtem barev. Z této skutečnosti vyplývají některé jeho vlastnosti a schopnosti. AVAST32 je schopen práce již od nejmenšího rozlišení 640 x 480 bodů se 16–ti barvami až po maximální rozlišení, které dovoluje Váš počítač.

Doporučujeme vám používat rozlišení alespoň 800 x 600 bodů s více než 256 barvami, které umožní zobrazení jednotlivých součástí AVAST32 v lepší kvalitě, než umožňují nižší režimy. Kontaktujte vašeho správce systému a informujte se na možnosti nastavení konfigurace vašeho monitoru.

Všechny programy si automaticky zjišťují aktuální konfiguraci zobrazování a zjištěným informacím přizpůsobují svůj vzhled a částečně i chování.

V praxi to znamená, že na systémech s 256 a méně barvami na bod jsou použity obrázky s nižším rozlišením a tím pádem ne tak kvalitní. Také na systémech s instalovanými „malými“ fonty je vzhled jednotlivých součástí AVAST32 jemně změněn tak, aby odpovídal použitým fontům.

Používání myši

Systém Microsoft Windows 95 ale i nové Microsoft Windows NT zavádějí využití pravého tlačítka myši, které jistě všichni na svých hlodavcích máte. Toto tlačítko se důsledně používá pro vyvolání kontextového menu, tzn. menu, jehož obsah je aktualizován podle stavu programu a místa, nad kterým bylo toto tlačítko stištěno.

AVAST32 plně podporuje tyto konvence a kontextové menu můžete vyvolat prakticky v každém okně libovolné součásti produktu. V několika případech to je dokonce jediný způsob, jak pokračovat v práci s AVAST32 dále. Proto se neostýchejte a pokaždé, když si nebudete vědět rady, stiskněte pravé tlačítko myši nad objektem, se kterým si nevíte rady.

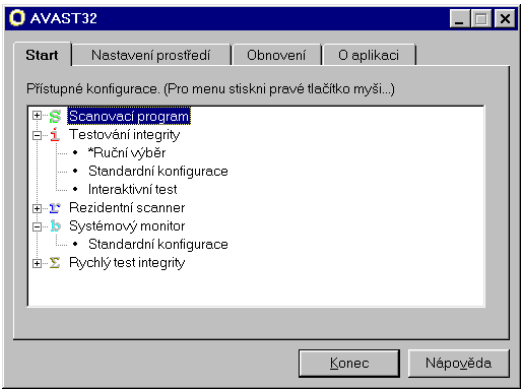
Nápověda

Ve všech programech souboru AVAST32 je možné používat pravé tlačítko myši. Vždy, pokud je to možné, obsahuje nabídnuté menu položku „**Co je to?**“, která umožní zobrazit stručný popis příslušného ovládacího prvku.

Tato stránka je úmyslně prázdná

Konzole testů – shell

- **Spuštění konzole**
- **Parametry příkazové řádky**
- **Co vám konzole nabízí?**
- **Stránka pro startování a konfiguraci testů**
- **Jiné stránky**
- **Konfigurace konzole**
- **Instalace nových verzí některých souborů**
- **Informace o programu**



Konzole testů (neboli shell) je program, který slouží k jednoduchému spouštění všech ostatních součástí AVAST32, nastavování specifických konfigurací pro tyto součásti a případné instalaci nových verzí některých souborů. Program jako takový nic netestuje. Většina uživatelů AVAST32 s ním přijde nejčastěji do styku při rutinní kontrole systému. Pouze ve speciálních případech, například pokud chcete spouštět některé programy automaticky při startu systému, musíte se zaobírat jednotlivými součástmi produktu samostatně.

Spuštění konzole

Konzole testů se spouští stejným způsobem, jako všechny ostatní programy operačního systému. Je zcela jedno, zda to provedete z menu systému, vyhledáním z některého menu systému nebo programu, z exploreru nebo okna DOSu. Všechny způsoby jsou si úplně rovnocenné a výsledkem je spuštění tohoto programu.

Nicméně nejjednodušší způsob je použití hlavního menu systému (standardně umístěného v levém spodním rohu obrazovky v Microsoft Windows 95) nebo cvaknutím na ikonu v pořadači (hlavně pro ty, kteří používají Microsoft Windows NT bez nového uživatelského rozhraní). Spuštění má za následek otevření okna programu a zobrazení jeho první stránky.

Všechny uživatelské programy, které jsou součástí produktu AVAST32, mají stejný tvar. To znamená zobrazují tzv. „**záložkový dialog**“, nebo jinak, dialog, který se skládá z několika oken a simuluje pořadač (například telefonní). Tato forma je standardní pro nové operační systémy a výrazně zjednodušuje ovládání programu. Přepínání jednotlivých stránek je opravdu jednoduché a věříme, že jste se s tímto tvarem okna již setkali.

Parametry příkazové řádky

Konzole testů nerozeznává žádný parametr příkazové řádky. Je tudíž úplně jedno, zda zde nějaký uvedete nebo ne, program je ignoruje.

Co vám konzole nabízí?

Stručně řečeno, konzole nabízí stránku pro spouštění jednotlivých programů a jejich konfiguraci se jménem „**Start**“ a některé další informační a servisní stránky.

V současné verzi vám konzole testů nabízí stránku pro:

1. startování a konfiguraci jednotlivých programů,
2. nastavování parametrů konzole,
3. instalaci nových verzí některých souborů,
4. informační stránku o programu,
5. stránku s informacemi o AVS.

Stránka pro startování a konfiguraci testů

Jediným informačním i obslužným prvkem na této stránce je okno s hierarchickým seznamem aktuálně přístupných konfigurací. Základním prvkem tohoto okna je „**konfigurace**“, která určuje:

1. co se bude testovat,
2. jak se to bude testovat.

V dalších verzích AVAST32 může konfigurace obsahovat i další informace, například o čase spouštění. O změnách budete včas informováni.

Příslušných konfigurací může být pro každý program více, jejich počet závisí pouze na vás a na některých limitech používaného operačního systému (z těchto limitů můžeme například jmenovat maximální počet položek v okně tohoto typu, který je 32768. Nicméně si myslíme, že dosáhnout tohoto limitu není reálně možné).

Vlastní spuštění programu je velice snadné. Dvakrát cvakněte na jednu ze zobrazených konfigurací a příslušný program se spustí. V případě, že program může existovat v paměti pouze jednou (rezidentní programy), je zobrazeno hlavní okno existujícího programu a zazní zvukové znamení.

Popis vlastního obsahu jednotlivých konfigurací je uveden v příslušných kapitolách níže.

Jiné stránky

Konzole testů obsahuje další stránky, které neslouží přímo ke spouštění jednotlivých testů, ale také mají svůj nezastupitelný význam. Mezi další stránky patří:

1. konfigurace konzole,
2. instalace nových verzí některých souborů,
3. informativní stránka.

Konfigurace konzole

Stránka konfigurace konzole slouží výhradně ke konfiguraci vlastního programu. Všechny ostatní programy, které jsou součástí produktu AVAST32 mají vlastní konfiguraci pro–

gramu nebo podobnou konfiguraci nepotřebují. Nastavením libovolného přepínače v této stránce nebo změnou obsahu libovolného okna nemůžete změnit nastavení dalších součástí AVAST32.

Konfigurace konzole umožní nastavit kromě dalších vlastností také jednu důležitou schopnost programu, kterou je schopnost automatického obnovování definičního souboru virů při startu konzole. Tato vlastnost může být důležitá hlavně pro správce většího množství počítačů, kdy stačí instalovat definiční soubor do sdíleného adresáře na souborovém serveru a všichni uživatelé si jej při prvním spuštění konzole instalují na svůj lokální pevný disk. Tato aktualizace může být úplně automatizovaná bez jakéhokoli dotazu uživateli.

Instalace nových verzí některých souborů

Stránka pro instalaci nových verzí neslouží ke kompletní instalaci nové verze AVAST32. Jejím úkolem je pouze zjednodušit instalaci některých částí produktu, zejména definičního souboru virů, který předplatitelé naší antivirové služby dostávají automaticky každý měsíc.

Obsluha této stránky je velice snadná. Jediné, co na této stránce můžete vidět, je stručná informace, tlačítko pro obnovení definičního souboru virů a tlačítko pro smazání uložené informace o poloze nových verzí definičního souboru. AVAST32 si automaticky zjistí, zda máte něco k instalování a pokud ano, příslušnou operaci provede. Před jakýmkoli přepsáním původního souboru se ovšem zeptá, zda tuto operaci chcete opravdu vykonat nebo ne. V žádném případě nepřepíše žádný soubor bez vašeho vědomí.

Informace o programu

Stránka s informacemi o programu neobsahuje žádný ovládací prvek, ale přesto byste ji měli věnovat určitou pozornost. Jsou zde uvedeny důležité informace:

1. kdo vlastní licenci programu,
2. aktuální informace o operačním systému,
3. detailní informace o překladu programu,
4. informace o autorských právech vztahujících se k programu.

Některé z těchto informací budete pravděpodobně potřebovat, když se obrátíte na naší firmu se žádostí o technickou podporu.

Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že tyto informace neposkytnete.

Tato stránka je úmyslně prázdná

Mám virus v počítači?

- **Spuštění programu**
- **Parametry příkazové řádky**
- **Co nabízí program pro hledání virů?**
- **Hlavní stránka programu**
- **Seznam detekovaných souborů**
- **Seznam virů**
- **Informace o programu**

Jedním ze základních kamenů jakéhokoli antivirového systému je program pro hledání virů (tzv. „**scanner**"). Jeho činnost bývá prakticky všude stejná. Program prohledává zadané soubory nebo adresáře a hledá, zda se v nich nenachází známý virus. Základní princip vypadá velice jednoduše a i ve skutečnosti není složitý. Horší to už bývá s vlastní implementací algoritmů, ve které se projeví vyspělost jednotlivých produktu.

AVAST32 samozřejmě program pro hledání virů obsahuje. Jeho princip se také výrazně neodlišuje od obecných principů. Program dle aktuální konfigurace prohledává jednotlivé oblasti na discích a zjišťuje, zda se v nich nenachází příznak viru. Program nehledá každý virus v celé jeho délce, ale hledá pouze jeho příznak, který může být jednoduchý (prostý řetězec znaků) nebo naopak složitý (některý z implementovaných algoritmů pro viry polymorfní). Při nalezení prvního příznaku viru program na tuto skutečnost upozorní a inicializuje seznam detekovaných souborů.

Může se také stát, že některý soubor není možné otestovat. V tomto případě je soubor také umístěn do seznamu detekovaných souborů, ovšem na jiné místo s poznámkou, že soubor nebyl testován.

Spuštění programu

Pro spuštění programu platí stejná pravidla jako pro spouštění jakéhokoli jiného programu ve vašem operačním systému.

Nejjednodušší metodou však stále zůstává použití konzole testů. Zde můžete zároveň určit počáteční nastavení konfigurace. Za běhu samozřejmě můžete zvolit jinou nastavenou konfiguraci nebo můžete určit potřebná data manuálně.

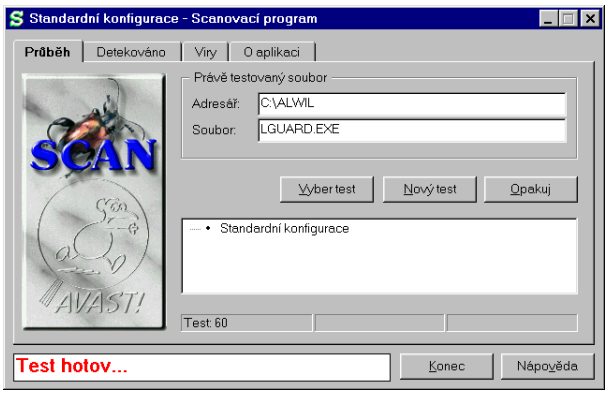
Parametry příkazové řádky

Program akceptuje jeden parametr uvedený na příkazové řádce. Obecný předpis pro spouštění programu je:

```
LGW [@<jméno konfigurace>]
```

kde „@“ je znak, kterým musí parametr začínat (pokud je uveden) a „<**jméno konfigurace**>“ je jedno ze jmen uvedených v seznamu možných konfigurací konzole testů. Pokud chcete použít jedno z rezervovaných jmen (jsou uvedena hvězdičkou), musíte vynechat první znak (tuto hvězdičku).

V případě, že nepoužijete žádný parametr příkazové řádky, spustí se program v manuálním režimu a pro spuštění testů budete moci vybrat jednu z nabízených konfigurací ve vlastním programu nebo nastavit konfigurační data manuálně stiskem příslušného tlačítka.



Co nabízí program pro hledání virů?

Program nabízí uživateli několik stránek, ve kterých jsou zobrazeny veškeré potřebné informace. Jednotlivé stránky jsou:

1. hlavní stránka,
2. seznam detekovaných souborů,
3. seznam virů,
4. stránka s informacemi o programu.

Hlavní stránka programu

Hlavní stránka programu zobrazuje průběh a statistiku testování. Umožňuje průběh testování ovládat (pozastavit či zrušit aktuální testování) a také určit jinou konfiguraci manuálně nebo výběrem ze seznamu nabízených položek.

Ovládací prvky se zde redukují na tlačítka, jejichž činnost je vyjádřena jejich popisem a okno se seznamem aktuálně přístupných konfigurací. Ne všechna tlačítka a informační prvky jsou viditelná po celou dobu. Aktuálně nepřístupné objekty jsou buď skryty nebo se nedají použít a jejich vzhled je změněn oproti normálnímu stavu (jsou „zešedlé“).

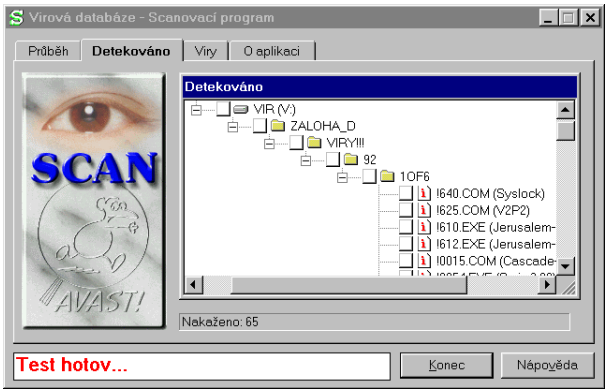
Zároveň je na stránce zobrazován průběh testování. To znamená jméno souboru a jméno adresáře, ve kterém je testovaný soubor umístěn. V případě, že je testovaný soubor dlouhý, je možné, že zůstane zobrazen mnohem delší dobu, než ostatní soubory. Nicméně, skutečnost, že program nemění jméno a adresář neznamená, že program nepracuje. Pouze probíhá testování příslušného souboru a doba testu je přímo závislá na rychlosti vašeho počítače a velikosti instalované operační paměti.

Seznam detekovaných souborů

Seznam detekovaných souborů je stránka určená pro zobrazení výsledků testů. Na ní jsou zobrazeny všechny detekované soubory, což jsou:

1. soubory, které vykazují známky infekce virem,
2. soubory, které se z libovolné příčiny nepovedlo otestovat,
3. infikované systémové oblasti disků,
4. přítomnost viru v paměti.

Tato stránka je organizována stejným způsobem jako seznam souborů, který můžete vidět v „**prohlížeči (exploreru)**“. Hierarchická struktura uspořádání souborů na disku je uchována i v tomto zobrazení, a tak můžete rychle vidět, kde všude máte infikované soubory.



Soubory, které nemohly být z jakýchkoli příčin testovány jsou seřazeny v samostatném stromu (jsou odděleny od správně otestovaných, ale infikovaných souborů pro lepší přehled), který také kopíruje hierarchickou strukturu souborů na disku.

Aktualizace seznamu souborů není okamžitá. Z důvodů rychlosti programu se aktualizace této stránky provádí ihned po nalezení detekovaného souboru pouze v případě, že tato stránka je aktivní. Pokud tomu tak není, detekované soubory se ukládají do interního zásobníku programu a do stránky se uloží až v okamžiku, kdy se stane aktivní. Tato operace může v některých případech trvat až několik minut, což se týká hlavně počítačů s nižším výkonem a nedostatkem paměti.

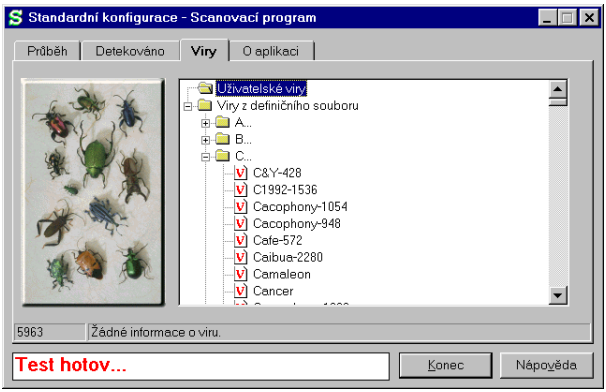
Prakticky všechny položky zobrazené v seznamu je možno označit cvaknutím levého tlačítka myši, ale v současné verzi není toto označení využíváno.

Pro lepší orientaci v seznamu detekovaných souborů je možné změnit charakter okna se seznamem z pevného okna, které se nedá roztáhnout na volně plovoucí okno, jehož velikost si můžete upravit podle aktuálních potřeb. Tuto schopnost programu je možné vyvolat pomocí kontextového menu přístu-

pného po stisku pravého tlačítka myši. Nicméně při základním nastavení, které je použito při startu programu, je okno pevné a neměnné.

Seznam virů

Seznam hledaných virů je abecedně uspořádaná struktura všech programu známých virů bez ohledu na to, zda jde o virus získaný z definičního souboru nebo jde o uživatelsky definovaný virus. Zde můžete vidět všechny základní typy virů, které je program schopen zjistit včetně těch, které si definujete vy.



Na stránce můžete také vidět celkový počet detekovaných virů a jejich stručný popis, který můžete získat cvaknutím levého tlačítka myši na jménu příslušného viru. Podrobnější popis některých specifických virů můžete najít v příloze E tohoto manuálu.

Podrobnější popis všech známých virů, jejich činnosti a zvláštností není k dispozici. Není únosné ani vhodné zjišťovat všechny podrobnosti o každém viru hlavně z důvodu jejich obrovského množství. Případní zájemci o podrobnější informace o jednotlivém viru se mohou obrátit na pracovníky naší firmy, kteří jim je rádi poskytnou. Způsob kontaktu naší firmy je uveden na začátku tohoto manuálu.

Jednou z důležitých vlastností dobrého programu pro hledání virů je schopnost dovolit zkušenému uživateli definici vlastních virů. Zde ovšem musíme zdůraznit, že pouze „**zkušenému uživateli**“. Špatná definice viru může způsobit falešný poplach a z toho plyne možnost škod (například známe dost příkladů, kdy uživatel po hlášení o infikovaném souboru jej okamžitě smazal bez dalšího testování). Z návrhu interních algoritmů není program pro hledání virů schopen rozhodnout, zda je aktuálně nalezený vzorek viru vytvořen uživatelem nebo je standardní součástí dodávaného definičního souboru virů, proto důrazně doporučujeme opatrnost a důkladné testy před trvalým zařazením definice virů do prostředí AVAST32.

Nevýhodou je zde rovněž skutečnost, že nemůžete definovat algoritmus pro hledání nového viru, ale pouze prostý řetězec znaků. Ve spojení se skutečností, že „moderní“ viry jsou často „**polymorfní**“, si skutečná identifikace viru žádá dost času a velkou dávku zkušeností.

Pokud si myslíte, že jste opravdu identifikoval nový virus, můžete jeho charakteristiku zadat pomocí kontextového menu. Definice viru spočívá ve vyplnění všech nabízených dialogů. Každá definice viru musí vyhovovat určitým kritériím, které program při zadávání kontroluje. Pokud nezadáte všechny údaje správně, nemůže být definice použita.

Správně vložené definice jsou programem použity až při následující inicializaci definičního souboru virů. Ten je inicializován pouze jednou a to prvním programem, který používá knihovnu pro antivirové testování. Každý další program (stejný nebo jiný) použije stejná pracovní data jako první. Tento postup byl zvolen z důvodů ušetření operační paměti a rychlosti spouštění programů.

Každá vlastní definice poněkud zpomaluje průběh programu (což také vyplývá z konstrukce interních algoritmů) a proto doporučujeme určitou střízlivost při vytváření vlastních definic.

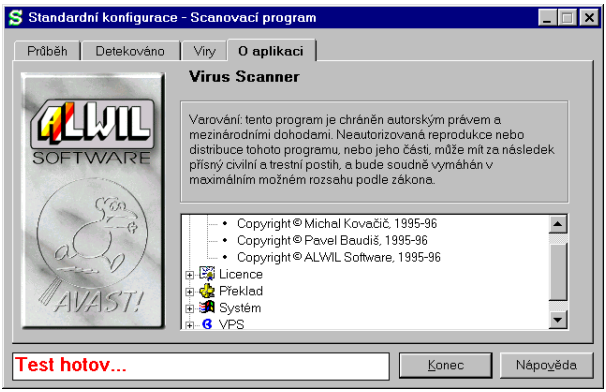
Je důležité, aby použitý identifikační řetězec nezačínal binární nulou (0x00) a znakem 0x90 a zároveň první dva byty nesmí být otazníky (to znamená nesmíte použít sekvenci „????“ na začátku identifikačního řetězce).

Pokud vlastní definici doručíte naší firmě nebo ještě lépe, pokud naší firmě pošlete podezřelý soubor nebo disketu, provedeme rozbor za vás a v případě pozitivní identifikace viru zařadíme otestovanou definici do definičního souboru virů. To je téměř ideální způsob, jak naložit s neznámým virem (ideální by jistě bylo, kdyby neznámý virus vůbec neexistoval).

Informace o programu

Stránka s informacemi o programu neobsahuje žádný ovládací prvek, ale přesto byste ji měli věnovat určitou pozornost. Jsou zde uvedeny důležité informace:

1. kdo vlastní licenci programu,
2. verze definičního souboru virů,
3. aktuální informace o operačním systému,
4. detailní informace o překladu programu,
5. informace o autorských právech vztahujících se k programu.



Některé z těchto informací budete pravděpodobně potřebovat, když se obrátíte na naší firmu se žádostí o technickou podporu.

Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že tyto informace neposkytnete.

Tato stránka je úmyslně prázdná

Změnil se mi některý soubor?

- **Spuštění programu**
- **Parametry příkazové řádky**
- **Co nabízí program pro detekci změn?**
- **Hlavní stránka programu**
- **Seznam detekovaných souborů**
- **Kritéria změn souborů**
- **Vyhodnocení seznamu detekovaných souborů**
- **Testování více oblastí najednou**
- **Informace o programu**

Již ne zcela běžnou součástí antivirových systémů je program, který testuje, zda se v systému něco změnilo. Protože virus musí existovat někde na pevném disku (alespoň v současné době to je nutná a nevyhnutelná podmínka existence viru), je zřejmé, že se jedná o změny na pevných discích počítačů.

Obecný princip práce programu je ještě jednodušší než v případě programu pro hledání virů (scanneru). Jde o pouhé porovnání údajů uložených v databázi s údaji, které aktuálně přečtete z disku. Pokud dojde ke změně, je zapotřebí toto změnu ohlásit, i když se nemusí jednat o známku přítomnosti viru.

Z výše uvedených odstavců je zřejmé, že program tohoto typu je jediná spolehlivá metoda, jak odhalit libovolný virus na vašem počítači. Ale protože je to metoda velice obecná, její použití není příliš jednoduché a v konečném důsledku spočívá pouze a výhradně na bedrech každého z vás. Důsledné a pravidelné používání programu tohoto typu vám zaručí větší bezpečnost, než pouhé hledání virů klasickým programem (scannerem).

Systém AVAST32 program tohoto typu zajisté obsahuje, jde o program pro testování integrity dat. Dle aktuálního nastavení konfigurace prohledává jednotlivé oblasti na disku a zjiš–

ťuje, zda se v nich nezměnil některý soubor, nic nepřibylo, ale ani nic neubylo. Při nalezení změny program aktualizuje seznam detekovaných (změněných, nových a smazaných) souborů.

Může se také stát, že některý soubor není možné otestovat. V tomto případě je soubor také umístěn do seznamu detekovaných souborů, ovšem na jiné místo s poznámkou, že soubor nebyl testován.

Spuštění programu

Pro spuštění programu platí stejná pravidla jako pro spouštění jakéhokoli jiného programu ve vašem operačním systému.

Nejjednodušší metodou však stále zůstává použití konzole testů. Zde můžete zároveň určit počáteční nastavení konfigurace. Za běhu samozřejmě můžete zvolit jinou nastavenou konfiguraci nebo můžete určit potřebná data manuálně.

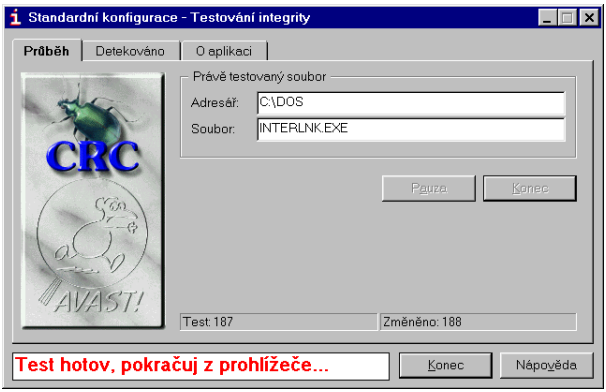
Parametry příkazové řádky

Program akceptuje jeden parametr uvedený na příkazové řádce. Obecný předpis pro spouštění programu je:

```
AGW [@<jméno konfigurace>]
```

kde „@“ je znak, kterým musí parametr začínat (pokud je uveden) a „**<jméno konfigurace>**“ je jedno ze jmen uvedených v seznamu možných konfigurací konzole testů. Pokud chcete použít jedno z rezervovaných jmen (jsou uvedena hvězdičkou), musíte vynechat první znak (tuto hvězdičku).

V případě, že nepoužijete žádný parametr příkazové řádky, spustí se program v manuálním režimu a pro spuštění testů budete moci vybrat jednu z nabízených konfigurací nebo nastavit konfigurační data manuálně stiskem příslušného tlačítka.



Co nabízí program pro detekci změn?

Program nabízí uživateli několik stránek, ve kterých jsou zobrazeny veškeré potřebné informace. Jednotlivé stránky jsou:

1. hlavní stránka,
2. seznam detekovaných souborů,
3. informace o programu.

Hlavní stránka programu

Hlavní stránka programu zobrazuje průběh a statistiku testování. Umožňuje průběh testování ovládat (pozastavit či zrušit aktuální testování) a také určit jinou konfiguraci manuálně nebo výběrem ze seznamu nabízených položek.

Ovládací prvky se zde redukují na tlačítka, jejichž činnost je vyjádřena jejich popisem a okno se seznamem aktuálně přístupných konfigurací. Ne všechna tlačítka a informační prvky jsou viditelné po celou dobu. Aktuálně nepřístupné objekty jsou buď skryty, nebo se nedají použít a jejich vzhled je změněn oproti normálnímu stavu (jsou „zešedlé“).

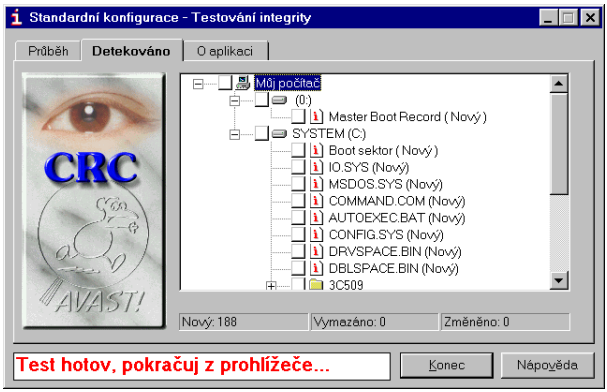
Zároveň je na stránce zobrazován průběh testování. To znamená jméno souboru a jméno adresáře, ve kterém je testovaný soubor umístěn. V případě, že je testovaný soubor dlouhý, je možné, že zůstane zobrazen mnohem delší dobu, než ostatní soubory. Nicméně, skutečnost, že program nemění jméno

a adresář neznamená, že program nepracuje. Pouze probíhá testování příslušného souboru a doba testu je přímo závislá na rychlosti vašeho počítače a velikosti instalované operační paměti.

Seznam detekovaných souborů

Seznam detekovaných souborů je stránka určená pro zobrazení výsledků testů. Na této stránce jsou zobrazeny všechny detekované soubory, což jsou:

1. změněné soubory,
2. soubory, které se nepovedlo otestovat z libovolné příčiny,
3. změněné systémové oblasti disku.



Tato stránka je organizována stejným způsobem jako seznam souborů, který můžete vidět v „**prohlížeči (exploreru)**“. Hierarchická struktura uspořádaní souborů na disku je uchována i v tomto zobrazení a tak můžete rychle vidět, kde všude máte infikované soubory.

Soubory, které nemohly být z jakýchkoli příčin testovány jsou seřazeny v samostatném stromu, který podobně kopíruje hierarchickou strukturu souborů na disku.

Aktualizace seznamu souborů není okamžitá. Z důvodů rychlosti programu se aktualizace této stránky provádí ihned po nalezení detekovaného souboru pouze v případě, že tato stránka je aktivní. Pokud tomu tak není, detekované soubory se ukládají do interního zásobníku programu a do stránky

se uloží až v okamžiku, kdy se stane aktivní. Tato operace může v některých případech trvat až několik minut. To se týká speciálně počítačů s nižším výkonem a nedostatkem paměti.

Pokud program nalezne alespoň jeden modifikovaný soubor, automaticky zobrazí tuto stránku po skončení testu.

Prakticky všechny položky zobrazené v seznamu se dají označit cvaknutím levého tlačítka myši. Toto označení má velký význam. Jenom označené soubory mohou být uloženy jako správné v databázi, kterou si program vytváří a udržuje.

Označení jednotlivých souborů nebo stromu souborů je možné cvaknutím levého tlačítka myši na příslušném místě. Vyvolání funkcí pracujících se seznamem souborů je možné cvaknutím pravého tlačítka myši v okně seznamu.

Pro lepší orientaci v seznamu detekovaných souborů je možné změnit charakter okna se seznamem z pevného okna, které se nedá roztáhnout na volně plovoucí okno, jehož velikost si můžete upravit podle aktuálních potřeb. Tuto schopnost programu je možné vyvolat pomocí kontextového menu pří–stupného po stisku pravého tlačítka myši. Nicméně při základ–ním nastavení, které je použito při startu programu, je okno pevné a neměnné.

Kritéria změn souborů

Program pro detekci změn sleduje všechny důležité pa–rametry souborů a pokud se některý z nich změní, označí soubor jako změněný. Jednotlivé parametry jsou:

1. čas vytvoření souboru, [Č]
2. čas posledního zápisu do souboru, [Č]
3. atributy souboru, [A]
4. velikost souboru, [V]
5. obsah souboru. [O]
6. alternativní jméno souboru [J]
7. soubor je infikován virem [#]

V závorkách jsou uvedeny značky, které jsou zobrazeny v prohlížeči detekovaných souborů za jejich jmény. Zde se mohou vyskytovat i další texty, nicméně jejich význam je již plně zřejmý z jejich obsahu.

Ne všechny parametry jsou sledovány v obou podporovaných operačních systémech. Například čas vytvoření souboru není testován v systému Microsoft Windows 95 protože jej nepodporuje vlastní operační systém. Zároveň je zde jedna výjimka. Pokud nastavíte parametry konfigurace příslušným způsobem, program je schopen ignorovat změnu archivního bitu. Tato vlastnost může být s výhodou použita v případě častého zálohování obsahů disků. Standardní zálohovací programy mění obsah archivního bitu zálohovaného souboru a tak se po úspěšně provedeném zálohování můžete dopracovat k výsledku, že všechny soubory na vašem počítači byly změněny.

Vyhodnocení seznamu detekovaných souborů

Je velice pravděpodobné, že při každém spuštění programu pro testování integrity dat zjistíte, že se některé soubory v systému změnily. Vyhodnocení těchto změn je velice důležité a je ve své podstatě jediným smyslem existence programu tohoto typu.

Existuje mnoho příčin, proč by se ten který soubor měl změnit a pouze jedna z nich je nákaza virem. Je opravdu důležité, abyste uměli rozpoznat tento zřídkavý případ, ale zároveň vás musíme upozornit, že toto rozpoznání nemusí být jednoduché.

Pro bližší orientaci vám nabízíme několik poznatků a zkušeností, které můžete ve své praxi použít. Nicméně nejlepším učitelem je praxe a vlastní zkušenosti. Také musíme zdůraznit, že každý z vás používá počítač na něco jiného a tím pádem se mu na jeho pevných discích mění různá data.

Podrobně sledujte typy změn jednotlivých souborů. Například pouhá změna atributů neznamená napadnutí souboru virem, ale na druhé straně může indikovat, že v systému se děje něco nekalého. Samozřejmě, pokud jste od posledního spuštění programu zálohovali některým z komerčních nebo více méně standardních programů, je změna atributů zcela vysvětlitelná.

Podrobně sledujte typy změněných souborů. Pokud se vám změní obsah a velikost zdrojového souboru k vašemu programu, je to zřejmě změna legální. Na druhé straně změna

obsahu souboru COMMAND.COM znamená prakticky stoprocentně napadení souboru virem (pokud jste neinstalovali novou verzi operačního systému).

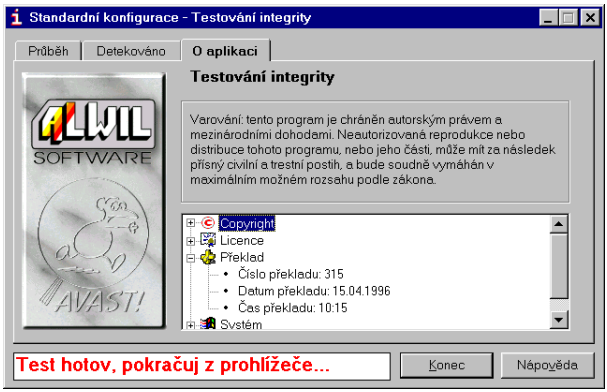
Výše uvedený odstavec se dá zobecnit tak, že změna jakéhokoli spustitelného souboru (tedy, pokud nejste programátor a nevytváříte nové verze programů nebo pokud jste neinstalovali novou verzi jakéhokoli programového vybavení) znamená s velkou pravděpodobností nákazu virem. Dávejte si zároveň pozor na skutečnost, že spustitelné soubory nemusí být označeny výraznou příponou „COM" nebo „EXE" ale mohou mít prakticky libovolnou příponu. Operační systém typ souboru obecně nekontroluje, ale řídí se jeho obsahem. Proto je spustitelným souborem i například soubor „pokus.scr" nebo „avast95.vxd". Existují i viry, které jsou schopné napadnout „BAT" soubory a dále se úspěšně šířit.

Hitem poslední doby jsou takzvané „**Makro viry**". Ty jsou opravdu záludné, protože se jako první viry šíří pomocí dokumentů a ne spustitelných souborů. Proto si dávejte velký pozor i na soubory, které produkují programy obsahující „**Makro jazyk**". Jako zářivý příklad mohou posloužit všechny komponenty Microsoft Office: Microsoft Word, Microsoft Excel, …

Testování více oblastí najednou

Konfigurace programu pro testování integrity dat může obsahovat více oblastí pro testování najednou (například všechny lokální pevní disky). V dnešní době nejsou žádnou výjimkou disky o velikosti 1 GB nebo větší a průměrná velikost disků neustále prudce roste. Na druhé straně ještě stále je 32 MB paměti zřídkavým jevem. Z tohoto důvodu jsme při návrhu programu učinili kompromis, který spočívá v tom, že se jednotlivé nastavené oblasti testují samostatně po sobě. Má to tu výhodu, že program nemusí zpracovávat obrovské množství informací o všech oblastech najednou. Na druhé straně ovšem tento kompromis způsobil skutečnost, že program po zpracování každé oblasti požádá uživatele o její vyhodnocení a případné uložení dat o změněných souborech do databáze (aktualizace databáze). Až po této aktualizaci pro každou oblast program pokračuje ve zpracovávání dalších dat.

Ve skutečnosti to znamená, že program čeká na vyvolání kontextového menu v prohlížeči a vybrání jedné z položek, které pracují se změnami.



Informace o programu

Stránka s informacemi o programu neobsahuje žádný ovládací prvek, ale přesto byjste ji měli věnovat určitou pozornost. Jsou zde uvedeny důležité informace:

1. kdo vlastní licenci programu,
2. aktuální informace o operačním systému,
3. detailní informace o překladu programu,
4. informace o autorských právech vztahujících se k programu.

Některé z těchto informací budete pravděpodobně potřebovat, když se obrátíte na naší firmu se žádostí o technickou podporu.

Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že tyto informace neposkytnete.

Rychlý test integrity dat

Tento program je určen pro rychlou kontrolu změn obsahu jednotlivých vybraných souborů. Vychází ze stejné metody jako **Program pro testování integrity dat**. Údaje o souborech (kontrolní součty) se však neukládají do databáze, ale do Registru Windows 95 resp. Windows NT, kde jsou uloženy systémové informace těchto dvou prostředí. Množiny souborů, které chceme otestovat v rámci jednoho běhu, zadáváme při nastavení konfigurace pro tento program. Počet souborů v konfiguraci není omezen, avšak velký počet souborů v jedné konfiguraci je v rozporu s filosofií tohoto testu (jednoduchý a rychlý). Při testu se vypočte kontrolní součet souboru a porovná se součtem, uloženým v Registru. Uvedený test je výhodné použít pro rychlé zjištění změn základních důležitých systémových souborů jako např. win.com (command.com), io.sys, gdi.exe, gdi32.dll apod.

Program běží ve dvou módech. Buď je možné spustit test tak, že uživatel může sledovat průběh a výsledky testu v dialogovém okně nebo nechat proběhnout test skrytě a pouze v případě nalezení změny alespoň jednoho souboru, program vypíše zprávu na obrazovku, případně vydá zvukový signál. V případě změny ovšem program spustí následně test s dialogem, v němž je vidět, které soubory byly změněny a jejich kontrolní součty. Jestliže zjistíte, že změna souboru byla způsobena korektním způsobem (např. přeinstalováním software), můžete obnovit kontrolní součet souboru v konfiguraci. K tomuto účelu slouží kontextové menu "Obnovit vybrané soubory". I tento program má standardní konfiguraci, která obsahuje základní soubory operačního systému.

Spuštění programu:

Pro spuštění programu platí stejná pravidla jako pro spouštění jakéhokoli jiného programu ve vašem operačním systému. Nejjednodušší metodou však stále zůstává použití konzole

testů. Zde můžete zároveň určit počáteční nastavení konfigurace.

Parametry příkazové řádky:

Program akceptuje jeden parametr uvedený na příkazové řádce. Obecný předpis pro spouštění programu je:

```
SGW [@<jméno konfigurace>]
```

kde „@" je znak, kterým musí parametr začínat (pokud je uveden) a „<jméno konfigurace>" je jedno ze jmen uvedených v seznamu možných konfigurací konzole testů. Pokud chcete použít jedno zrezervovaných jmen (jsou uvedena hvězdičkou), musíte vynechat první znak (tuto hvězdičku).

V případě, že nepoužijete žádný parametr příkazové řádky, spustí se program v manuálním režimu a pro spuštění testů budete moci vybrat jednu z nabízených konfigurací nebo nastavit konfigurační data manuálně stiskem příslušného tlačítka.

Co nabízí Rychlý test integrity dat

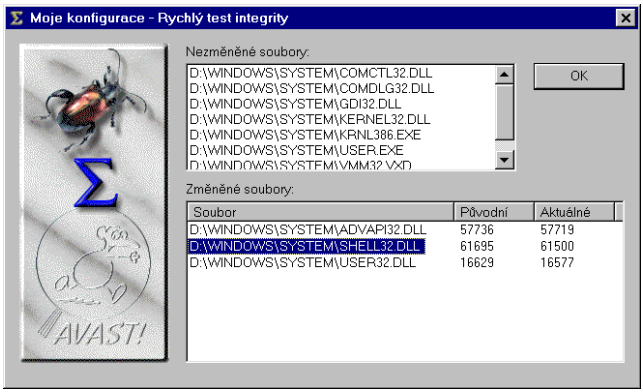
Rychlý test integrity nabízí pouze

1. hlavní stránku

Hlavní stránka programu

Hlavní stránka obsahuje dva seznamy souborů. V jednom seznamu jsou soubory beze změn a ve druhém soubory, ve kterých byla nalezena změna. V průběhu testu se seznamy plní jmény souborů, které již prošly testem. V seznamu změněných souborů jsou u každého z nich uvedeny dva jeho kontrolní součty – původní a právě spočítaný. Jestliže zjistíte, že změny souboru byly způsobeny korektním způsobem (např. přeinstalováním software), můžete obnovit kontrolní součet souboru v konfiguraci. K tomuto účelu slouží kontextové menu "Obnovit vybrané soubory". Toto menu aktivujete stiskem pravého tlačítka myši na okénko se seznamem souborů, které byly změněny. Nejprve ovšem musíte označit příslušné soubory v daném seznamu.

Podle nastavení konfigurace může Rychlý test integrity běžet také skrytě a nechat oznámit pouze nalezené změny souborů.



Tato stránka je úmyslně prázdná

Co s nalezeným virem?

- **Je to falešný poplach?**
- **Poplach způsobený použitím dvou scannerů najednou**
- **Poplach způsobený imunizací programů**
- **Poplach způsobený žertovnými programy**
- **Poplach způsobený chybou…**
- **Je to opravdu virus!!!**
- **První akce**
- **Jaký typ viru infikoval můj počítač?**
- **Kombinované (multipartitní viry)**
- **Viry, které zůstávají instalované v paměti**
- **Viry napadající soubory**
- **Viry napadající systémové oblasti disků**
- **Makro viry**

Je to falešný poplach?

Před tím, než propadnete panice a začnete mazat detekované soubory, volat antivirovou službu nebo požádáte o časově neomezenou dovolenou, musíte zjistit, zda je detekovaný soubor opravdu napaden nebo zda se jedná o falešný poplach. Ten může být způsoben několika různými příčinami, například:

1. poplach způsobený použitím dvou scannerů najednou,
2. poplach způsobený imunizací souborů,
3. poplach způsobený žertovnými programy,
4. poplach způsobený chybou techniky, programového vybavení nebo uživatele.

AVAST32 je vytvářen se zřetelem na minimalizaci falešných poplachů. Pravidelné testování proti nim zahrnuje asi 4 GB (4096 MB) souborů různého původu a obsahu. Nicméně i přes takto důkladné testování se může stát, že AVAST32 poskytne falešné hlášení. Pokud se tak stane, prosím spojte se s námi. Pomůžete nám zlepšit náš produkt a vy se budete moci cítit bezpečněji.

Pokud nebudete rozumět dalšímu výkladu této kapitoly, nic si z toho nedělejte. Zkušenost v práci s počítačem nepatří mezi vrozené vlastnosti. Pouze se v případě nalezení viru obraťte na odborníky.

Poplach způsobený použitím dvou scannerů najednou

Pokud používáte několik různých scannerů najednou nebo těsně po sobě, může se stát, že vám některý z nich ohlásí virus v paměti. Důvod pro toto hlášení je jednoduchý. Každý ze scannerů potřebuje alespoň na chvíli mít informace o virech nezakódované a přístupné v paměti. Pokud ve stejném okamžiku testuje tuto paměť jiný scanner nebo pokud je tato paměť přesunuta do virtuální paměti a později použita bez vyčištění, může se stát, že jsou tyto informace příčinou falešného poplachu.

Situace je jednodušší, pokud jsou tyto scannery napsány „špatně“, tzn. tak, že nečistí svou paměť. V tomto případě je velice pravděpodobné, že v paměti naleznete několik (např. 5 a více) různých druhů virů. V tomto případě je situace jasná, jde o falešný poplach.

Horší situace je v případě, že jsou scannery napsány „dobře“ a paměť si po sobě čistí. I v tomto případě se může stát, že naleznete virus v paměti.

Jak zjistit, zda se nejedná o falešný poplach? Je to dost snadné, ale možná časově náročné. Ukončete práci se všemi aplikacemi, ukončete operační systém a vypněte počítač síťovým vypínačem. Znovu jej zapněte a nastartujte operační systém. Spusťte scanner, který vám hlásil přítomnost viru v paměti. Pokud jej opakovaně nehlásí, pokuste se reprodukovat práci (spouštění programů), kterou jste dělali před spouštěním scannerů a po chvíli znovu spusťte testování proti virům. Pokud ani v tomto případě není nalezen virus v paměti, jedná se o falešný poplach.

AVAST32 důsledně čistí veškerou používanou paměť a co více, veškeré informace a vzorky virů uchovává pouze v kódovaném stavu. Pouze v okamžiku testování dekóduje informace o jednom viru a po použití tuto informaci smaže. To znamená,

že v každém okamžiku může být v paměti maximálně jeden dekódovaný vzorek viru.

Poplach způsobený imunizací souborů

Existují antivirové prostředky, které nabízí a pracují s funkcí, kterou nazýváme „**imunizace souborů**“ nebo s funkcí, která nabízí připojení kontrolní sumy k testovanému souboru. Při následujícím testování tyto prostředky jednoduše zkontrolují vloženou informaci s aktuálním stavem a na základě výsledku mohou oznámit podezření z napadení souboru virem. Tento proces je velice rychlý a poměrně jednoduchý pro implementaci.

Ovšem tento poměrně jednoduchý a rychlý proces s sebou nese několik zásadních problémů. Představte si dva produkty takto pracující používané pro testování jednoho souboru. Jejich střídavé používání se navzájem ruší a oba produkty budou hlásit, že soubor byl změněn.

Další problém je skutečnost, že pouhé otestování souboru jej fyzicky změní. Když pomineme problémy autorských práv originálních souborů, vyvstává zde otázka, zda si můžete být jisti, že změněný soubor bude i nadále pracovat tak, jak jeho originál. Pravděpodobně ano, ale existují programy, které se před spuštěním zkontrolují a nebudou pracovat k případě jakékoli změny. Navíc výše uvedené řádky platí pouze pro výkonné soubory. Jakákoli změna datových souborů s sebou nese vysoké riziko havárie programu, který tyto datové soubory používá.

*Pokud si myslíte, že se viry nemohou šířit v datových souborech, měli jste donedávna pravdu. Dnes již existuje speciální skupina virů („**Makro viry**“). Tyto viry se šíří výhradně pomocí datových souborů.*

AVAST32 žádným způsobem nemodifikuje žádný testovaný soubor. Z důvodů větší bezpečnosti jej dokonce otevírá pouze pro čtení, aby ani náhodou nemohlo dojít k jejich narušení. Pokud si některé součásti AVAST32 ukládají informace o souborech, dělají tak do samostatného souboru.

Pouze ve speciálním případě, při odstraňování nalezených virů, jsou soubory zapisovány, ale i tak je tento proces prováděn na kopii souboru a až po úspěšném dokončení je opravený soubor zapsán s původním jménem.

Poplach způsobený žertovnými programy

Pokud se vám stane, že se počítač začne chovat nezvykle až podezřele, nemusí jít o virus. Může se jednat o „žertovný" program, který vám nainstaloval na počítač kolega, nebo který je vám podstrčen s falešnou nebo zavádějící informací o jeho účelu. Případem může být instalace předvádění „lechtivých" obrázků při startu počítače. Slabší povahy nebo méně zkušení uživatelé mohou mít problémy s uvedením do původního stavu a podobný „žert" mohou považovat za působení zvlášť zákeřného viru.

Nicméně nemusí to být pravda. A jak rozeznat „žert" od opravdového viru? Může to být obtížné. Přesné hranice těchto dvou skupin není možné stanovit. Je zapotřebí vycházet z konkrétní situace. Například viry si nemohou dovolit předvádět nějaké grafické obrázky (navíc v barvách), protože ty jsou dost veliké. Nejdůležitější rozdíl, který ovšem není snadné rozeznat, je to, že se viry rozmnožují a „žerty" ne.

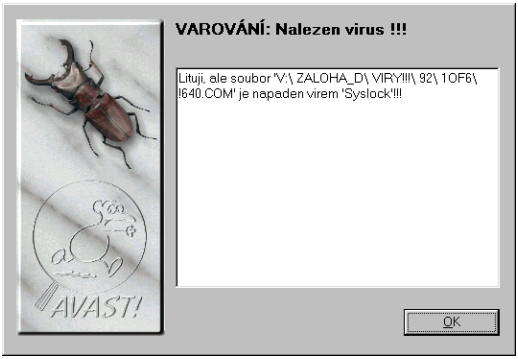
Poplach způsobený chybou techniky, programového vybavení nebo uživatele.

Problémy s technikou, instalovanými programy nebo dalšími zařízeními mohou být snadno zaměněny s virovou nákazou. Například častými problémy, které bývají takto zaměňovány, jsou problémy s tiskem. Existuje ovšem velice málo virů, které mohou způsobovat tyto problémy.

Na druhou stranu rozlišit hlášení „**Memory parity error**" může jenom odborník, protože toto hlášení může být způsobeno vadným paměťovým čipem ale také virem, který jej vypíše na obrazovku. Zde mohou pomoci jenom zkušenosti.

Je to opravdu virus!!!

Pravděpodobně první, co vás napadne, může být „**Proč právě já?!**“. Není to nic divného, velká většina uživatelů se již s virem setkala a nebezpečí nehrozí pouze počítačovým „poustevníkům“. Při troše štěstí nemusí nákaza způsobit velkou škodu. **Na druhé straně štěstí více přeje připraveným!!**



První akce

Základem je nepropadnout panice. Škoda, kterou virus mohl způsobit, může být zanedbatelná v porovnání s tím, co můžete způsobit vlastní ukvapenou akcí.

Panika je váš nepřítel. Pokud jste typ, který snadno panikaří, při nalezení viru nechte počítač na pokoji a běžte si dát šálek kávy. Pak zavolejte vašeho správce počítače. Uvidíte, že problém není až tak vážný.

Klidně si přečtete informaci, kterou vás program o nalezení viru informoval. Pravděpodobně bude obsahovat informaci o typu viru. Pokud tomu tak není, jistě v scanneru naleznete možnost získat alespoň stručnou informaci o příslušném viru. Tyto informace budete později potřebovat.

Pokud chcete něco dělat bez pomoci druhých, klidně ukončete práci všech pracujících programů a uložte si svá data. Může se také stát, že musíte dokončit právě prováděný program. Nic se neděje, nechte jej dokončit, co je zapotřebí. Máte

čas, jenom nepatrná část virů je závislá na čase, po který jsou aktivní. Vyvarujte se pouze spouštění dalších programů (pokud to jde). V žádném případě nevypínejte počítač síťovým vypínačem. Důsledky by mohly být pro vaše data na pevném disku katastrofální.

*Vypnutí počítače síťovým vypínačem bez předchozího ukončení práce operačního systému („**shut down**“) je zlozvyk srovnatelný s kouřením marihuany. Také se nemusí nic stát…*

Pokud se vám povedlo ukončit operační systém, vypněte počítač síťovým vypínačem. Odpočiňte si, protože nastala doba přemýšlení, co dělat dále.

Tento čas je zapotřebí využít. Nepotřebujete se jenom zbavit se viru, ale potřebujete zjistit nebo alespoň s velkou pravděpodobností zjistit zdroj nákazy (pravděpodobně váš přítel s nejnovější verzí známé hry). Velice důležitou otázkou je, jak dlouho můžete mít virus v počítači.

Raději buďte pesimističtí, vyplatí se to. Podcenění této doby znamená udělat první krok k opakované infekci!!

Neméně důležité je promyslet si, zda jste nemohl rozšířit virus dále. Je jedno, zda máte nakažen firemní počítač a vaše firma rozeslala tisíce nakažených disket, nebo jste pouze věnoval novou verzi hry svému příteli. V obou případech je nejlepší ihned informovat všechny, kterých se může potenciální nákaza týkat. **Udělejte to teď!!**

Ostuda spojená s rozšířením virové nákazy je mnohem snesitelnější, když na nebezpečí sami upozorníte. V případě firmy jde o důvěru zákazníků, kterou můžete úplně ztratit, pokud zjistí nákazu a zjistí, že jste o ní věděli a neinformovali je (možná si to můžete dovolit).

Jednou z nejdůležitějších věcí, které musíte posoudit je to, zda skutečně máte zálohovaná všechna důležitá data z infikovaného počítače.

Každé odstraňování viru s sebou nese riziko kompletní ztráty dat na vašich pevných discích i v případě, že odstraňování provádí vyškolený a velice zkušený odborník.

Je nám jasné, že o potřebě zálohovat dobře víte. Ale ruku na srdce, kdy naposled jste zálohoval? A pokud to děláte pravidelně, zkusil jste někdy obnovit uložená data nazpátek? A i když obě podmínky splňujete, máte záložní kopii zálohovacího programu jinde než na infikovaném počítači? Co když se na ten počítač již více nedostanete?

Takže, pokud nemáte aktuální zálohu, teď právě je čas ji udělat. Již se nedá nic dělat a musíte ji vykonat s vědomím, že zálohovaná data mohou obsahovat virus a zároveň, že každé další spouštění počítače může zvyšovat stupeň infikování systému. Ale nedá se nic dělat. Záloha je opravdu zapotřebí i v případě, že další práci bude vykonávat někdo úplně jiný (hlavně někdo, kdo nenese žádnou odpovědnost za vaše data).

Takže malé shrnutí. V případě nákazy virem:

1. dokončete práci, zbytečně nespěchejte ale ani neotálejte s dalšími opatřeními,
2. zjistěte co nejvíc informací o viru,
3. ukončete práci operačního systému,
4. vypněte počítač síťovým vypínačem,
5. rozmyslete si, jak dlouho můžete mít počítač nakažen a odkud pravděpodobně nákaza přišla,
6. informujte všechny, kterým jste mohl nakažená data nebo média rozeslat,
7. pokud to je zapotřebí, zazálohujte. Nenechávejte nic na náhodě!!!

Pokud jste splnil tyto body, můžete přistoupit k další práci. Zde musíte kriticky ohodnotit své vlastní schopnosti a zkušenosti s počítačem. Pokud tomu moc nerozumíte, nedoporučujeme vám odstranění viru vlastními silami. Pokud ale budete rozumět dalšímu výkladu, můžete to zkusit bez odborné pomoci. Jak na to? Na tuto otázku se pokusíme odpovědět.

Jaký typ viru infikoval můj počítač?

Je důležité vědět, jaký typ viru je přítomen na vašem počítači. Další postup na tom přímo závisí a zároveň některé jemné nuance určení typu viru mohou postup odstraňování virů zřetelně změnit.

Pokud se někomu bude zdát následující výklad málo odborný, je to způsobeno maximální snahou o zachování čitelnosti této kapitoly i pro ty naše uživatele, kteří se nesetkávají s viry pravidelně.

Takže základní typy virů jsou:

1. kombinované (multipartitní viry),
2. viry, které zůstávají instalované v paměti,
3. viry napadající soubory,
4. viry napadající systémové oblasti disků,
5. makro viry

Prakticky všechny výše uvedené typy virů napadají pouze spustitelné soubory. Proto v dalším textu budeme implicitně předpokládat, že napadený soubor je program libovolného typu. Pouze kapitola Makro viry pojednává o virech v datových souborech (dokumentech).

Pokud narazíte na velice zřídka se vyskytující virus, který mění nebo modifikuje datové soubory, máte pravděpodobně smůlu v tom, že tato data jsou velice nevěrohodná nebo přímo nepoužitelná. Zároveň neexistuje prostředek, jak zničené datové soubory opravit (snad kromě zálohy statických dat).

V dalším textu budeme předpokládat, že používáte operační systém Microsoft Windows 95 nebo Microsoft Windows NT. Odstraňování virů v systému DOS se může lišit od zde uvedených postupů.

Kombinované (multipartitní viry)

Kombinované viry jsou jednoduše viry, které napadají některou z kombinací souborů, systémových oblastí disků a paměti najednou. Jejich odstraňování je kombinací odstraňování jednoduchých typů virů v přesně určeném pořadí. Pro toto pořadí platí:

1. není možné odstraňovat virus z disku, pokud je přítomen v paměti,
2. při odstraňování virů z disků je zapotřebí odstranit viry ze systémových oblastí disků jako první,
3. viry v jednotlivých souborech se odstraňují až jako poslední.

Viry, které zůstávají instalované v paměti

Tyto viry nejsou instalované pouze v paměti, ale jistě jsou přítomny i někde na disku.

Pokud vám některý „odborník" bude tvrdit, že virus může být v paměti bez toho, aby byl přítomen někde jinde (na pevném disku, disketě nebo jiném médiu podobného typu), obraťte se na někoho jiného. Vaše data budou mnohem bezpečnější.

Zároveň nemůžete odstraňovat virus z vašeho systému v okamžiku, kdy je přítomen v operační paměti a je aktivní.

Virus může být v paměti a zároveň nebýt aktivní. Představte si situaci, že kopírujete infikovaný soubor z diskety na disketu. I v tomto případě je používaná operační paměť počítače a zdrojový i výsledný soubor jsou nahrány v ní. To znamená, že virus může v paměti existovat i po ukončení kopírování jednoduše proto, že není důvod, proč takto použitou paměť čistit. To ovšem neznamená, že virus v této podobě může jakkoli škodit.

Důvod je prostý, virus ihned napadne každý program nebo systémovou oblast disku, kterou se pokusíte vyléčit. S tím neuděláte nic. Obecně platí, že nemůžete eliminovat virus v paměti v době, kdy je v ní přítomen. Samozřejmě, mohou existovat výjimky, ale na to se nemůžete spolehnout.

Zároveň musíme zdůraznit, že viry určené speciálně pro tyto operační systémy dnes prakticky neexistují a z těch několika velice řídkých případů žádný není schopen zůstat rezidentně v paměti. Pokud se situace změní, budeme vás o tom informovat.

Z předchozího odstavce vyplývá, že v paměti může být jenom virus určený pro systém DOS, který se do ní dostal při startu počítače nebo při práci v DOSovém okně. Pokud se zároveň

jedná o virus, napadající systémové oblasti disků, můžete přejít přímo ke kapitole o virech tohoto typu. Pokud jde o viry napadající soubory, řešení, jak odstranit virus z paměti není složité.

V tomto druhém případě nakonfigurujte operační systém tak, aby při startu nepouštěl žádný DOSový program a restartuje jej. Zní to jednoduše, ale realita již tak jednoduchá být nemusí. V těchto operačních systémech nemusí být tak snadné zjistit, které všechny programy se spouštějí při startu. Nejsou to totiž jenom programy ze startovací skupiny ale mohou to být také programy, kterých jméno je zapsáno na přesně určených místech v „**Registru**" operačního systému. Navíc ne všechny programy musejí mít viditelnou ikonu na pracovní ploše.

Nicméně, pokud se vám podařilo nastartovat počítač bez jakýchkoli DOSových programů, nebudete mít virus v paměti a můžete pokračovat dále.

Viry napadající soubory

Odstranění virů ze souborů je jednoduchá a dosti nezáživná práce. Hlavní problém spočívá v rozhodnutí, jak virus odstranit. Máte zase na výběr několik možností.

Stoprocentní obnovení zabezpečí pouze restaurování souborů ze záložních kopií (samozřejmě, pokud zálohu máte a pokud i tato záloha není napadená stejným nebo jiným typem virů). Obnova ze záložních kopií může být jednoduchá a spolehlivá. Pokud pravidelně věnujete čas zálohování, zjistíte, proč se to vyplatí. Práce je to rychlá a spolehlivá.

Pokud používáte pravidelně program pro kontrolu integrity a máte k dispozici aktuální verzi databáze, máte také prakticky po starostech. AVAST32 umožní restaurovat soubory napadené prakticky všemi viry (přibližně 95 procent různých druhů virů). Spolehlivost obnovy je stejná jako v případě obnovy souborů ze záložních kopií, protože AVAST32 kontroluje, zda se mu povedlo soubor restaurovat do posledního bitu.

Pokud nic z výše uvedených odstavců nemůžete použít, začíná být situace vážnější. Stále ještě nemusíte přijít o žádné programy. Musíte ale mít k dispozici originální diskety nebo jejich kopie. Znamená to ovšem podstatně více práce, protože nakažené programy musíte odinstalovat a opakovaně na–

instalovat, což s sebou nese spoustu známých problémů s uchováním pracně vymyšlených konfigurací.

Deinstalace programů neznamená jejich prosté smazání z disku. Všechny „solidní" programy pro tyto operační systémy mají schopnost deinstalace, která má na starost více než pouhé smazání souborů.

Pokud ani tento způsob nemůžete použít, máte problém. Opravdu velký problém, protože vám doporučíme pouze smazání napadených souborů. Existuje sice ještě jedna potenciální varianta, kterou můžete použít, ale její výsledky mohou být dosti tristní. Jde o pokus o odstranění virů ze souborů pomocí některého jiného antivirového balíku. Toto odstranění má jednu velkou nevýhodu. Nemůžete zjistit, zda je opravený soubor ve stejném stavu, v jakém byl před napadením. To je také hlavní důvod, proč AVAST32 žádnou podobnou vlastnost neobsahuje.

Viry napadající systémové oblasti disků

Existuje obrovské množství virů schopných napadnou systémovou oblast pevných disků. Ovšem jen několik z nich je tzv. „kombinovaných virů", které jsou schopny napadnout a šířit se také pomocí souborů. Proto s malou výhradou můžeme říci, že pokud jste nalezl virus v systémové oblasti, stalo se to tak, že jste se pokoušel nastartovat počítač z diskety. Je jedno, zda se to povedlo nebo ne, pokud byl na té disketě virus, napadl Váš počítač bez ohledu na to, jaký operační systém normálně používáte.

Je úplně zbytečné se domnívat nebo dokonce někoho přesvědčovat, že například virus „J&M" neboli „JiMi" se dostal do vašeho počítače pouhým přečtením dat z diskety. Jednoduše to není pravda, ať již vám to tvrdí kdokoli. Je to prostě nesmysl.

Výjimkou ovšem je například virus „OneHalf", který se může šířit pomocí souborů, což znamená, že spuštěním infikovaného souboru dojde k napadení počítače. Podobných virů je ovšem naprosté minimum.

Napadení počítače virem tohoto typu je nepříjemné a může být fatální. V případě systému Microsoft Windows 95 ještě není situace tak zlá. Virus je možné odstranit pomocí standardní záchranné diskety, kterou si můžete vytvořit při instalaci systému nebo kdykoli jindy pomocí standardních prostředků Microsoft Windows 95 (položka „Přidej/Odeber programy" v „Kontrolních panelech"). Z této diskety je možné systém nastartovat a standardním postupem virus odstranit.

Standardní postup zde znamená nastartovat systém ze systémové diskety a spuštění následujících programů v pořadí a ve tvaru, v jakém jsou zde uvedeny:

```
fdisk /MBR
sys C:
```

Je pouze důležité, abyste nepoužili systémovou disketu jiného operačního systému (DOS) a aby tato disketa nebyla napadena virem. Po úspěšném provedení těchto příkazů bude virus ze systémových oblastí disku provozujícího Microsoft Windows 95 odstraněn.

Zcela jiná situace je v případě Microsoft Windows NT. Pokud se vám povede infikovat systém tímto virem, budete mít problémy. Problémy mohou být snadno řešitelné nebo vůbec neřešitelné. Nic mezi tím neexistuje.

Pokud se vám povede nastartovat operační systém, máte prakticky vyhráno. Můžete použít schopností obnovy operačního systému, které jsou v něm zabudovány a ty se postarají o zbytek. Pokud ovšem nenastartujete systém vůbec, je zle a vaše poslední naděje spočívá v tom, kterou systémovou oblast disku systém napadl. Pokud je to oblast zvaná „Master Boot Record", můžete zkusit klasický program FDISK z DOSu verze 6 a vyšší. Po nastartování počítače z nezavirované systémové diskety DOSu 6 a vyššího spustíte program:

```
fdisk /MBR
```

Pokud se po úspěšném spuštění tohoto programu povede nastartovat Microsoft Windows NT, dejte si sklenku šampaňského (nebo Kolalokovy limonády, záleží jen na vás). Máte na to právo. Pokud ani toto nepomůže, připravte se na to, že budete muset nainstalovat Microsoft Windows NT kompletně od začátku, což s sebou nese vysokou pravděpodobnost ztráty

veškerých dat. Je nám líto, ale v současné době lepší postup neznáme.

Makro viry

O makro virech se toho nedá povědět mnoho. Tyto viry pracují pouze do té míry, do které pracují příslušné aplikace pod vašim operačním systémem. Pokud zde není rozdíl v jazykové mutaci jednotlivých programů na různých počítačích, jsou tyto viry plně kompatibilní a pracují tak, jak autoři předpokládali.

Způsob jejich odstranění je přímo závislý na příslušné aplikaci.

Například viry pracující pod populárním textovým editorem Microsoft Word 6.0 jsou v současné době velmi populární. Ovšem – a to je štěstí většiny uživatelů – tyto viry existují pouze v anglických nebo německých mutacích a tak nemohou českou lokalizovanou verzi Wordu napadnout.

Odstranění makro viru z dokumentu není prosté a zcela nejjednodušší metoda je tato:

1. otevřít dokument,
2. otevřít menu Soubor/Šablony,
3. použít tlačítko Organizátor a v něm položku Marka,
4. vyberte si volbu makra v dokumentu a všechny je smažte,
5. pokud ještě máte nějaký dokument, pokračujte bodem 1,
6. jinak navolte makra ze šablony normal.dot a všechny je smažte,
7. podle našich zkušeností byste měl mít nyní klid až do další infekce.

Není vyloučeno, že v některé z dalších verzí AVAST32 bude přímo zabudovaná podpora pro odstranění tohoto druhu virů. Jistě vás o této vlastnosti budeme včas informovat.

Tato stránka je úmyslně prázdná

Konfigurace testů

- **Vytvoření konfigurace programu pro hledání virů**
- **Vytvoření konfigurace programu pro detekci změn**
- **Vytvoření konfigurace pro rychlý test integrity dat**
- **Vytvoření uživatelské definice viru**

Až sem jste mohli číst dost povídání o konfiguraci, ale co to vlastně konfigurace je? Nemáme v úmyslu zde předkládat nějakou obecně platnou filozofickou definici. Pro potřeby souboru antivirových programů AVAST32 je konfigurace seznam parametrů řídících běh programu.

Konfigurace v kontextu této kapitoly přímo ovlivňuje způsob provádění testů. Nemá nic společného s vlastní konfigurací programu, například s barvou a umístěním okna, použitými fonty,… Tato konfigurace je popsána na jiném místě v případě, že existují parametry, které se mohou nastavovat.

Reálné uložení těchto parametrů v době, kdy je počítač vypnut, není pro normálního uživatele důležité. Pokud máte opravdu zájem detailně sledovat uložení konfiguračních dat, doporučujeme důkladně prostudovat přílohu C, kde je místo jejich uložení přesněji popsáno.

Na tomto místě musíme upozornit, že přímá změna konfiguračních parametrů AVAST32 nebo v horším případě jiných programů nebo operačního systému může vést k zhroucení postižené části a ztrátě dat. Proto všechny manuální změny nechte na odbornících pro daný operační systém.

Jak nějakou konfiguraci vytvořit? Máte k dispozici dva způsoby, které jsou plně nahraditelné a jejich výsledkem je úplně rovnocenná konfigurace. Prvním z nich je použití kon–

textového menu z konzole testů a druhým je použití tlačítka „**Nový test**“ z hlavního okna programu, který vytváření konfigurací podporuje. Tyto dva způsoby se liší jenom v okamžiku zadávání jména konfigurace. V prvním z nich musíte zadat jméno jako první, ve druhém jako poslední parametr. Ve druhém případě je zadání jména konfigurace a její uložení volitelné. Nicméně v každém případě je tato konfigurace použita pro testování.

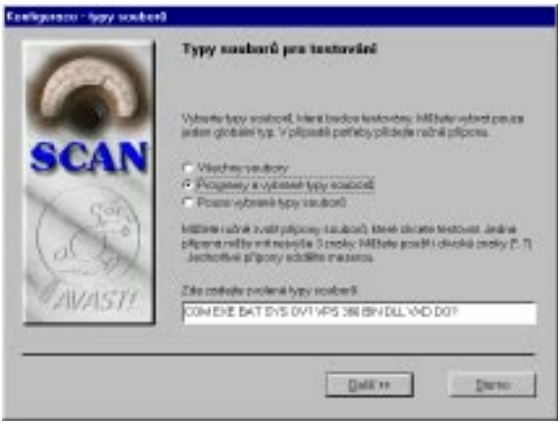
Zadávání jednotlivých parametrů probíhá prostřednictvím samostatných dialogů, kde jsou jednotlivé parametry uspořádány do skupin podle svého významu. Pokud chcete definovat některou konfiguraci, musíte projít veškeré dialogy až do konce. Zrušit definici můžete kdykoli stiskem tlačítka „**Storno**“, přičemž jsou zadaná data zrušena bez další výstrahy.

Pokud používáte konzoli testů, můžete již vytvořenou konfiguraci změnit. Jediný rozdíl oproti vytvoření nové konfigurace je ten, že při změně již existující nezadáváte její jméno. Proto bude v další části popsáno pouze vytvoření nové konfigurace.

Vytvoření konfigurace programu pro hledání virů

Vytváření konfigurace programu má následující kroky:

1. zadání jména konfigurace (pouze v případě, že jste vyvolal vytváření konfigurace z konzole testů)
2. určení typů souborů, které budou testovány. Typy souborů můžete určit obecně, vyjmenováním příslušných typů souborů nebo jejich kombinací,



Pokud chcete urychlit rutinní testování, zvolte test pouze vyjmenovaných typů souborů. Pokud tak učiníte, program nebude muset kontrolovat typ každého souboru podle jeho obsahu a rozeznávat, zda jde nebo nejde o výkonný soubor (program).

3. oblasti pro testování. Můžete použít některého z obecných nastavení, která se zjišťují až v době běhu programu nebo můžete manuálně (opravdu manuálně nebo výběrem z dialogu) zadat potřebné oblasti. Pod pojmem oblast se zde rozumí disk nebo adresář. Jméno disku nebo adresáře můžete zadat standardní konvencí známou z dob operačního systému DOS nebo můžete použít UNC (Universal Naming Convention),
4. další jednoduché parametry. Tato skupina obsahuje jednoduché přepínače, které modifikují průběh testů a z části také chování programu,
5. vytváření REPORT souboru. Tato skupina umožňuje specifikovat zda vůbec a pokud ano, kde a jakým způsobem vytvářet textový soubor s informacemi o průběhu testování,
6. hlášení o nalezení viru. Toto hlášení je zobrazeno v případě nalezení prvního viru v souborech, viru v systémové oblasti libovolného disku nebo viru v paměti,
7. určení, zda chcete vytvořenou konfiguraci uložit (pouze pokud jste vyvolal vytvoření konfigurace přímo z programu pomocí tlačítka „**Nový test**“).

Vytvoření konfigurace programu pro detekci změn

Vytváření konfigurace programu pro detekci změn má následující kroky:

1. zadání jména konfigurace (pouze v případě, že jste vyvolal vytváření konfigurace z konzole testů,
2. určení typů souborů, které budou testovány. Typy souborů můžete určit obecně, vyjmenováním příslušných typů souborů nebo jejich kombinací.

Pokud chcete urychlit rutinní testování, zvolte test pouze vyjmenovaných typů souborů. Pokud tak učiníte, program nebude muset kontrolovat typ každého souboru podle jeho obsahu a rozeznávat, zda jde nebo nejde o výkonný soubor (program).

3. oblasti pro testování. Můžete použít některého z obecných nastavení, která se zjišťují až v době běhu programu nebo můžete manuálně (opravdu manuálně nebo výběrem z dialogu) zadat potřebné oblasti. Pod pojmem oblast se zde rozumí disk nebo adresář. Jméno disku nebo adresáře můžete zadat standardní konvencí známou z dob operačního systému DOS nebo můžete použít UNC (Universal Naming Convention),

4. další jednoduché parametry. Tato skupina obsahuje jednoduché přepínače, které modifikují průběh testů a z části také chování programu,
5. určení místa, kde budou uloženy jednotlivé soubory s údaji o souborech. Máte k dispozici dvě možnosti. Uložit tyto soubory v některém konkrétním adresáři (což je způsob, který doporučujeme) anebo nechat tuto položku prázdnou a databázové soubory ukládat do kořenových adresářů jednotlivých disků. V případě, že chcete testovat vzdálený disk, **musíte určit**, kde bude příslušný databázový soubor umístěn, nebo **musíte mít právo** zápisu do kořenového adresáře příslušného disku,
6. určení, zda chcete vytvořenou konfiguraci uložit (pouze pokud jste vyvolal vytvoření konfigurace přímo z programu pomocí tlačítka „**Nový test**“).

Vytvoření konfigurace pro rychlý test integrity dat

Vytváření konfigurace programu má následující kroky:

1. zadání jména konfigurace (pouze vpřípadě, žejste vyvolal vytváření konfigurace zkonzole testů)
2. výběr souborů, jejichž změny chcete zjišťovat. V dialogovém okně je uveden seznam souborů, který tato konfigurace obsa–

huje. Pokud vytváříte novou konfiguraci, je seznam pochopitelně prázdný. Soubor můžete přidat buď ručně tak, že vypíšete plnou cestu se jménem do příslušného editačního políčka a do seznamu zařadíte stiskem tlačítka "Přidat", nebo použít tlačítko "Procházet", které aktivuje standardní dialog pro otevírání souborů. Vybraný soubor se automaticky přidá do seznamu a v editačnímho políčku zůstane cesta do jeho adresáře. Můžete totiž kromě jména souboru použít v cestě masku (např. *.dll) a pak se do seznamu zařadí všechny soubory v daném adresáři, odpovídající masce. Pro takto vybrané soubory se spočítají kontrolní součty a spolu s plným jménem souboru se uloží do Registru Windows 95 resp. Windows NT pro pozdější porovnání při testu. Jméno souboru s cestou a s příslušným kontrolním součtem se zobrazuje v seznamu souborů konfigurace. V této fázi lze soubory z konfigurace také vymazat.

3. další dva parametry. Jednak volba, zda při každém běhu zobrazovat průběh a výsledky testu v dialogovém okně nebo nechat proběhnout test skrytě a pouze v případě nalezení změny alespoň jednoho souboru vydat upozornění a zvukový signál, s následným zobrazením výsledků. Druhý parametr povolí (zakáže) zvukovou signalizaci při nalezení změny (neshodě součtů) souboru v dialogovím okně a umožní případný výběr zvuku (.wav). Standardní nastavení je bez zvukové signalizace a skrytý test.

Vytvoření uživatelské definice viru

Vytváření vlastní definice viru má následující kroky:

1. informace o problémech, které může způsobit nesprávná nebo špatně zvolená definice,
2. určení jména viru. Toto jméno musí být jedinečné nejenom mezi uživatelem definovanými viry, ale nesmí se vyskytovat ani mezi viry z definičního souboru dodávaného s AVAST32,
3. určení typů oblastí, které je schopen virus napadnout. To znamená jaké typy souborů je virus schopen napadnout, zda napadá systémové oblasti disků nebo dokonce zůstává rezidentní v paměti,
4. určení charakteristického řetězce viru, které je nejchoulostivější operací při definici nového viru. To neznamená, že zde nemůžete zadat jakýkoli identifikační řetězec, který vyhovuje určitým jednoduchým podmínkám, ale jde o to, aby daný řetězec měl smysl a pracoval alespoň tak dobře, jak definice z dodávaného definičního souboru. Nezapomeňte, že jakýkoli program je jenom tak dobrý, jak je dobrá jeho nejslabší část. Špatná volba identifikačního řetězce může zcela znehodnotit výsledky AVAST32,
5. dotaz, zda opravdu chcete zařadit definici pro testování virů.

Tato stránka je úmyslně prázdná

Průběžné testování – rezidentní scanner

- **Spuštění programu**
- **Parametry příkazové řádky**
- **Tvar hlášení**
- **Co nabízí program pro průběžné testování?**
- **Nastavení parametrů testování**
- **Nastavení varování**
- **Informace o programu**

Osobní počítače jsou nejčastěji používány v kancelářích. Naprostá většina uživatelů používá pouze několik programů (například textový procesor, tabulkový procesor, případně prezentační program atd.) a ani ty nespouští mnohokrát denně. Pokud jste právě takový uživatel, je pro vás program tohoto typu ideálním řešením.

Co to znamená rezidentní? Jde přece o pojem běžný ve světě starého DOSu a AVAST32 je určen pro zcela jiný typ operačních systémů. Nicméně obecná koncepce starých rezidentních programů může být převzata a implementována i do systémů Microsoft Windows. V tomto konkrétním případě se jedná o program, který neustále od svého spuštění sleduje, zda se operační systém nepokouší spustit některý jiný proces (program) nebo se nepokouší číst data z diskety. Pokud jednu z těchto činností zjistí, přeruší operační systém a zkontroluje, zda není spouštěný program napaden, nebo zda čtená disketa neobsahuje virus.

Při pozitivní detekci viru na disketě vás program upozorní a v případě infekce programu jej odmítne spustit. V případě infikovaných disket můžete pokračovat v práci s touto disketou pouze po potvrzení, že tuto skutečnost berete do úvahy.

Spuštění programu

Pro spuštění programu platí stejná pravidla jako pro spouštění jakéhokoli jiného programu ve vašem operačním systému.

Instalační program vám nabídne možnost automatického spouštění programu při startu systému. Tento způsob doporučujeme pro převážnou většinu našich uživatelů. Pokud tomu tak není, nejjednodušší metodou stále zůstává použití konzole testů. Program pro průběžné testování se vám povede spustit pouze jednou. Každý následný pokus o spuštění vede pouze k zobrazení hlavního okna již spuštěného programu společně se zvukovým znamením.

Program po spuštění nevytvoří standardní ikonu v hlavním panelu Microsoft Windows 95, ale umístí svou zmenšenou ikonu na jeho pravé straně. K vyvolání programu stačí cvaknout levým tlačítkem myši na tuto ikonu a program zobrazí své hlavní okno.

Parametry příkazové řádky

Program pro průběžné testování nerozeznává žádný parametr příkazové řádky. Je tudíž úplně jedno, zda zde nějaký uvedete nebo ne, program je ignoruje.

Tvar hlášení

Algoritmy rezidentní scanneru byly vyřešeny tak, že program je schopen oznámit zprávu uživateli v standardním dialogovém okně, jak je znáte z operačního systému. Po dobu jeho zobrazování je možná práce s dalšími programy mimo toho, který událost vyvolal.

Pokud je hlášení zapotřebí v okamžiku zobrazování okna DOSu v celoobrazovkovém režimu, je obrazovka přepnuta do grafického módu a okno varování je zobrazeno běžným způsobem.

Co nabízí program program pro průběžné testování?

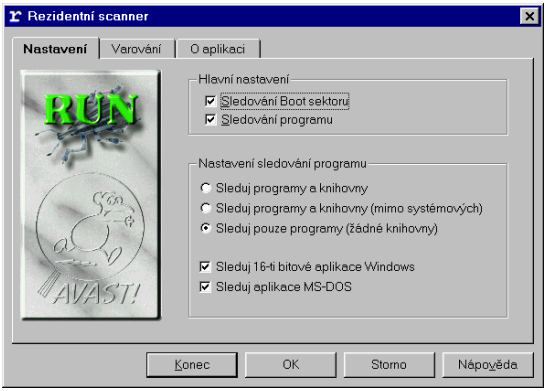
Program nabízí uživateli několik stránek, ve kterých jsou zobrazeny veškeré potřebné informace. Jednotlivé stránky jsou:

1. nastavení parametrů testování,
2. nastavení varování,
3. informace o programu.

Nastavení parametrů testování

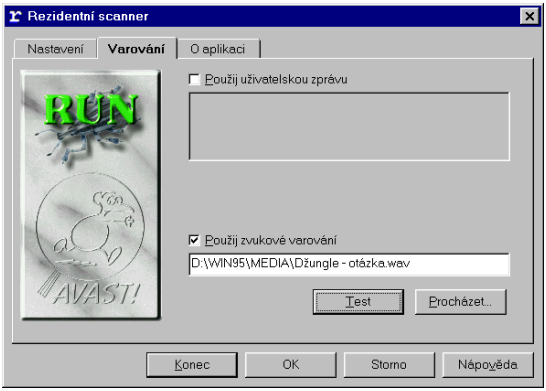
Parametry testování jsou rozděleny do dvou skupin. Jedná se o testování systémového sektoru všech používaných disket a sledování spouštěných programů. Co se týče systémových oblastí disket, zde není co nastavovat. Buď je sledování aktivní nebo ne.

Co se týká sledování spouštěných programů, je možné nastavit, které hlavní skupiny se budou testovat. Omezením počtu sledovaných souborů se urychlí práce, ale zároveň vám může některý virus uniknout a infikovat celý systém.



Nastavení varování

Tato stránka programu slouží na nastavení komunikace programu s uživatelem v případě zjištění viru v některém ze sledovaných objektů.



Informace o programu

Stránka s informacemi o programu neobsahuje žádný ovládací prvek, ale přesto byjste ji měli věnovat určitou pozornost. Jsou zde uvedeny důležité informace:

1. kdo vlastní licenci programu,
2. verze definičního souboru virů,
3. aktuální informace o operačním systému,
4. detailní informace o překladu programu,
5. informace o autorských právech vztahujících se k programu.

Některé z těchto informací budete pravděpodobně potřebovat, když se obrátíte na naší firmu se žádostí o technickou podporu.

Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že tyto informace neposkytnete.

Průběžné sledování – systémový monitor

- **Spuštění programu**
- **Parametry příkazové řádky**
- **Tvar hlášení**
- **Co nabízí systémový monitor?**
- **Nastavení parametrů testování**
- **Informace o programu**

Systémový monitor je druhým a zatím posledním příkladem „rezidentních" programů AVAST32. V tomto případě se jedná o program, který neustále od svého spuštění sleduje práci systému souborů vašeho operačního systému a v případě zjištění operace, která odpovídá nastavení, se zeptá uživatele, zda je tato operace oprávněná či nikoli.

V případě pozitivní odpovědi na dotaz programu, je operace dokončena. V případě, že si nepřejete zvolenou operaci dokončit, vše, co je zapotřebí udělat, je odpovědět negativně.

Spuštění programu

Pro spuštění programu platí stejná pravidla jako pro spouštění jakéhokoli jiného programu ve vašem operačním systému.

Instalační program vám nabídne možnost automatického spouštění programu při startu systému. Tento způsob doporučujeme pro převážnou většinu našich uživatelů. Pokud tomu tak není, nejjednodušší metodou stále zůstává použití konzole testů. Program pro průběžné testování se vám povede spustit pouze jednou. Každý následný pokus o spuštění vede pouze k zobrazení hlavního okna již spuštěného programu společně se zvukovým znamením.

Program po spuštění nevytvoří standardní ikonu v hlavním panelu Microsoft Windows 95, ale umístí svou zmenšenou ikonu na jeho pravé straně. K vyvolání programu stačí

cvaknout levým tlačítkem myši na tuto ikonu a program zobrazí své hlavní okno.

Parametry příkazové řádky

Program pro průběžné testování nerozeznává žádný parametr příkazové řádky. Je tudíž úplně jedno, zda zde nějaký uvedete nebo ne, program je ignoruje.

Tvar hlášení

Algoritmy systémového monitoru v kombinaci s vlastnostmi operačního systému neumožňují zobrazení hlášení ve tvaru standardního dialogu tak, jak je znáte z operačního systému. Hlášení programu je zobrazováno ve velice strohém stylu systémového hlášení, které je normálně používáno jenom pro vážná systémová hlášení. Po dobu jeho zobrazování není možná práce s dalšími programy, nicméně je možné použít myš pro zadání odpovědi.

Pokud je hlášení zapotřebí v okamžiku zobrazování okna DOSu v celoobrazovkovém režimu, je obrazovka přepnuta do grafického módu a okno varování je zobrazeno běžným způsobem.

Co nabízí systémový monitor?

Program nabízí uživateli několik stránek, ve kterých jsou zobrazeny veškeré potřebné informace. Jednotlivé stránky jsou:

1. nastavení parametrů testování,
2. informace o programu.

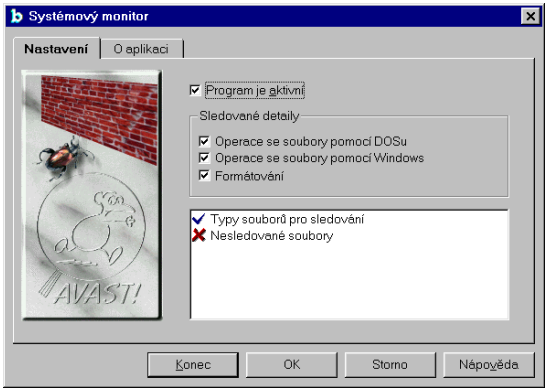
Nastavení parametrů testování

Tato stránka umožňuje nastavit celkový stav programu, to znamená, že lze program zapnout nebo vypnout. V případě, že je program zapnut, je možné blíže nastavit jednotlivé parametry sledování jednoduchým zaškrtnutím příslušného tlačítka.

V hlavním okně programu je také možné nastavit prakticky libovolné množství typů souborů, které chcete sledovat (extenzí) o libovolné délce, přičemž program plně podporuje dlouhé jména souborů operačního systému.

Do stejného okna je možné nastavit prakticky libovolný počet souborů, které program nebude sledovat. Ve skutečnosti ovšem operace s těmito soubory také sleduje, ale v případě zjištění souboru zde uvedeného nezobrazí žádné hlášení a operaci povolí. Soubory, které nemá program sledovat, je zapotřebí zadat s plnou cestou.

Jako v ostatních programech zde nejsou zobrazena žádná tlačítka pro přidávání nebo ubírání položek. Vše potřebné můžete vykonat pomocí kontextového menu, které se zobrazí po stisku pravého tlačítka myši.



Informace o programu

Stránka s informacemi o programu neobsahuje žádný ovládací prvek, ale přesto byste jí měli věnovat určitou pozornost. Jsou zde uvedeny důležité informace:

1. kdo vlastní licenci programu,
2. aktuální informace o operačním systému,
3. detailní informace o překladu programu,
4. informace o autorských právech vztahujících se k programu.

Některé z těchto informací budete pravděpodobně potřebovat, když se obrátíte na naší firmu se žádostí o technickou podporu.

Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že tyto informace neposkytnete.

Příloha A: Návrhy a doporučení

- **Spuštění programu při startu systému**
- **Program pro hledání virů a program pro detekci změn**
- **Automatické ukončení programu**
- **Průběžné testování**
- **Urychlení odezvy systému**

V této kapitole můžete najít naše doporučení, rady a nápady, které vám mohou pomoci při používání našeho produktu. Nápady a návrhy jsou rozčleněny podle jednotlivých částí AVAST32. Hned na začátku jsou uvedeny obecně platné informace. Informace platné jenom pro určitý program jsou uvedeny v odstavci pro tento program.

Spuštění programu při startu systému

Každý program produktu AVAST32 je možné spustit automaticky při startu systému. Pro toto spuštění je ovšem nutno konfigurovat operační systém tak, aby o vašem požadavku věděl. To znamená, že musíte přesunout jednotlivé programy nebo jejich zástupce (shortcut) do pořadače „**Nabídka Start (Start Menu)**“ pro Microsoft Windows 95 nebo do skupiny „StartUp“ pokud používáte Microsoft Windows NT bez nového uživatelského rozhraní. Způsob, jak to uděláte, je popsán v manuálu operačního systému a liší se pro jednotlivé operační systémy.

Programy, které rozeznávají parametr na příkazové řádce, jej musí mít uveden, jinak budou po startu čekat na jeho zadání. Výhodně zde můžete využít možnost minimalizace okna při startu a schopnost automatického ukončení některých programů.

Program pro hledání virů a pro detekci změn

Některé vlastnosti těchto dvou programů jsou společné, proto nápady a návrhy uvedené v tomto odstavci můžete použít v těchto programech stejným způsobem.

Automatické ukončení programu

Nerezidentní programy mohou automaticky ukončit svojí práci a tím uvolnit systémové zdroje. Pro využití této vlastnosti je zapotřebí splnit dvě podmínky:

1. nastavit přepínač pro automatické ukončení do stavu „**zapnuto**“,
2. program nesmí detekovat žádný soubor v testované oblasti.

Pokud používáte program pro detekci změn, ujistěte se, že v testované oblasti nejsou ukládány databázové soubory tohoto programu. Ty jsou při každém uložení změn modifikovány a tím pádem také detekovány. Program nemůže ukončit svoji práci automaticky. S výhodou zde využijete možnost ukládání těchto souborů do některého adresáře.

Průběžné testování

Některé vlastnosti těchto dvou programů jsou společné, proto nápady a návrhy uvedené v tomto odstavci můžete použít v těchto programech stejným způsobem.

Urychlení odezvy systému

Uživatelé, kteří intenzívně využívají systém, mohou zjistit, že program pro průběžné testování může zpomalit spuštění některých programů. Protože i nepatrné zpoždění může být někdy na závadu, nabízíme vám doporučení, jak toto zdržování omezit na minimum.

1. omezte používání DOSových programů na minimum. Testování programů pracujících v okně DOSu je podstatně pomalejší než testování přirozených 32–bitových programů,

2. pokud musíte použít DOSový program, důrazně doporučujeme jeho spouštění přímo z pracovní desky počítače (Desktopu). Používání mezikroku, například program „**Norton Commander**“ nebo „**Manažer M602**“ výrazně zpomaluje odezvu systému (například používání zmíněného Norton Commanderu zpomalí odezvu systému až o 300 procent při spouštění programu, ale ne při jeho samotném běhu).
3. používejte „**Prohlížeč (Explorer)**“ tak často, jak můžete. Použitá technologie testů a vlastní technologie prohlížeče výrazně urychlí odezvu počítače.

Tato stránka je úmyslně prázdná

Příloha B: Rozdíly práce mezi Windows NT a Windows 95

- **Přítomnost jednotlivých programů**
- **Problémy s viry napadajícími systémové oblasti pevných disků**
- **Testování paměti**

Microsoft Windows NT a Microsoft Windows 95 jsou zcela odlišné operační systémy. Microsoft Windows NT je systém založený na zcela odlišných základech a principy jeho práce se s Microsoft Windows 95 dají porovnat jenom stěží. Microsoft Windows 95 je stále poplatný modelu klasických Microsoft Windows 3.x. Stručně řečeno, můžeme Microsoft Windows NT porovnat k modernímu a výkonnému operačnímu systému, zatímco Microsoft Windows 95 jsou principiálně velmi podobné systému Microsoft Windows 3.11 se všemi jeho nedostatky i výhodami.

Z hlediska AVAST32 se tyto rozdíly (až na malé výjimky) stírají společným programátorským rozhraním, přičemž uživatel našeho produktu může pozorovat pouze nepatrné odlišnosti v práci produktu.

Základní odlišnost těchto operačních systémů z hlediska jejich vlivu na soubor antivirových programů AVAST32 je kompatibilita těchto systémů s klasickým DOSem. Na úrovni Microsoft Windows NT není zaručena a veškeré funkce DOSu vykonává sám operační systém, přičemž kontroluje jejich správnost a oprávněnost ještě před jejich vykonáním. Na druhé straně Microsoft Windows 95 stále obsahují klasické jádro DOSu, které je využíváno i při práci přirozených 32–bitových programů a kompatibilita s DOSem je z tohoto hlediska zaručena.

Tento rozdíl má značný vliv na činnost AVAST32 v těchto operačních systémech. Jednotlivé rozdíly vám nyní přiblížíme.

Přítomnost jednotlivých programů

V Microsoft Windows NT nejsou v současné době implementovány některé programy, které můžete vidět ve verzi pracující v Microsoft Windows 95. Jedná se o náhrady klasických rezidentních programů, tzn. Rezidentní scanner a Systémový monitor.

Problémy s viry napadajícími systémové oblasti pevných disků

Pokud virus tohoto typu napadne systém pracující pod operačním systémem Microsoft Windows 95, existuje zde možnost nastartovat operační systém z diskety. Pokud ji nemáte vytvořenou (vytváří se při instalaci systému), můžete si ji kdykoli vytvořit pomocí položky „**Přidat/Ubrat programy**“ v „**Kontrolních panelech**“. Pomocí této diskety můžete odstranit virus ze systémových oblastí klasickým způsobem.

Tato možnost ale u Microsoft Windows NT neexistuje. Operační systém není možné startovat z diskety a pokud si vzpomenete na možnost formátovat disk tohoto systému jiným způsobem než jej formátuje klasický DOS, zjistíte, že odstranit virus tohoto typu může být opravdu obtížné. Velice obtížné může být již pouhé nastartování infikovaného systému.

Testování paměti

Otestování paměti přirozeného 32–bitového programu není tak snadné, jak se může na první pohled zdát. Program má totiž k dispozici samostatný adresový prostor o délce 2 GB (2048 MB). Naštěstí v Microsoft Windows 95 je ta část adresového prostoru, kde mohou přebývat „**dnešní**“ viry, mapována do adresového prostoru programu ve Microsoft Windows 95. To ovšem není pravda v Microsoft Windows NT, který nemusí být plně kompatibilní s DOSem.

Z těchto poznámek vyplývá, že operační paměť se testuje v systému Microsoft Windows 95 (pokud to uživatel požaduje a pokud je AVAST32 správně nainstalován). V operačním systému Microsoft Windows NT se paměť netestuje.

Tato stránka je úmyslně prázdná

Příloha C: Manuální změny nastavení

Manuální nastavení souboru antivirových programů AVAST32 je možné, i když jej můžeme doporučit pouze odborníkům na příslušný operační systém. V případě nesprávné změny konfiguračních dat produktu může dojít k jeho nesprávné funkci. Změna konfiguračních dat jiných programů nebo vlastního systému může vést k poškození interních dat, zhroucení operačního systému a tím také ke ztrátě dat umístěných na pevném disku.

Pokud vám není znám pojem „Registr", přeskočte tuto kapitolu. Hrozí vážné nebezpečí poškození samotného systému!!

Interní data programu jsou umístěna v tzv. „**Registru**". I zde mohou být data umístěna v různých oblastech ale AVAST32 používá následující:

```
HKEY_LOCAL_MACHINE\Software\ALWIL Software\AVAST32
HKEY_CURRENT_USER\Software\ALWIL Software\AVAST32
```

Zde můžete nalézt všechny konfigurační parametry produktu AVAST32. Jednotlivé klíče se mohou dále větvit až o několik stupňů a veškeré změny nesmí toto větvení poškodit.

Detailní popis jednotlivých zde umístěných hodnot není předmětem tohoto manuálu. Důrazně však varujeme před jakýmkoli mazáním položek a jakoukoli změnou numerických hodnot, které většinou obsahují důležité informace.

Jedinou výjimkou může být manuální smazání AVAST32 z vašeho počítače, kdy vám doporučujeme smazat všechny zde uvedené parametry včetně jejich klíčů.

Tato stránka je úmyslně prázdná

Příloha D: Manuální deinstalace

Manuální deinstalace produktu AVAST32 je možná, i když její provádění doporučujeme pouze odborníkům na příslušný operační systém. V případě nesprávné manuální deinstalace může dojít k takovému poškození interních dat systému, že může dojít k úplné ztrátě dat umístěných na pevném disku.

Manuální deinstalace spočívá ve dvou krocích:

1. Spuštění standardní deinstalace (viz příslušnou kapitolu),
2. Manuální smazání všech zbylých souborů, které zůstaly na disku po standardní deinstalaci. Jedná se zejména o soubory v instalačním adresáři a v adresáři Microsoft Windows. Zároveň můžete smazat celý instalační adresář.
3. Smazání všech položek v „**Registru**“ týkajících se AVAST32. Tyto informace jsou popsány v předchozí příloze. Lze rovněž použít (a je to doporučeno v tomto případě) program CLEAR.EXE, který se nachází na první instalační disketě. Jednoduchou nápovědu, týkající se tohoto programu, dostanete po jeho spustění s parametrem otazník. Tento program naprosto zničí jakékoli pozůstatky po AVAST32 v „**Registru**“ a je tím potenciálně nebezpečnou zbraní v rukou nepovolaných.

Pokud vám není znám pojem „Registr“, poslední krok neprovádějte. Hrozí vážné nebezpečí poškození samotného systému!!

Tato stránka je úmyslně prázdná

Příloha E: Charakteristika některých 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 spouštěn 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 programů.

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 Parameter 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. Program VGUARD tento virus odstranit neumí, protože 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 klávese 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 provede 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 programů 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 aktivování 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.

Další viry

Nové viry se objevují zcela pravidelně. Jejich popis můžete najít například v časopisu Screen, který pravidelně vydáváme, popř. v souboru READ.ME na distribuční disketě.

Příloha F: Otázky a odpovědi

Otázka: AVAST32 nepíše česky, co mám dělat?

Odpověď: AVAST32 v současné verzi nemanipuluje s fonty. To znamená, že autoři programu nechali výběr příslušného typu a velikosti fontu plně na systémových knihovnách. Program je navržen tak, aby psal česky při standardní instalaci systému. Pokud jste instaloval některé nové fonty nebo produkty, které instalují nové fonty, mohl jste si příslušný standardní font přepsat a pak s vámi AVAST32 nebude komunikovat česky.

Otázka: AVAST32 má divné barvy. Jak je mám změnit? Také zobrazovaný obrázek není pokaždé stejný.

Odpověď: Opět musíme konstatovat, že AVAST32 se žádným způsobem nesnaží manipulovat s barvami. Váš problém vyplývá ze způsobu práce systému s barvami. AVAST32 používá standardní systémové nastavení barev, takže jejich změnu musíte provést globálně pomocí prostředků operačního systému. Pokud jste zaregistroval, že Váš kolega má zobrazen jiný obrázek v oknech AVAST32, je to způsobeno nastavením barevné hloubky vašeho počítače. Na systémech s 16 a 256 barvami se zobrazuje zjednodušený obrázek. Na počítačích, které mají nastaveno více barev, zobrazuje se obrázek s 256 optimalizovanými barvami, který již vypadá velice realisticky. Důvody tohoto rozlišení jsou také ukryty ve způsobu práce operačního systému s barvami.

Otázka: AVAST32 nelze nainstalovat anebo je výsledek instalace nekorektní. Co mám dělat?

Odpověď: Důkladně si přečíst kapitolu o instalaci.

Tato stránka je úmyslně prázdná

Příloha G: Seznam instalovaných souborů

Instalace programu uloží většinu souborů potřebných pro práci AVAST32 do jednoho adresáře. Pouze několik z nich je uloženo do systémového adresáře Microsoft Windows. AVAST32 při své práci může vytvářet další soubory, kterých umístění není určeno a závisí na nastavení parametrů jednotlivých testů. Jde zejména o report soubory (RPT) a databázové soubory (AGW).

V této kapitole můžete najít abecední seznam souborů, které používá AVAST32. Je možné, že nové verze AVAST32 budou používat některé další soubory nebo naopak, některé ze zde uvedených souborů nebudou zapotřebí. O všech těchto změnách však budete podrobně informovaní.

V tabulce uvedené níže znamená AVAST32 instalační adresář, který si můžete zvolit v okamžiku instalace.

Soubor	*Umístění*	*Stručný popis*	*NT*	*Win95*
ADMIN.TXT	AV32	Popis administrátorské instalace	•	•
AGW.EXE	AV32	Program pro testování integrity dat	•	•
ARF.DLL	AV32	Knihovna pro restaurování zm. souborů	•	•
AVAST.EXE	AV32	Konzole testů (shell)	•	•
AV32.CNT	AV32	Pomocný soubor nápovědy	•	•
AV32.HLP	AV32	Vlastní texty nápovědy	•	•
AV32X.HLP	AV32	Texty nápovědy pro funkci "Co je to ?"	•	•
AVAST95.VXD	AV32	Systémová podpora přístupu k diskům		•
AVCOMMON.DLL	AV32	Knihovna společných funkcí	•	•
AVCOMPR.DLL	AV32	Knihovna pro kompresi databází	•	•
AVLANG.DLL	AV32	Knihovna jazykově závislých informací	•	•
DEISL1.ISU	AV32	Datový soubor pro řízení deinstalace	•	•
EDR.DLL	AV32	Knihovna pro dekompresi souborů	•	•
FGW.DLL	AV32	Výkonná část Systémového monitoru		•
FGW.EXE	AV32	Systémový monitor		•
FGW.VXD	AV32	Sys. podpora Systémového monitoru		•

FGW16.DLL	Win	Knihovna pro zprac. 16 bitových prog.		•
LGW.DEF	AV32	Prázdný soubor pro definici uživ. virů	•	•
LGW.EXE	AV32	Program pro hledání virů	•	•
LGW.VPS	AV32	Definiční soubor virů	•	•
LICENSE.TXT	AV32	Licenční ujednání ohledně AV32	•	•
MFC?0.DLL	Win	Knihovna MFC	•	•
MSVCRT?0.DLL	Win	Knihovna C++	•	•
RGW.DLL	AV32	Výkonná část Rezidentního scanneru		•
RGW.EXE	AV32	Residentní scanner		•
RGW16.DLL	Win	Knihovna pro zprac. 16 bitových prog.		•
RGW32.DLL	Win	Knihovna pro zprac. 32 bitových prog.		•
RGW95.VXD	AV32	Sys. podpora Rezidentního scanneru		•
README.TXT	AV32	Popis změn, proti manuálu	•	•
VIRFOUND.WAV	AV32	Zvuková signalizace nalezení viru	•	•
VPS.DLL	AV32	Knihovna pro antivirové testování	•	•
UNINST.EXE	AV32	Program pro řízení deinstalace	•	•