Antivirový systém AVG 4.0 pro WINDOWS - Index

Informace o programu AVGW

Funkce, která zobrazí základní informace o verzi AVGW, kterou používáte, vèetnì pøípadného oznaèení subverze, datum uvolnìní této verze k distribuci a informaci o jazykové verzi.

Dùležitým údajem je také ***sériové èíslo*** uživatele a oznaèení ***majitele licence***. Tyto informace se do programu AVGW zapisují bìhem instalace a pozdìji je již není možno zmìnit.

Pokud je Vaše instalace oznaèena jako ***neregistrovaná***, nebylo bìhem instalace zadáno správné sériové èíslo - program AVGW je funkèní, ale nebude možné v budoucnu provádìt aktualizaèním programem náhradu novìjší podoby programu AVGW.EXE.

V pøípadì, že máte jakékoliv dotazy týkající se sériového èísla Vaší instalace, mùžete se obrátit na výrobce systému

Velmi dùležité jsou informace o souborech AVI a AVF, které vaše instalace používá. Uvìdomte si prosím, že tato data/informace ovlivòují rozsah a schopnosti testù provádìných programem AVGW - tj. dva programy stejné verze, ale s rùznými datovými soubory, se budou lišit v rozsahu kontroly.

Pokud uživatel používá vlastní soubory pro uživatelskou validaci, pøípadnì vlastní popis externích virù, jsou v okénku zobrazeny pøíslušné informace.

Informace o virech

Zobrazí základní údaje o virech, detekovaných vaší instalací systému AVGW. Množství detekovaných virù je závislé na verzi vaší instalace a na souborech AVI/AVF.

Upozoròujeme uživatele, že informace uvedené v tomto pøehledu jsou maximálnì **zestruènìny** - tj. obsahují pouze jméno viru a typ napadení (soubor/systémová oblast).

Pokud požadujete podrobnìjší informace o konkrétním typu viru, mùžete je získat funkcí "***Podrobnìjší informace***". Systém AVG ve verzi 4.0 obsahuje podrobný popis nejrozšíøenìjších virù u nás - tj. není k dispozici ke všem virùm obsaženým ve virové databance. Seznam virù, pro které bude podrobnìjší popis k dispozici bude rozšiøován.

Informace o prostøedí

Zobrazí základní informace o prostøedí, ve kterém program AVGW pracuje - typ a verzi operaèního systému, ovladaèe pamìti, režim procesoru, velikost základní a XMS pamìti apod.

O pøíznacích heuristické analýzy

Tato volba zobrazí seznam pøíznakù, tak jak je oznaèuje heuristická analýza spolu s jejich podrobnìjším vysvìtlením. Tento seznam je také k dispozici v uživatelské dokumentaci programu AVG.

Antivirový test

Antivirový test je založen na principu vyhledávání "***virových identifikátorù***". Pro komplexnost je antivirový test v programu AVGW doplnìn také o detekci algoritmù a rychlou heuristickou analýzu.

O tom, zda je používána rychlá heuristická analýza, informuje uživatele ikona - "svìtélko". Pokud má zelenou barvu, je provádìna rychlá heuristická analýza, pokud je šedivá, není analýza provádìna.

Pøed vlastním testem musí uživatel vybrat požadované zaøízení k testu Vlastní antivirový test probíhá v tìchto krocích :

Test systémových oblastí

Nejprve jsou otestovány systémové oblasti zaøízení (program AVGW sám urèuje typ testovaného zaøízení a jaké systémové oblasti tedy bude testovat).

Pro pevné disky je to ***Partition table*** a ***Boot sektor***.
Pro diskety je to pouze ***Boot sektor***.
U sí□ových zaøízení nebo u nìkterých pseudo-zaøízení je test systémové oblasti vynechán.

V pøípadì, že systémové oblasti jsou v poøádku, vypíše program zprávu na obrazovku.

V pøípadì, že v testované systémové oblasti byl zjištìn virus, je vypsáno hlášení o nalezení viru - Nalezen virus.

Okamžitý výpis hlášení o nalezených virech a okamžitou volbu akce je možné zmìnit na odlišný režim, kdy jsou hlášení vypisována do spoleèného okna a uživatel volí akce podokonèení celého testu - Nastavení Antivirového testu.

Test souborù

Po provedení testu systémových oblastí pokraèuje antivirový test kontrolou souborù na zaøízení. Bìhem testu jsou vypisovány informace o prùbìhu testu a informace o závažných skuteènostech, které byly zjištìny.

V programu AVGW.EXE jsou postupnì vypisovány informace o právì testovaném adresáøi a právì testovaném souboru. Pokud test zjistí závažnìjší informace. vypíše pøíslušné hlášení do okna ve spodní èásti. Do tohoto okna jsou vypisovány nejen informace o souborech napadených virem, ale také informace o nestandardních souborech - napø. internì komprimovaných. Hlášení o tìchto nestandardních souborech lze potlaèit v Nastavení antivirového testu - Hlásit nestandardní soubory.

V pøípadì, že byl detekován virus, je oznaèen napadený soubor, typ a jméno viru a uživateli jsou nabízeny možnosti pro øešení této situace - Nalezen virus

Režim výpisu hlášení

Okamžitý výpis hlášení o nalezených virech a okamžitou volbu akce je možné zmìnit na odlišný režim, kdy jsou hlášení vypisována do spoleèného okna a uživatel volí akce až po dokonèení celého test. Tento režim je možné nastavit v Nastavení Antivirového testu - Test bez hlášení. Po provedení testu celého zaøízení se vždy vypíše souhrnná informace o otestovaném zaøízení - poèet testovaných souborù, poèet nalezených virù a

vyléèených souborù apod.

Heuristická analýza

Princip heuristické analýzy

Heuristická analýza nevyhledává na rozdíl napø. od Antivirového testu v testovaných objektech nic konkrétního. Naopak - testuje kód testovaného souboru - tj. prochází jednotlivé instrukce a analyzuje jejich praktický význam. Funkce dokáže zachytit nekorektní èinnosti testovaného programu. Heuristická analýza tedy nevyhledává konkrétní viry na základì virových identifikátorù, ale vyhledává viry na základì nekorektních èinností, které virus provádí. Její nejvìtší výhodou je tedy schopnost detekovat virus nezávisle na tom, zda je známý èi nikoliv.

Zjednodušená podoba heuristické analýzy, oznaèovaná jako ***Rychlá heuristická analýza*** je také volitelnou souèástí Antivirového testu.

Pøed vlastním testem musí uživatel vybrat zaøízení, které požaduje otestovat. Vlastní heuristická analýza se provádí v tìchto krocích :

Test systémových oblastí

V rámci heuristické analýzy jsou nejprve otestovány systémové oblasti zaøízení (program AVGW sám urèuje typ testovaného zaøízení a jaké systémové oblasti tedy bude testovat).

Pro pevné disky je to **Partition table** a **Boot sektor**.
Pro diskety je to pouze Boot sektor.
U sí□ových zaøízení je test systémové oblasti vynechán.

V pøípadì, že jsou systémové oblasti v poøádku, vypíše program zprávu na obrazovku. V opaèném pøípadì je vypsáno hlášení o nalezení viru. Je oznaèena napadená oblast a nalezený virus a uživateli jsou nabízeny volby pro odstranìní viru - Nalezen virus.

Test souborù

Po provedení testu systémových oblastí je zahájen test souborù. Informace o prùbìhu testu jsou vypisovány do okna - jméno testovaného adresáøe a jméno právì testovaného souboru. V pøípadì, že heuristická analýza zjistila v testovaném souboru nekorektní instrukce, jsou vypisovány také zjištìné pøíznaky.

V pøípadì, že byl detekován virus, je oznaèen napadený soubor a je-li znám, také typ a jméno viru a uživateli jsou nabízeny volby pro odstranìní viru - Nalezen virus.

Program AVGW umožòuje provést heuristickou analýzu ve dvou, z pohledu uživatele rozdílných provedeních. V prvním pøípadì se test zastaví ihned v okamžiku, kdy dojde k nalezení napadeného souboru a okamžitì se oèekává rozhodnutí uživatele. Druhá možnost pouze zapíše nalezený napadený soubor do seznamu a vlastní akci je možno øešit až poté, co je otestováno celé zaøízení nebo adresáø. Tuto volbu lze nastavit v Nastavení heuristické analýzy.

Závìreèné hlášení

Na konci celého testu každého zaøízení se vždy vypíše souhrnná informace o testovaném zaøízení - poèet testovaných souborù, poèet nalezených virù a vyléèených souborù.

Nalezen virus

V pøípadì, že Antivirový test nebo Heuristická analýza zjistily bìhem provádìného testu virus, oznámí tuto skuteènost uživateli a nabízí volbu další akce.

Další postup závisí na tom, zda virus byl nalezen v systémové oblasti nebo v souboru.

Virus v systémové oblasti

Program AVGW nabízí tyto volby:

Pokraèovat
Test pokraèuje v testování další systémové oblasti, pøípadnì zahájí test souborù. Vlastní virus je ponechán v napadené oblasti.

Informace
Podá podrobnìjší informace o nalezeném viru - informace, které pøípadnì analýza zjistila.

Odstranit virus
Tato funkce vede k odstranìní viru ze systémové oblasti. Program AVGW používá k odstranìní viru ze systémové oblasti dvì rozdílné techniky:

Léèení viru
Léèení viru spoèívá v odstranìní viru z napadené systémové oblasti. Pro odstranìní viru ze systémové oblasti používá program AVGW univerzální techniku, která vychází ze skuteènosti, že naprostá vìtšina virù tohoto typu používá stejný princip šíøení.

Rekonstrukce oblasti
U pevných diskù tato funkce spoèívá v nahrazení napadené systémové oblasti døíve vytvoøenou záložní kopií. Tuto záložní kopii lze vytvoøit pomocí funkce funkce Zálohování systémových oblastí. U disket spoèívá princip této funkce v nahrazení napadeného Boot sektoru obecnì platnou strukturou této oblasti.

Vzhledem ke skuteènosti, že systémové oblasti mají pro chod poèítaèe klíèový význam, nabízí program pøed vlastním provedením funkce Léèení nebo Rekonstrukce, možnost uložení tzv. "***Zpìtných informací na disketu***".

Virus v souboru

V pøípadì, že program AVGW zjistil virus v souboru, nabízí tyto volby :

Pokraèuj
Provádìný test bude pokraèovat do nalezení dalšího viru nebo do konce testovaného zaøízení.

Nonstop
Provádìný test bude pokraèovat - jakýkoliv další nalezený virus bude pouze vypsán do seznamu nalezených virù - nebude se znovu nabízet dialog pro volbu akce.

Informace
Zobrazí podrobnìjší informace, které test zjistil o testovaném souboru - respektive o zjištìném viru.

Léèit virus
Tato funkce, pøi svém úspìšném provedení, vede k odstranìní viru z napadeného souboru a uvedení tohoto souboru do pùvodního stavu. Program AVGW ve verzi 4.0 rozlišuje dvì techniky léèení:

Heuristické léèení
Heuristické léèení je založeno na analýze napadeného souboru a analýze konkrétního viru - jedná se tedy o obecný postup, kdy nezáleží na tom, zda je virus známý nebo ne. O možnosti použití heuristické techniky léèení èasto rozhoduje pøítomnost pøíznaku B - pokud je nalezen tento pøíznak bude heuristické léèení možné. Pro zvýšení pravdìpodobnosti úspìchu heuristického léèení lze také zvolit v menu Nastavení heuristické analýzy - zvláštní mód pro léèení.

Obnova souboru
Obnova souboru využívá informací uložených ve srovnávací databázi k rekonstrukci napadeného souboru do pùvodní podoby. Pøi léèení souborù doporuèujeme využívat možnosti ***zálohování napadených souborù*** - dostupné v menu Obecné nastavení testù, kdy program AVGW vytvoøí pøed vlastním léèením nejprve kopii souboru pro pøípad, kdy by v procesu léèení došlo k jeho znièení.

Smazat napadený soubor
Provede smazání napadeného souboru tak, aby již nebylo možné jej obnovit.

Pøejmenovat soubor
Provede pøejmenování napadeného souboru. Vhodné pro situace, kdy chcete napadené soubory na zaøízení zachovat beze zmìn, ale také bez nebezpeèí, že dojde k jejich nechtìnému spuštìní.

Léèit vše
Léèit vše je totožné s funkcí léèit, s tím rozdílem, že program automaticky otestuje zbytek testovaného zaøízení a pokusí se léèit všechny napadené soubory, které nalezne. Tato funkce je optimální pro léèení zaøízení s mnoha napadenými soubory - po ukonèení testu je však nezbytné zaøízení znovu pøetestovat, aby uživatel zjistil úspìšnost léèení na konkrétních souborech.

Konec
Ukonèí pøedèasnì provádìný test.

Srovnávací test

Princip tohoto typu testu je založen na logickém pøedpokladu, že každá virová nákaza po sobì zanechá na napadeném zaøízení zmìny - u napadených souborù se vìtšinou zmìní jejich velikost a obsah (nìkdy také datum a èas), u napadených systémových oblastí pak pouze jejich obsah. Tohoto pøedpokladu využívá funkce, oznaèovaná jako srovnávací test.

Funkce si vytváøí a udržuje vlastní datový soubor, oznaèovaný jako **srovnávací databáze**, s jehož pomocí dokáže zjistit k jakým zmìnám na testovaném zaøízení došlo.

Pøed vlastním testem musí uživatel vybrat zaøízení, které požaduje otestovat.

Vlastní prùbìh srovnávacího testu se liší v závislosti na tom, zda na testovaném zaøízení již existuje srovnávací databáze èi nikoliv.

Založení databáze

Pokud na testovaném zaøízení dosud neexistovala srovnávací databáze, je o této skuteènosti uživatel informován a mùže požádat o její založení. Po potvrzení založí program databázi novou, zkontroluje zadané zaøízení/adresáø a do novì vzniklé databáze automaticky uloží potøebné informace o všech souborech na zaøízení/adresáøi, jejichž rozšíøení odpovídá nastaveným typùm.

Test proti existující databázi

Pokud na testovaném zaøízení srovnávací databáze již existuje, následuje skuteèný srovnávací test - porovnání údajù z databáze proti reálnému stavu. Prùbìh srovnávacího testu je maximálnì automatizován. Uživateli jsou k dispozici informace o právì testovaném adresáøi a souboru, pøípadnì struèné informace o detekovaných zmìnách. Po otestování celého zaøízení jsou všechny zjištìné zmìny znovu zobrazeny spolu s detailním popisem. Srovnávací test programu AVGW rozeznává tyto typy zmìn:

Zmìna systémové oblasti

Pøedstavuje závažnou zmìnu. Pokud jste na svùj poèítaè od poslední aktualizace srovnávací databáze neinstalovali napø. nový operaèní systém, nebo nìkterý systémový software, pøípadnì neinstalovali nový hardware (nový pevný disk, apod.) mùže být zmìna systémové oblasti závažným pøíznakem virové infiltrace.

Zmìna systémové oblasti (Boot sektor) u pseudo-zaøízení (napø. diskù obsluhovaných komprimaèními programy - Stacker, DoubleSpace ...) mùže mít zcela korektní pùvod.

Zmìna testovaného souboru

Srovnávací test zjistil nesouhlas reálných údajù o souboru proti záznamu z databáze. V pøípadì, že oznaèený soubor nebyl v poslední dobì korektnì zmìnìn - napø. nová verze programu, apod. - mùže tato zmìna oznaèovat virovou infiltraci. Dùležitou informací také je, kterého kontrolovaného parametru se zjištìná zmìna týká. Zmìna atributù souboru nebo èasu vytvoøení není samozøejmì tak závažná, jako zmìna obsahu souboru a/nebo jeho délky.

Soubor byl smazán

Soubor, mající svùj záznam v databázi nebyl na zaøízení nalezen. Byl pravdìpodobnì smazán, pøejmenován nebo pøesunut do jiného adresáøe.

Soubor je nový
Soubor na zaøízení existuje, ale v databázi nemá žádný záznam.

Vyhodnocení zmìn

Poté co Srovnávací test dokonèil test zaøízení/adresáøe, pøedloží zjištìné zmìny uživateli . Na uživateli nyní je, aby ty zmìny, které považuje za korektní, oznaèil a tím je uložil do srovnávací databáze jako nový standard pro pøíští testy - Vyhodnocení srovnávacího testu.

Vyhodnocení srovnávacího testu

Pro ukonèení srovnávacího testu, pøedloží program AVGW uživatel seznam nalezených zmìn. Srovnávací test rozeznává tyto typy zmìn :

Zmìnìna systémová oblast
Obsah systémové oblasti je jiný, než jaký je uložen ve srovnávací databázi. Pokud nedošlo ke zmìnì konfigurace poèítaèe, mùže tato zmìna znamenat virovou nákazu.

Výjimkou jsou zaøízení obsluhovaná programy pro komprimaci dat v reálném èase (Stacker apod.), kdy obsah Boot sektoru je pøi každém testu jiný - náhodný.

Zmìnìn soubor
Soubor na zaøízení je jiný, než jeho obraz ve srovnávací databázi. O typu zmìny informuje uživatel text, pøípadnì lze využít volbu Informace.

Nový soubor
Na zaøízení byl nalezen soubor, který nemá svùj obraz ve srovnávací databází - je tedy nový.

Smazaný soubor
Ve srovnávací databázi jsou uloženy informace o souboru, který však nebyl na testovaném zaøízení nalezen - soubor byl tedy smazán.

Oznaèení korektních zmìn

Na uživateli nyní je, aby ty zmìny, které považuje za korektní, oznaèil a tím je uložil do srovnávací databáze jako *nový standard* pro pøíští testy - Vyhodnocení srovnávacího testu. Výbìr a oznaèení zjištìných zmìn se provádí následujícím zpùsobem:

Zvolenou zmìnu je možné oznaèit prostøednictvím **myši**. V pøípadì, že požadujete odznaèení, zopakujte stisk myši na již oznaèeném souboru.

Pro **spoleèné oznaèení** více zmìn stejného typu lze s výhodou využít voleb

- Oznaè vše
- Odznaè vše
- Oznaè všechny zmìny
- Odznaè všechny zmìny
- Oznaè všechny smazané
- Odznaè všechny smazané
- Oznaè všechny nové
- Odznaè všechny nové

Pokud nebyl zjištìn nìkterý typ zmìn, nejsou k dispozici ani pøíslušné volby.

Informace - podá podrobnìjší informace o zjištìné zmìnì.

Ukonèit - ukonèí vyhodnocení Srovnávacího testu, aniž by byl aktualizován obsah srovnávací databáze.

Uložit do databáze - ukonèí Srovnávací test a aktualizuje obsah srovnávací databáze o všechny zmìny, které uživatel oznaèil jako korektní.

Závìreèné hlášení

Poslední informací, kterou Srovnávací test zobrazí, je informaèní okno obsahující výsledek testu.

Automatická aktualizace

Pro zjednodušení vyhodnocení srovnávacího testu lze využít nastavení, kdy se nové nebo smazané soubory do srovnávací databáze *ukládají automaticky* - uživateli jsou nabízeny pouze zmìnìné soubory - Nastavení srovnávacího testu.

Výbìr zaøízení k testu

Pøed vlastním testem - antivirovým testem, heuristickou analýzou a srovnávacím testem musí uživatel vždy vybrat to zaøízení, pøípadnì adresáø na tomto zaøízení, které požaduje otestovat.

Na obrazovce je zobrazen dialog, ve kterém je vypsán seznam existujících zaøízení vašeho poèítaèe. Ke každému zaøízení je také vypisován jeho **typ** - lokální, sí□ové apod. a **informace**, zda na zaøízení existuje srovnávací databáze (existence srovnávací databáze se netestuje na disketách a sí□ových zaøízeních).

Pro výbìr zaøízení se zobrazí, ve kterém uživatel mùže vybrat k testu jedno nebo libovolný poèet zaøízení. Pøi výbìru lze také zadat konkrétní adresáø, který má být testován (bude otestován vèetnì podadresáøù). Výbìr zaøízení, které požadujete testovat je následující.

Test jednoho zaøízení
Oznaète zaøízení, které chcete testovat a zvolte volbu **Spustit test**.

Test adresáøe
Pokud chcete testovat vybraný **adresáø** na zaøízení, oznaète pøíslušné zaøízení a zvolte volbu **Výbìr adresáøe**. V nabízeném adresáøovém stromì pak bìžným zpùsobem vyberte adresáø, který požadujete otestovat. Výbìr zvoleného adresáøe provedete volbou **Vybrat**. Vrátíte se zpìt do výbìru zaøízení - u zvoleného zaøízení je však nyní i oznaèení vybraného adresáøe. Pro jeho otestování zvolte volbu **Spustit test**.

Spoleèný test
Pokud požadujete otestování více zaøízení/adresáøù spoleènì, použijete volbu **Pøidat**. Zvolte požadované zaøízení/adresáø zpùsobem uvedeným výše, místo volby Spustit test však zvolte volbu **Pøidat**. Vybrané zaøízení/adresáø se zapíší do seznamu ve spodní èástí dialogu. Nyní mùžete vybírat další testované zaøízení/adresáø. V okamžiku, kdy seznam obsahuje všechny požadované zaøízení/adresáøe k testu, zvolte volbu **Spustit test** - postupnì se otestují všechny požadované oblasti.

Vymazání seznamu
Pokud požadujete smazání seznamu zaøízení/adresáøù zvolte volbu **Vyprázdnit** - seznam se vymaže.

Dvojstisk myši
Pro zjednodušení výbìru zaøízení k testu lze také využít rychlé opakované stisknutí levého tlaèítka myší - tzv. **dvojstisk**. Sami si mùžete zvolit, co tento dvojstisk bude znamenat - v Obecném nastavení testù. Standardní nastavení odpovídá volbì **Spustit test**. Další možné nastavení jsou **Výbìr testovaného adresáøe**, **Pøidat do seznamu** nebo nastavení, kdy dvojstisk nemá **žádný význam**.

Zopakujme si, jaký význam mají jednotlivé volby v dialogu výbìru testovaného zaøízení/adresáøe.

Zpìt - ukonèí výbìr zaøízení/adresáøe.

Pøidat - pøidá nastavené zaøízení/adresáø do seznamu ve spodní èásti dialogu. Význam volby Pøidat mùže mít také dvojstisk myši, pokud je tato volba nastavena v Obecném nastavení testù.

Vyprázdnit - vymaže obsah seznamu ve spodní èásti dialogu.

Nastavení - vyvolá dialog s možností zmìny nìkterých parametrù testu.

Spustit test - aktivuje test na všechna zaøízení/adresáøe, které jsou uvedeny ve spodním seznamu, pøípadnì že tento seznam je prázdný, pak na zaøízení/adresáø, který je právì nastaven. Význam volby Spustit test mùže mít také dvojstisk myši, pokud je tato volba nastavena v Menu nastavení - Obecném nastavení testù.

Výbìr adresáøe - aktivuje funkci pro výbìr jednoho adresáøe na testovaném zaøízení. Význam volby Výbìr adresáøe mùže mít také dvojstisk myši, pokud je tato volba nastavena v Obecném nastavení testù.

Seznam testovaných zaøízení/adresáøù - vícenásobný seznam zaøízení/adresáøù, které byly do seznamu pøidány volbou Pøidat. Obsah tohoto seznamu je také možné editovat ruènì - jednotlivé volby se oddìlují støedníkem.

Test pamìti RAM

Funkce otestuje pamì poèítaèe na pøítomnost viru. Tato funkce je vyvolána automaticky ihned po spuštìní programu AVGW, pokud toto automatické spouštìní není potlaèeno v Obecném nastavení testù.

Pokud chcete v programu AVGW.EXE používat test operaèní pamìti RAM je nezbytné, aby byl **øádnì instalován program AVGSYSW.EXE**. Bez pøítomnosti tohoto programu není možné test operaèní pamìti provést

Pokud byl bìhem testu operaèní pamìti nalezen virus, oznámí program tuto skuteènost uživateli a nabízí možnosti *Pokraèovat* nebo *Restartovat poèítaè*.

Nastavení Antivirového testu

Umožní zmìnit parametry, které mají vztah k funkci Antivirový test. Mìnit lze tato nastavení:

Typy rozšíøení pro antivirový test

Umožòuje zvolit mezi standardní množinou typù rozšíøení souborù, které mají být testem kontrolovány, nebo nastavit vlastní typy.

Ménì zkušené uživatele upozoròujeme, že z pohledu virù nejsou dùležité soubory typu *.TXT, *.DBF, ale pouze soubory programové - EXE, COM, OVL apod. Naopak, pokud budete požadovat testování napøíklad textových souborù, mùžete to vést k mylným hlášením.

Použít rychlou analýzu

Urèuje, zda se bìhem antivirového testu bude provádìt také tzv. rychlá heuristická analýza.

Hlásit nestandardní soubory

Urèuje, zda se mají hlásit soubory typu PKLITE, DIET, LZEXE, imunizované programy apod. Tyto programy mají z pohledu operaèního systému nestandardní strukturu a program AVGW na nì uživatele upozoròuje. Vypnutím hlášení nestandardních souborù lze oznaèování tìchto souborù potlaèit.

Nastavení èasové výzvy

Umožòuje definovat èasovou periodu - poèet dní. Pokud od posledního spuštìní antivirového testu uplyne více jak nastavený poèet dní, upozorní vás program AVGW pøi svém spuštìní na vhodnost spuštìní tohoto testu.

Test bez hlášení

Ve standardní podobì vypisuje antivirový test hlášení o napadených nebo podezøelých souborech **okamžitì** pøi jejich zjištìní. Test se tedy zastaví a pokraèuje až po volbì uživatele.

V pøípadì, že nastavíte volbu Test bez hlášení, bude antivirový test o nalezených, napadených nebo podezøelých souborech pouze vypisovat hlášení a výbìr vlastní akce bude možné provádìt až **po skonèení celého testu**.

Nastavení heuristické analýzy

Nastavení pro Heuristickou analýzu umožòuje nastavit tyto parametry:

Typy rozšíøení pro Heuristickou analýzu
Umožòuje zvolit standardní množinou typù rozšíøení nebo nastavit vlastní typy rozšíøení.

Ménì zkušené uživatele upozoròujeme: Heuristická analýza by nemìla testovat jiné soubory než programové - vìtšinou tedy typ EXE, COM. Pokud budete heuristickou analýzou testovat jiné typy souborù - napø. datové, bude analýza produkovat nesmyslná hlášení s možností mylných poplachù.

Hlásit nestandardní soubory
Urèuje, zda se mají hlásit soubory typu PKLITE, DIET, LZEXE, imunizované programy apod. Tyto programy mají z pohledu operaèního systému nestandardní strukturu a program AVGW na nì uživatele upozoròuje. Vypnutím hlášení nestandardních souborù lze oznaèování tìchto souborù potlaèit.

Exportovat podezøelé soubory
Urèuje, zda má heuristická analýza pøi nalezení souboru, podezøelého z výskytu neznámého viru, vytváøet soubor _GRISOFT.VIR se vzorkem podezøelého souboru.

Nastavení èasové výzvy
Umožòuje definovat èasovou periodu - poèet dní. Pokud od posledního spuštìní Heuristické analýzy uplyne více jak nastavený poèet dní, upozorní Vás program AVGW pøi svém spuštìní na vhodnost provedení tohoto testu.

Nastavení pro pokroèilé

V souvislosti s možností nastavení nìkterých parametrù heuristické analýzy (oznaèovaných zde jako parametry pro pokroèilé), uveïme toto dùležité upozornìní:

Zmìna nastavení heuristické analýzy
Heuristická analýza ve svém standardním nastavení je optimálnì vyladìna s ohledem na její schopnost detekovat složité viry a souèasnì s ohledem na minimalizaci mylných hlášení. Jakýkoliv zásah do tìchto parametrù mùže vést k destabilizaci heuristické analýzy.

Maximální èasový limit
Omezuje dobu, po kterou mùže heuristická analýza testovat jeden soubor. Standardní nastavení je 10 vteøin. Je nutné si uvìdomit, že v naprosté vìtšinì pøípadù se tento limit nevyužívá - tj. analýza ukonèí test døíve.

Hloubka zábìru
Maximální poèet instrukcí
Tyto dva parametry ovlivòují poèet instrukcí, které analýza v testovaném souboru otestuje (emuluje jejich provedení). Parametr Maximální poèet instrukcí udává skuteèný poèet instrukcí, po jejichž provedení se analýza ukonèí. Parametr Hloubka zábìru oznaèuje, kolik instrukcí do souboru má analýza proniknout.

Analyzovat nestandardní soubory
Soubory s nestandardní strukturou - soubory zpracované pomocí programù typu PKLITE, DIET, LZEXE apod. pøedstavují pro heuristickou analýzu ve vìtšinì pøípadù znaèné zdržení. Pøestože heuristická analýza pozná tyto soubory, provádí jejich analýzu -

vìtšinou zbyteènì.

Citlivá detekce cyklù
Analýza dokáže detekovat pøípadný výskyt cyklù v programu a tyto pak prochází ve zrychleném režimu. Vysokou citlivostí lze docílit detekce i nejsložitìjších a fragmentovaných virù. Nízká citlivost zvýší rychlost testu za cenu snížení potenciální spolehlivosti pøi detekci složitého polymorfu.

Krokovat alternativní adresy
Jedná se o dodateèné krokování tìch partií programu, ke kterým se analýza nedopracovala pøi základním testu. Jedná se o èásti kódu, ke kterým vedou podmínìné odskoky v programu. Použití této volby umožní podstatnì úplnìjší informace o pøípadném viru v souboru. Vzhledem k nárùstu velikosti testovaných oblastí nelze vylouèit zvýšení poètu mylných hlášení.

Nastavení pro léèení virù
Nastavuje zvláštní charakter heuristické analýzy, který mùže být užiteèný pro léèení nìkterých velmi složitých polymorfních virù. Nastavením parametru Nastavení pro léèení virù se heuristické analýze umožní delší postup do testovaného kódu a zvýší se pravdìpodobnost, že virus bude možno odstranit funkcí heuristické léèení. Heuristická analýza v tomto módu pracuje na èásteènì odlišném principu - automaticky doplòuje nìkterá systémová volání apod.

Tento mód je skuteènì alternativní k bìžnému bìhu heuristické analýzy. Nelze tedy nahradit pouhým zvìtšením poètu testovaných instrukcí nastavením parametrù Poèet instrukcí a Hloubka zábìru.

Emulovat frontu instrukcí
Snaha zrychlit provádìní instrukcí vedla firmu Intel k vytvoøení tzv. fronty instrukcí. Mikroprocesor si do ní z pamìti "pøednaèítá" instrukce, které pravdìpodobnì budou provádìny po dokonèení právì zpracovávané instrukce. Pokud program zmìní instrukci, která je již naètena ve frontì, procesor se o tom nedozví a zpracuje pùvodní instrukci. Manipulace s instrukcemi, které už jsou ve frontì, patøí k relativnì bìžným technikám používaným viry (a nejen jimi) k ochranì programu pøed trasováním a analýzou. Instrukèní fronta neexistovala na procesorech 8086 a Pentium ji sice má, ale zásah do ní rozpozná a v takovém pøípadì její obsah "zahodí" a naète ji znovu.

AVGW implicitnì nastavuje tento parametr na hodnotu, která odpovídá procesoru na kterém bìží. Zapíná tedy emulaci na procesorech 80286, 80386 a 80486. Pøi bìhu na procesorech 8086 a Pentium je emulace vypnuta.

Nastavení srovnávacího testu

Umožní nastavit ty parametry programu, které ovlivòují chování Srovnávacího testu.

Typy rozšíøení pro Srovnávací test

Umožòuje zvolit standardní množinu typù rozšíøení nebo nastavit vlastní typy rozšíøení. Je možné nastavit libovolné typy rozšíøení, je nutné si však uvìdomit, že pokud nastavíte napø. *.*, budete zahlceni množstvím zmìn v souborech typu TXT, DBF apod., tedy v souborech, které nejsou z virového pohledu vùbec dùležité.

Nastavení èasové výzvy

Umožòuje definovat èasovou periodu - poèet dní. Pokud od posledního spuštìní Srovnávacího testu uplyne více jak nastavený poèet dní, upozorní Vás program AVGW pøi svém spuštìní na vhodnost spuštìní srovnávacího testu.

Jméno srovnávací databáze

Umožòuje nastavit jméno srovnávací databáze - tedy souboru, do které ukládá srovnávací test údaje o testovaném zaøízení. Standardní jméno této srovnávací databáze je AVG40.GRS.

Automaticky aktualizovat smazané soubory
Automaticky aktualizovat nové soubory

Srovnávací test kromì zmìnìných souborù zjišuje a oznamuje uživateli také soubory nové (nemají dosud svùj obraz ve srovnávací databázi) a smazané (existuje o nich záznam v databázi, ale na zaøízení již neexistuji). Tyto zmìny nejsou z virového pohledu vìtšinou podstatné a uživatel si proto mùže nastavit jejich automatickou aktualizaci - tj. nové nebo smazané soubory se budou automaticky ukládat do srovnávací databáze bez toho, že by se nabízeli k potvrzení uživateli.

Nastavení obecných parametrù testù

Toto nastavení je v podstatì spoleèné pro všechny výše uvedené typy testù.

Test horní pamìti RAM

Umožòuje definovat, zda Test operaèní pamìti RAM bude testovat také pamì v rozsahu 640KB - 1MB.

Vytváøet záložní kopie

Umožòuje nastavit program AVG tak, aby pøed každým pokusem o léèení souboru napadeného virem nejprve vytvoøil záložní kopii napadeného souboru. Tato kopie mùže být velmi užiteèná v pøípadì, kdy proces léèení byl neúspìšný a došlo k nevratnému poškození napadeného souboru - uživatel má k dispozici pùvodní funkèní kopii zavirovaného souboru. Pøi vytváøení záložní kopie se používá zmìna rozšíøení souboru - napøíklad soubor COMMAND.COM bude pøejmenován na COMMAND.C##.

Test pamìti RAM po spuštìní

Definuje, zda se po spuštìní programu AVGW má automaticky spustit Test operaèní pamìti RAM.

Dvojstisk myši

Definuje, jaký význam bude mít dvojstisk levého tlaèítka myši bìhem výbìru zaøízení pøed jednotlivými testy. Je možné nastavit tyto volby:

Spustit test
Dvojstisk myši spustí vlastní test - Antivirový, Srovnávací nebo heuristickou analýzu, podle toho, o jaký typ testu jde.

Výbìr adresáøe
Dvojstisk myši vyvolá funkci na výbìr testovaného adresáøe.

Pøidat do seznamu
Do seznamu testovaných oblastí pøidá právì zvolené zaøízení/adresáø.

Nepoužito
Dvojstisk myši nebude mít žádný význam.

Seznam testovaných oblastí

Urèuje, zda se seznam testovaných oblastí (tento seznam lze vytvoøit volbou Pøidej) bude pøed každým testem mazat, nebo zda se zachová poslednì urèený seznam testovaných oblastí.

Nastavení parametrù prostøedí

Umožòuje nastavit parametry, ovlivòující vnìjší chování programu.

Zvukový výstup

Nastavení zvukového výstupu umožòuje definovat, zda program AVGW bude pro detekci významnìjších událostí používat zvukový signál.

Výpis protokolu

Výpis protokolu (oznaèovaný jako report soubor nebo log) - nastavuje textový soubor, do nìhož bude program AVGW zapisovat doplòující informace o provádìných testech. Obsah tohoto souboru poskytuje detailní pøehled o provádìných testech.

Zaznamenávat konfiguraci

Zaznamenávat konfiguraci - nastavuje automatické ukládání konfigurace tak, jak byla pøípadnì nastavena uživatele bìhem použití programu AVGW do konfiguraèního souboru pøi ukonèení programu. Program AVGW.EXE vytváøí konfiguraèní soubor se jménem AVGW.CFG.

Definice uživatelského hesla

Program AVGW uvolòuje nìkteré, privilegované funkce , až po zadání platného pøístupového hesla. Standardní, obecnì platné heslo, není možné zmìnit a je uloženo v souboru HESLO na instalaèní disketì.

Kromì tohoto hesla je možné definovat ***volitelné uživatelské heslo*** a to používat pøi bìžné práci. Zadání nového uživatelského hesla je možné pouze tehdy, pokud bylo v daném sezení zadáno platné heslo.

Volba typu písma - výbìr fontu

Umožòuje uživateli nastavit si vlastní typ písma, které je používáno pro výpis pomocných informací na spodním øádku okna programu AVGW. Aktivace této volby volá dialog pro výbìr nového typu písma. Pokud zvolíte nový typ písma, je nutné uložit novou konfiguraci na disk a restartovat program AVGW.EXE.

Sí□ová komunikace

V pøípadì, že pracujete v sí□ovém prostøedí standardu Novell Netware, je možné využít funkci *sí□ové komunikace*. Pokud je tato funkce zapnuta a je definován uživatel/skupina a antivirový test nebo heuristická analýza naleznou na vašem poèítaèi virus, bude pøíslušnému uživateli nebo skupinì uživatelù zaslána zpráva o nalezení viru.

Pokud nastavíte sí□ovou komunikaci na volbu ANO, je nutné zadat jméno uživatele, kterému mají být zprávy odesílány a jméno souboru, do kterého se mají tato hlášení zapisovat - napø. pokud není uvedený uživatel pro hlášení dostupný.

Správce sítì musí zajistit pøístupová práva k vytváøení a zápisu log-souboru v zadaném adresáøi pro uživatele programu AVGW.

Uložení nastavení na disk

Provede manuální uložení nastavené konfigurace do konfiguraèního souboru. Zajistíte si tak, že Vámi nastavená konfigurace bude platná pøi dalších spouštìních programu. Program AVGW.EXE vytváøí konfiguraèní soubor se jménem AVGW.CFG.

Pokud požadujete, aby se Vámi zmìnìná konfigurace na disk ukládala *automaticky* vždy po ukonèení programu AVGW, je možné použít nastavení Zaznamenávat konfiguraci v Nastavení prostøedí.

Pokud bylo v daném sezení zadáno pøístupového heslo pro uvolnìní privilegovaných funkcí, je uložení aktuálního nastavení svázáno s pøístupovým heslem. Pokud v dalších sezeních nebude také zadáno platné pøístupové heslo, nebude možné ukládat zmìnìné nastavení. Tak je zajištìno, aby laický uživatel (neznalý pøístupového hesla) pozdìji nezmìnil nastavení provedené správcem systému - tj. mùže mìnit nastavení platné pro aktuální sezení, nedokáže je ale uložit na disk.

Standardní nastavení

Obnoví všechna nastavení programu AVGW na pùvodní, výrobcem definované hodnoty. Tato volba je ***privilegovaná*** - tj. je pøístupná až poté, co uživatel zadá platné pøístupové heslo v Menu SERVIS.

Zadání pøístupového hesla

Pøístupové heslo jistí v programu AVGW ty funkce, které lze z hlediska systému považovat za klíèové. Z tohoto dùvodu jsou nìkteré funkce standardnì nepøístupné - tj. v Menu jsou barevnì odlišeny. Pro jejich použití je nutné nejprve zadat platné pøístupové heslo.

Standardní heslo

Základní, vždy platné heslo, je uloženo v souboru **{HESLO}** na instalaèní disketì systému AVG. Tento soubor se bìhem instalace nekopíruje na pevný disk.

Uživatelské heslo

Kromì standardního, stále platného hesla, je možné definovat libovolné uživatelské pøístupové heslo heslo v menu Nastavení parametrù prostøedí.

Zálohování systémových oblastí

Naprostá vìtšina uživatelù ví, že systémové oblasti diskù a disket jsou nejen nositeli klíèových informací pro správný chod vašeho poèítaèe, ale také, že právì tyto oblasti se stávají cílem útokù virù napadajících systémové oblasti.

Odstraòování virù z tìchto oblastí je velmi choulostivá záležitost s ohledem na možnost havárie celého systému. Snad nejjednodušší a pøitom jednoznaènì nejspolehlivìjší technikou je vytvoøit si záložní kopie systémových oblastí a, v pøípadì jejich napadení èi poškození virem, využít tìchto kopií k obnovì do pùvodního stavu.

Všechny dùležité systémové oblasti se ukládají do jediného souboru, odkud si v pøípadì potøeby program AVGW dokáže zpìtnì vyzvednout potøebné informace. Ve verzi 4.0 systému AVG se ukládají tyto oblasti:

Partition tabulka - hlavní
Extended partition tabulky
Boot sektory zaøízení vytvoøených na pevném disku
CMOS pamì

Zálohování se nebude týkat tìch zaøízení, která jsou oznaèena jako sí ová.

Prvním krokem po zvolení funkce je zadání jména souboru, do kterého se uloží záložní kopie. Standardnì navržené jméno je A:\SYSTAB.GRS. Jméno, pøípadnì i umístìní, je samozøejmì možné zmìnit.

Obecnì nelze doporuèit uložení záložního souboru na stejné médium,které je zálohováno - v pøípadì havárie by bylo nepøístupné nejenom zaøízení, ale i záložní kopie.

Po zadání jména záložního souboru následuje vlastní zálohování. Pokud soubor záložních kopií již existuje, je na tuto skuteènost uživatel upozornìn a potvrdí pøepsání tohoto souboru. Program AVGW také testuje, zda zálohované systémové oblasti neobsahují virus. V takovém pøípadì by uložení systémových oblastí odmítl provést.

Obnova systémových oblastí

Funkce pro obnovu systémových oblastí umožòuje provést obnovu systémových oblastí poèítaèe prostøednictvím záložních kopií, které uživatel døíve vytvoøil funkcí Uložení systémových oblastí programu AVGW.

Po zvolení funkce pro obnovu systémových oblastí se uživateli nabídne dialog, ve kterém oznaèí ty systémové oblasti, které požaduje obnovit. Je možné oznaèit vždy pouze jednu oblast k obnovì.

Následuje zadání zaøízení, pro které požadujete obnovu provést. Toto zadání se nevypisuje v pøípadì, že požadujete obnovit pamì CMOS.

Dalším krokem je zadání souboru záložních kopií, který byl døíve vytvoøen pomocí funkce pro Zálohování systémových oblastí.

Po potvrzení požadavku na obnovu se provede obnova oznaèené systémové oblasti.

Krokování kódu

Je funkce urèená pro *znaènì pokroèilé uživatele*. Zpøístupòuje plnou heuristickou analýzu formou debuggeru - tj. umožní krokovat zvolený testovaný objekt po jednotlivých instrukcích. Je urèena pro uživatele, jejichž znalosti systému a assembleru dosahují takového stupnì, že jsou schopni posoudit korektnost testovaného objektu.

Tímto zpùsobem lze testovat

- Zvolené soubory
- Partition tabulku
- Boot sektory

Pro funkci krokování kódu lze nastavit tyto parametry:

- Detekce cyklù - jsou detekovány odskoky na opakující se adresy.
- EXE relokace - je provádìn pøepoèet relokací u EXE souborù Log soubor - je vytváøen samostatný report soubor pro provádìné krokování

Automatické spouštìní

Funkce pro automatické spouštìní pøedstavuje užiteènou pomùcku. Umožòuje nastavit si požadované intervaly spouštìní jednotlivých testù. Kdykoliv spustíte program AVGW, zkontroluje, zda nenastal èas pro automatické spuštìní testu.

Funkce umožòuje nastavit automatické spouštìní pro každý typ testu samostatnì. Volitelnými položkami jsou :

- den v týdnu, kdy se má test spustit
- požadované oblasti k otestování - Výbìr zaøízení
- parametry, ovlivòující chování testu - napø., zda bude možné test pøerušit èi nikoliv, zda se mají bìhem testu vydávat hlášení, apod.

Ovládání programu AVGW - Desktop

Ovládání programu AVGW, jako aplikace pro WINDOWS je standardizované. Nemìlo by tedy èinit bìžným uživatelùm potíže. Vlastní pracovní plocha je rozdìlena na tyto èásti :

Øádek Menu
Obsahuje nabídku dostupných funkcí, prostøednictvím Menu.

Ikony pro rychlé spuštìní
Jsou umístìny pod øádkem s Menu. Tyto ikony slouží k rychlému spuštìní nejèastìji volaných funkcí - Antivirového testu, Srovnávacího testu, Heuristické analýzy, Testu pamìti RAM a Ukonèení programu.

Informace o nastavení programu
Na desktopu programu AVG je také okno, obsahující informace o nastavení nejdùležitìjších parametrù. Toto okno má pouze informaèní hodnotu - informace zde zobrazené nelze z Desktopu AVGW mìnit - k tomuto úèelu slouží funkce z menu Nastavení testù a Nastavení prostøedí.

Jak kontaktovat výrobce

V pøípadì, že uživatelé programu AVGW potøebují kontaktovat výrobce systému, firmu **GRISOFT(c) SOFTWARE sro.**, mohou se na nás obrátit na tuto adresu :

GRISOFT(c) SOFTWARE sro.
Lidická 81, 602 00 Brno
tel : 05-413 212 62 / 224, 235, 245
fax : 05-412 114 32
BBS : 05-412 114 32
Internet : grisoft@grisoft.anet.cz

Aktualizace systému AVG

Antivirový systém AVG je pravidelnì aktualizován. Vlastní vývoj a aktualizace se provádí následujícím zpùsobem :

Pravidelná aktualizace

1x mìsíènì vydává výrobce systému, GRISOFT(c) SOFTWARE sro., aktualizaèní program, který je uživatelùm k dispozici **bezplatnì**. Aktualizaèní program, poté co jej spustíte, doplní nové viry do interní virové databanky a pøípadnì nahradí nìkteré z programù Vaší stávající instalace jejich novìjší, aktualizovanou, podobou. Jedná se tedy pøedevším o kvantitativní aktualizaci a kvalitativní zmìny menšího rozsahu.

Aktualizaèní program mùže zájemce získat na firemní stanici BBS, na anonymních FTP serverech, pøípadnì si mùže u výrobce objednat disketovou službu, kdy mu bude vždy 1x mìsíènì zaslána disketa s nejnovìjším aktualizaèním programem.

Nové verze systému AVG

V intervalu 9-10 mìsícù vydává výrobce nové verze systému AVG. Tyto nové verze s sebou pøináší výrazné zmìny, jako zcela nové funkce, podstatné zmìny ve stávajících funkcích apod. Nové verze jsou registrovaným uživatelùm nabízeny za výhodné UpGrade ceny.

Soubor _GRISOFT.VIR

V pøípadì, že heuristická analýza detekuje na testovaném zaøízení soubor, který považuje za napadený virem - poèet a "váha" zjištìných pøíznakù je velmi vysoká a nedokáže urèit o jaký konkrétní typ viru se jedná, exportuje vzorek viru do zvláštního souboru, oznaèovaného jako **_GRISOFT.VIR** v koøenovém adresáøi disku C:, a upozoròuje uživatele, že tento soubor by mìl být dopraven k výrobci.

Pracovníci naší firmy takto získaný vzorek analyzují a patøièným zpùsobem jej zahrnou do pøíštího vydání aktualizaèního programu - v pøípadì, že se jedná o nový virus, bude zaøazen do interní virové databáze, v opaèném pøípadì bude doplnìn do validaèního souboru.

Testovací makra

Testovací makra pøedstavují zajímavou možnost jak urychlit a zefektivnit èasto provádìné testy. Pøedstavte si, že uživatel velmi èasto provádí heuristickou analýzu adresáøe C:\DOS.

V praxi to znamená, že musí z menu Testy zvolit heuristickou analýzu, na zaøízení C: vybrat k testu adresáø \DOS a spustit heuristickou analýzu. Pokud by použil testovacího makra, celý proces by se podstatnì zjednodušil.

Prvním krokem je definice uživatelského makra. Uživatel pøipraví textový soubor, který obsahuje povolené pøíkazy, urèující požadované testy. Soubor mùže mít libovolné jméno - jeho rozšíøení však musí být .MAK.

Do tohoto souboru umístí popis požadované akce. Pøíkazy, používané k tomuto popisu jsou velice podobné pøíkazùm, které se používají pro vytvoøení a popis pøíkazového souboru. Jejich popis je uveden v uživatelské dokumentaci k programu.

Pøi spuštìní programu AVGW se zjišuje, zda v daném adresáøi existují soubory s rozøíøením *.MAK. Pokud ano, mùže využít uživatel v programu AVGW testovacích maker.