Úvod

Panda Antivirus

Panda Anti-Virus Professional je skupina programových balíkov pre komplexné riešenie ochrany pocítacov a pocítacových sietí pred vírusmi. Pokrýva všetky bezné platformy operacných systémov a je lokalizovaný do viacerých svetových jazykov. V nasledujúcich odsekoch strucne charakterizujeme jednotlivé programy, ktoré tvoria základ pre ponúkané produkty antivírusovej ochrany PANDA.

Stratégie ochrany

Panda Antivirus poskytuje pouzívatelovi kombináciu nasledovných techník ochrany:

- **Neustála ochrana:** neustála ochrana chráni pocítac pocas pouzívania pocítaca bez zásahu pouzívatela. Výhodou tejto metódy je poskytnutie plne automatickej ochrany.
- **Kontrola na poziadanie:** kontrola na poziadanie poskytuje pouzívatelovi moznost kontroly pocítacového systému kedykolvek. Stací zvolit oblast, ktorá sa má kontrolovat a vhodne nakonfigurovat spôsob kontroly.
- **Dezinfekcia:** v prípade nájdenia vírusu, má pouzívatel viacero mozností – pocnúc dezinfekciou, ktorá pozostáva z odstránenia vírusu zo súboru.
- **Heuristická analýza:** je alternatívou k regulárnej kontrole - umoznuje vypátranie neznámych druhov vírusov.
- **Hladanie znakov:** metóda pouzíva obdobný systém prehliadania súborov, ale na rozdiel od regulárnej kontroly umoznuje pouzívatelovi zadat jednotlivé retazce manuálne. Týmto spôsobom mozno vyhladat nový vírus – Technická podpora Panda Software zašle pouzívatelovi jednotlivé retazce korešpondujúce s novým vírusom a pouzívatel si má moznost okamzite otestovat ci sú súbory nakazené alebo nie.
- **Ostatné moznosti:** pod touto polozkou sú zoskupené viaceré crty anti-vírusu vytvorené na poskytovanie informácií, sluzieb a i.

Co je to 24h-365d® Panda Software Antivirus Insurance® ?

24h-365d® Panda Software Antivirus Insurance® je nový revolucný spôsob anti-vírusovej ochrany, ktorý poskytuje zákazníkom maximálnu moznú bezpecnost.

24h-365d® Panda Software Antivirus Insurance® je kombináciou produktov a sluzieb, ktorá ponúka najvyššiu úroben ochrany voci vírusom.

Panda Antivirus zahrna certifikácie:

- **ICSA Certification:** garantovaná prestíznou americkou asociáciou ICSA (International Computer Security Association). Produkty Panda detekujú 100% zo skupiny vírusov *In the Wild* (najcastejšie aktívne vírusy) a viac ako 90% zo skupiny *Zoo Collection* (kolekcia niekolko tisíc známych vírusov).

- **CheckMark Certification:** garantovaná British computer security magazine - *Secure Computing*.

Ak nie ste poistení s **24h-365d® Panda Software Antivirus Insurance®**, prichádzate o:

HOTLINE

Sluzbu HOTLINE môzu vyuzit **zadarmo registrovaní** zákazníci prostredníctvom telefónu, faxu, poštou alebo e-mailom. Kvalifikovaní odborníci Vám poskytnú pomoc pri riešení problémov, ktoré sa týkajú problematiky vírusových infekcií a ovládania softvéru Panda Anti-Virus Professional.

AKTUALIZÁCIA

Naše produkty sú neustále aktualizované, pricom berieme do úvahy pripomienky našich zákazníkov (HOTLINE a S.O.S. servis). Pravidelnú aktualizáciu mozno štandardne získavat kazdý mesiac resp. štvrtrok prostredníctvom Internetu alebo na médiách - podla priania zákazníka. Nová verzia samotného aktualizacného súboru je k dispozícií **denne**.

S.O.S. sluzba

Sluzba je orientovaná na minimalizáciu škôd, ktoré môzu byt spôsobené výskytom ešte neidentifikovatelného vírusu, respektíve vírusu, ktorý nie je mozno odstránit pomocou Panda Anti-Virus (bol detekovaný napr. heuristickou metódou vyhladávania). V prípade, ze zistíte pôsobenie neznámej vírusovej infekcie, zašlite nám prostredíctvom e-mailu infikované súbory. Problém je spolocnost Panda schopná vyriešit do 48 hodín (zaslanie novej verzie, ktorá rieši daný problém).

Panda INTERNET Server a BBS

Ak máte modem alebo prístup na Internet, môzete sa spojit so serverom spolocnosti Panda www.pandasoftware.com **alebo** www.pronetix.sk, kde môzete získat najnovšie informácie o produktoch Panda ako i aktualizáciu zakúpených produktov Panda na najnovšie verzie.

Odborné poradenstvo, Riziková analýza

Poskytujeme odborné poradenstvo pre vývoj a implementáciu zabezpecenia Vášho informacného systému vo forme analýzy a návrhu najvhodnejšej implementácie s prihliadnutím na špecifiká zákazníka. Túto sluzbu poskytujeme s nevyhnutnými nástrojmi a s prípadnou implementáciou do Vášho prostredia (podla zelania zákazníka).

Zberné centrum pre Slovensko

Spolocnost proNETIX ako výhradné zastúpenie Panda Software International pre Slovensko zabezpecuje zachytenie vírusov špecifických pre Slovensko, ich analýzu a následné zakomponovanie do systémov ochrany PANDA.

Inštalácia

Inštalácia pod Windows 95

Základná konfigurácia pracovnej stanice nevyhnutná pre inštaláciu je:

- IBM PC, PS/2 alebo 100% kompatibilný, procesor rady 386 alebo vyššej,
- minimum 4 MB RAM operacnej pamäti,
- minimum 4 MB volného miesta na pevnom disku,
- operacný systém Windows 95.

Samotná inštalácia je jednoduchá a pozostáva z nasledovných základných krokov:

1. Vlozte inštalacnú disketu s oznacením **Panda Anti-Virus Professional for Windows 95, DISK1** do mechaniky A: (alebo B:). Aktivujte program:

```
A:\SETUP.EXE
```

Ak inštalujete z CD-ROM, aktivujte program SETUP.EXE z adresára /INSTALL/WIN95/.

2. Po aktivovaní daného súboru sa inštalacný program bude informovat na adresár, do ktorého chcete inštalovat anti-vírus Panda. Implicitne je nastavený názov adresára ako:

```
C:\PAVPW95
```

V prípade potreby mozno daný názov zmenit, doporucuje sa implicitné nastavenie.

Po ukoncení procesu inštalácie si vyhladajte vo vnútri hlavného menu systému Windows 95 (Start/Programs menu/..) polozku **Panda Anti-Virus Professional for Windows 95**. Pred pouzitím doporucujeme pouzívatelom, preštudovanie súboru `readme.doc`, ktorý obsahuje najaktuálnejšie zmeny produktu vzhladom na predošlú verziu. Môze obsahovat informácie neuvedené v tomto manuále.

Pocas procesu inštalácie sa inštalacný program bude informovat, ci chcete inštalovat nasledujúce súcasti produktu:

- Neustála ochrana pre Windows 95 (Pernament protection under Windows 95),
- Systémová kontrola pocas behu bootovacieho procesu pocítaca (System scan during the PC boot process).

Volba **neustálej ochrany** umoznuje programu stálu kontrolu nad prevádzkou súborov v pocítaci. Prípadné vírusy budú detekované automaticky a pouzívatel nepotrebuje vyuzívat nástroje pre manuálne vyhladávanie vírusovej infekcie.

Systémová kontrola pocas behu bootovacieho procesu pocítaca má za úlohu zistit neziadúcu prítomnost vírusov pred štartom samotného operacného systému Windows 95. Táto moznost kontroluje nasledujúce casti systému pocítaca:

- RAM pamät
- boot sektory
- systémové súbory
- rezidentné (korenové) adresáre

Toto sledovanie cinnosti je vykonávané pocas trvania pociatocného zavádzania systému.

Inštalacný program aktivuje tieto dve polozky implicitne. Doporucujeme pouzívatelom ich inštaláciu.

Odinštalovanie

Program Panda Anti-Virus For Windows 95 mozno odinštalovat nasledujúcim spôsobom. V hlavnom menu zvolte polozku *Start/Settings/..* a dalej *Control Panel*. V okne *Control Panel* zvolte ikonu *Add/Remove Programs*. V zozname nainštalovaných aplikácií je zaradený adresár s názvom **Panda Anti-Virus Professional**. Oznacte adresár a stlacte tlacítko *Add/Remove*. Program Panda Anti-Virus Professional For Windows 95 bude následne odinštalovaný.

V prípade, ak pouzívate lokalizovanú verziu Windows 95, postupujte podla manuálu k danej verzii.

Aký význam má neustála ochrana ?

Úlohou neustálej ochrany je chránit pocítacový systém pocas práce od jeho štartu a zabránit nezelaným prienikom vírusovej infekcie.

Neustála ochrana je plne automatický systém – nevyzaduje obsluhu pouzívatelom. Monitoruje súbory, s ktorými sú vykonávané operácie.

Zavedením neustálej ochrany do systému sa podstatne zvýši úroven jeho zabezpecenia.

Zavedenie neustálej ochrany

Pri inštalácií programov Panda Anti-Virus pre Windows 95 má pouzívatel moznost volby inštalácie neustálej ochrany.

Pre konfiguráciu, prípadne deaktiváciu detekcného programu mozno vyuzit ikonu programu SENTINEL v roletovom menu systému Windows 95 (obycajne sa nachádza v pravom dolnom rohu plochy).

Ikona zobrazuje logo produktu a spolocnosti Panda. Ak je program aktivovaný, je sfarbenie ikony do zelena (medved), inác do siva.

Ak sa umiestni kurzor myši na túto ikonu, text v pop-up informuje o aktuálnom stave - aktívny (active) alebo neaktívny (inactive).

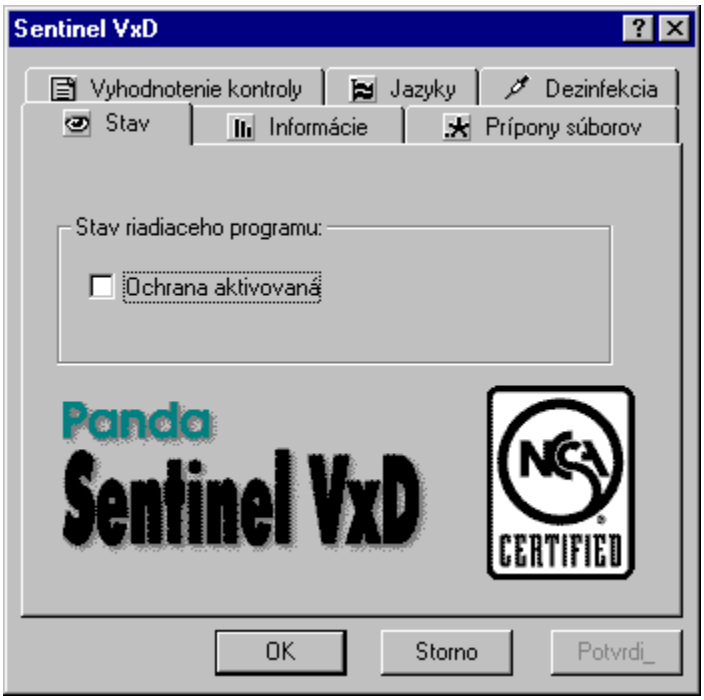
Hlavné menu konfigurácie programu SENTINEL sa zobrazí kliknutím lavým tlacítkom myši v priestore ikony Panda. Kliknutím pravým tlacítkom sa zobrazí menu:

- **Aktivovat/Deaktivovat** (Activate/Deactivate) – moznost aktivácie alebo deaktivácie programu SENTINEL VxD
- **Nastavenie konfigurácie** (Configure) - zobrazí sa okno konfigurácie SENTINELu
- **Ukoncit SENTINEL VxD** (Close) - program deaktivuje systém ochrany a ukoncí svoju cinnost.

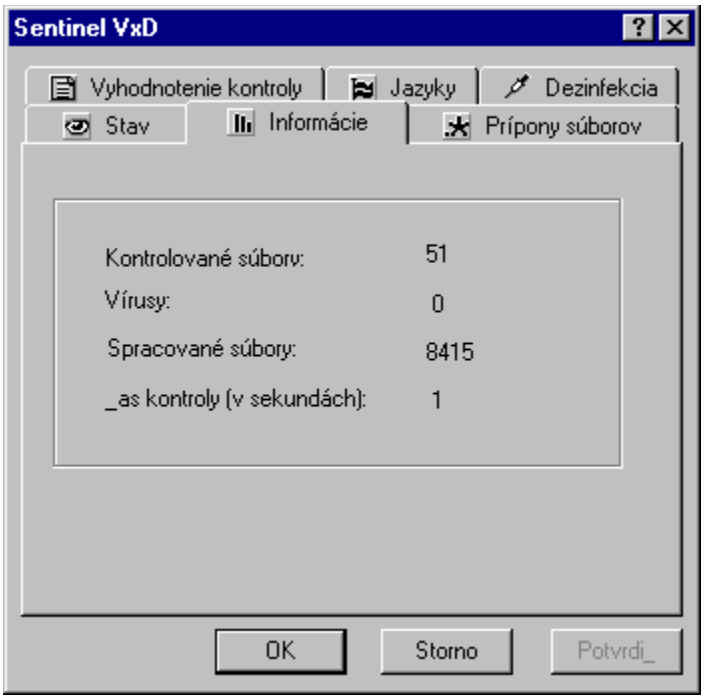
Konfigurácia neustálej ochrany

Stav (Status)

Okno zobrazuje aktuálny **Stav riadiaceho programu** neustálej ochrany – programu SENTINEL (Driver Status). Stav mozno zmenit – **Ochrana aktivovaná** (Activated) alebo neaktivovaná (ak nie je zaškrtnuté príslušné políčko).



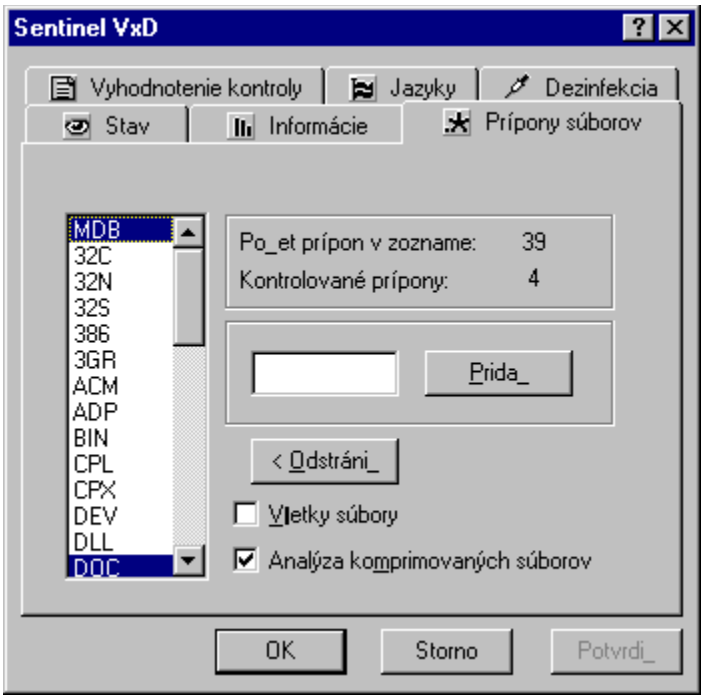
Informácie (Information)



V tomto okne sa nachádzajú numerické informácie:

- **Kontrolované súbory** (Files checked) - číslo zobrazuje pocet kotrolovaných súborov.
- **Vírusy** (Viruses Found) - číslo zobrazuje pocet súborov napadnutých infekciou, s ktorými bola vykonávaná operácia.
- **Spracované súbory** (Intercepted Files) - číslo zobrazuje pocet súborov zachytených Sentinelom, s ktorými bola vykonaná operácia. Súbory nemuseli byt kontrolované (podla konfigurácie).
- **Cas kontroly** (Total Scanning Time) - celkový cas potrebný na kontrolu súborov (v sekundách).

Prípony súborov (Scannable Extensions)



Prostredníctvom okna **Prípony súborov** (Scannable Extensions) mozno vybrat typy súborov podla prípony, ktoré sa majú kontrolovat. **Implicitne je nastavená kontrola** pre súbory s nasledovnými príponami: **EXE, COM, XLS, DOC, DOT, BOO, SYS a BIN**.

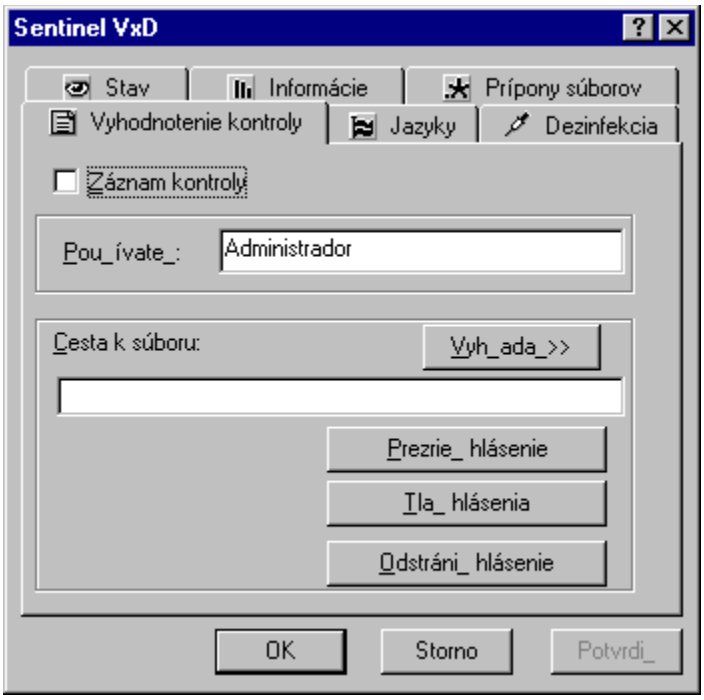
Tieto typy súborov sú najcastejšie napádané vírusovou infekciou. Prípony netreba do zoznamu doplnat.

Ak sa v zozname prípon nevyskytuje prípona súborov, ktoré je nevyhnutné kontrolovat, mozno ju pridat do zoznamu vpísaním do pola a stlacním tlacítka Add (Pridat). Tlacítko Remove (Odobrat) slúzi na odstránenie vopred oznacených koncoviek. V zozname sa môze nachádzat maximálne 50 koncoviek súborov. Pouzívatel má dalej moznost zvolit:

Všetky súbory (All) - v prípade aktivácie sa budú kontrolovat všetky súbory, s ktorými sa uskutocnuje operácia nezávisle od oznacených typov prípon v zozname. Táto moznost sa nemusí vyuzívat neustále, pretoze kontrola všetkých súborov môze zaberat viac casu, co však nemusí byt efektívne pri vyhladávaní infekcie. Aktivácia moznosti "Všetky súbory" je opodstatnená len v prípade, ak pouzívatel predpokladá moznost práce s infikovanými súbormi.

Analýza komprimovaných súborov (Analyze Compressed Files) - SENTINEL VxD automaticky analyzuje obsah komprimovaných súborov. Ak je táto moznost aktivovaná, SENTINEL VxD kontroluje súbory, ktoré sa nachádzajú vo vnútri komprimovaných súborov.

Vyhodnotenia kontroly (Results)



V tomto okne mozno nastavit spôsob generovania súboru, do ktorého sa zaznamenávajú všetky informácie o kontrole.

Súbor obsahuje názvy vírusov, napadnutých súborov a cas, kde boli zachytené.

Vyhodnotenie kontroly sa zaznamenáva len v prípade, ak je aktivovaná polozka:

- Záznam kontroly (Generate Report)

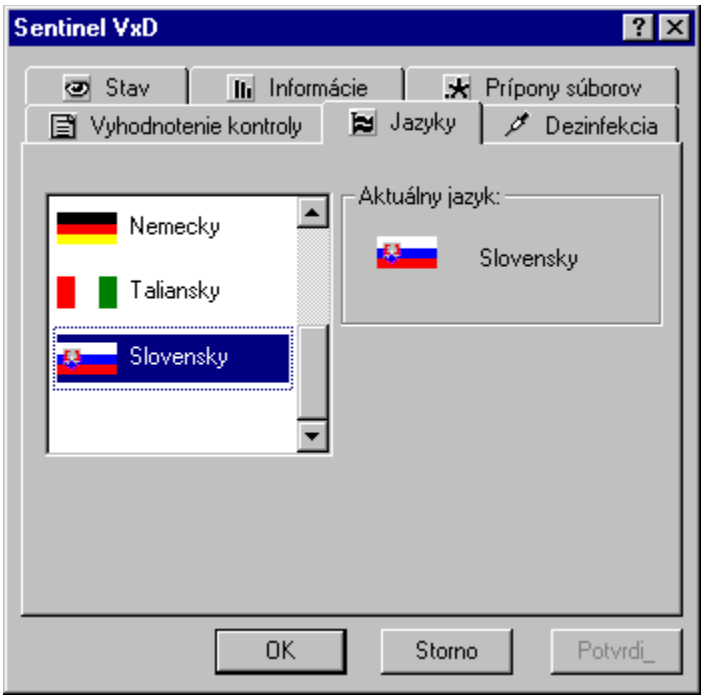
a je zadaná cesta do adresára, v ktorom sa má súbor nachádzat. Cestu môze pouzívatel definovat v casti okna (Cesta k súboru - Report Path) priamo, alebo pomocou tlacítka Vyhladat (Browse).

V prídade, ze s PC pracuje viac pouzívatelov, je potrebné uviest jeho meno (Pouzívatel - User). „Správca“ má moznost jednoduchšie identifikovat pouzívatela, ktorý pracoval s infikovanými súbormi.

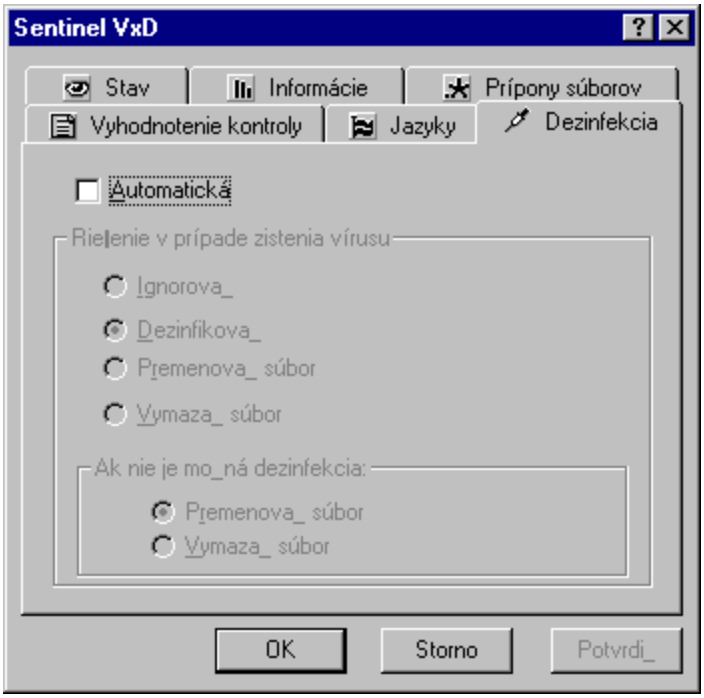
Pouzívatel má kedykolvek moznost vyvolat si príslušný súbor pomocou tlacítka **Prezriet hlásenie** (See Report Now). Tlacítko **Tlac hlásenia** (Print Report) slúzi na jednoduchú obsluhu tlace súboru. Ak súbor neobsahuje aktuálne informácie, mozno ho odstránit pomocou Odstránit hlásenie (Erase Report).

Jazyky (Languages)

V okne sa zobrazuje informácia o zvolenom aktuálnom jazyku (Current Language) a iných moznostiach volby jazyka. Tu mozno prepnút len jazyk programu SENTINEL (nie regulárneho programu).



Dezinfekcia (Disinfection)



Program SENTINEL umoznuje dezinfekciu súborov. Ak pouzívatel aktivuje polozku Dezinfekcia

(Disinfection), infikované súbory môzu byt dezinfikované bez zásahu pouzívatela.

Riešenie situácie v prípade zistenia vírusu (What to do if a virus is found):

- **Ignorovat** (Ignore) - v prípade napadnutia vírusom program zaznamená do výsledného hodnotenia dané zistenie, ale nevykoná ziadne opatrenia.
- **Dezinfikovat** (Disinfect) - v prípade napadnutia vírusom program dezinfikuje napadnuté súbory, ak je to mozné.
- **Premenovat súbor** (Rename file) - premenovanie infikovaných súborov.
- **Vymazat súbor** (Erase file) - vymazanie infikovaných súborov.

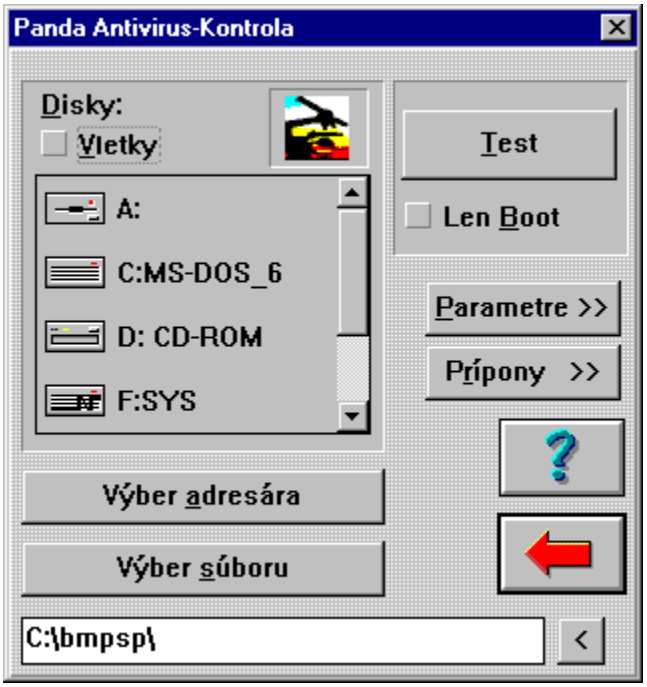
  Ak nie je mozná dezinfekcia súborov (If no disinfection possible):

  - **Premenovat súbor** (Rename file) – premenovanie infikovaných súborov.
  - **Vymazat súbor** (Erase file) – vymazanie infikovaných súborov.

Co znamená kontrola na poziadanie ?

Kontrola na poziadanie umoznuje pouzívatelovi otestovat si lubovolnú zvolenú cast pocítaca. Pri kazdej kontrole mozno zvlášt konfigurovat všetky mozné parametre.

Pouzitie kontroly na poziadanie



Kontrolu na poziadanie mozno uskutocnit realizáciou nasledovných krokov:

Pred aktiváciou regulárnej kontroly je nevyhnutné nastavit tieto parametre:

- **Vybrat cast z pocítacového systému, ktorá sa má kontrolovat.** Pouzívatel má nasledovné moznosti:
    - **Všetky (All)** - Ak pouzívatel zvolí túto moznost, anti-vírus kontroluje celý systém pocítaca, t.z. boot systém všetkých médií a diskov, obsah root adresárov a podadresárov na médiách a všetky súbory podla konfigurácie.
    - **Disky (Drives**) - Pouzívatel si musí zvolit aspon jedno z moznych médií (disk, disketa, CD-ROM), ktoré sa má kontrolovat. **Vzdy sa kontroluje boot systém zvoleného disku (média)**.
    - **Výber adresára (Select Directory)** – Pouzívatel špecifikuje adresár, v ktorého obsah sa má preverit. Ak zvolíme túto polozku, budú kontrolované zvolené adresáre a jeho príslušné podadresáre.
    - **Výber súboru (Select File)** – Pouzívatel špecifikuje súbor, v ktorý sa má kontrolovat.
    - **Len Boot (Only Boot)** - Prostredníctvom tejto polozky mozno skontrolovat boot systém jednotlivých médií pocítaca. Pouzívatel musí zvolit príslušné médium.
- **Špecifikovat parametre kontroly**

Nastavenie parametrov kontroly

Pouzívatel musí urcit nasledovné parametre kontroly:

- Oblast, ktorú treba skontrolovat.
- Prípony súborov.
- Všeobecné parametre kontroly.

Prípony súborov

Prostredníctvom tlacítka Extension mozno vybrat typy súborov podla prípony, ktoré sa majú kontrolovat. **Implicitne je nastavená kontrola** pre súbory s nasledovnými príponami: **EXE, COM, XLS, DOC, DOT, BOO, SYS a BIN**.

Ak sa v zozname prípon nevyskytuje koncovka súborov, ktoré je nevyhnutné kontrolovat, mozno danú koncovku pridat do zoznamu vpísaním do pola a stlacním tlacítka „+“ (Pridat). Tlacítko „-“ (Odobrat) slúzi na odstránenie vopred oznacených koncoviek. V zozname sa môze nachádzat maximálne 50 koncoviek súborov. Pouzívatel má moznost zvolit:

Všetky súbory (All) - v prípade aktivácie sa budú kontrolovat všetky súbory na príslušnom médiu nezávisle od oznacených typov koncoviek v zozname. Táto moznost sa vyuzíva zriedka, pretoze kontrola všetkých súborov môze zaberat vela casu, co však nemusí byt efektívne pri vyhladávaní infekcie. Aktivácia moznosti "Všetky súbory" je opodstatnená len v prípade zistenia prítomnosti vírusovej infekcie v pocítaci.

Tieto typy súborov sú najcastejšie napádané vírusovou infekciou. Prípony netreba do zoznamu doplnat a nemozno ich zo zoznamu odstránit.

General Options (Všeobecné parametre kontroly)

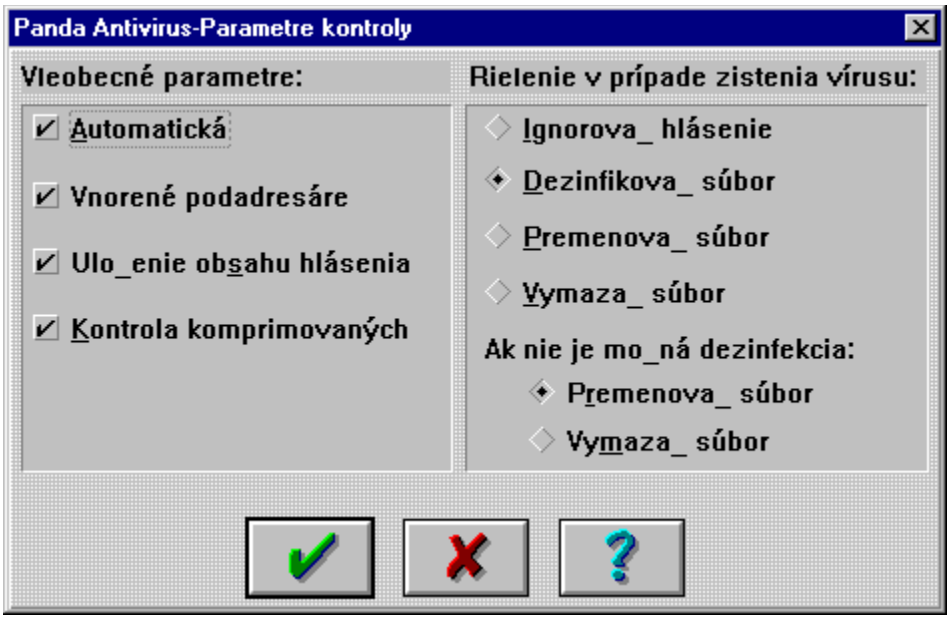
Po aktivácii tlacítka **Parametre (Options)** sa zobrazí okno **Parametre kontroly (Scan Options)**.

Okno osahuje nasledujúce polozky:

General Options (Všeobecné parametre):

Automatická kontrola **(Automatic)** - ak je polozka aktivovaná, program pracuje bez zásahu pouzívatela. V prípade zistenia vírusovej infekcie postupuje samostatne, po skoncení kontroly vypíše zoznam nevyhnutných operácií pocas kontroly a dezinfekcie ako aj výsledné vyhodnotenie.

Vnorené podadresáre (Nested subdirectories) - program vyhladáva vírusovú infekciu aj v podadresároch zvolených adresárov. Ak polozka nie je aktivovaná, kontrola sa vykonáva len vo zvolenom adresári, resp. v roote disku.



Ulozenie obsahu hlásenia (Save results) - informácie o priebehu kontroly sa ulozia a uchovajú v súbore na pevnom disku. Súbor je kedukolvek prístupný pouzívatelovi. Doporucuje sa vyuzitie tejto funkcie pre prípad, ak chce pouzívatel zaznamenat a neskoršie si pripomenút aktuálny stav kontroly.

Kontrola komprimovaných (Scan compressed) - aktivovaním sa kontroluje aj obsah komprimovaných súborov. Program kontroluje prípadné napadnutie komprimovaných súborov a súborov, ktoré sa v nich nachádzajú a sú regulárne.

Riešenie situácie v prípade zistenia vírusu (What to do if a virus is found):

- **Ignorovat** (Ignore) - v prípade napadnutia vírusom program zaznamená do výsledného hodnotenia dané zistenie, ale nevykoná ziadne opatrenia.
- **Dezinfikovat** (Disinfect) - v prípade napadnutia vírusom program dezinfikuje napadnuté súbory, ak je to mozné.
- **Premenovat súbor** (Rename file) - premenovanie infikovaných súborov.
- **Vymazat súbor** (Erase file) - vymazanie infikovaných súborov.

  Ak nie je mozná dezinfekcia súborov (If no disinfection possible):

  - **Premenovat súbor** (Rename file) – premenovanie infikovaných súborov.
  - **Vymazat súbor** (Erase file) – vymazanie infikovaných súborov.

Heuristická analýza

Test (Scan - Regulárna kontrola) umoznuje pouzívatelovi kontrolu systému na všetky známe vírusy. Investigate (Vyhladávanie vírusov analýzou súborov) umoznuje vypátranie neznámych druhov vírusov. Kontrola na poziadanie (Test) je úcinná v prípade, ak anti-vírus pozná správanie vírusu. V prípade, ze je vyvinutý úplne nový druh vírusu, nemusí neaktualizovaná verzia takúto infekciu pomocou regulárnej kontroly zaznamenat.

Heuristická metóda vymedzuje prítomnost vírusu podla správania programu pocas priebehu kontroly a nepokúša sa identifikovat vírus. To umoznuje zaznamenanie nového, ešte neidentifikovatelného vírusu (pre regulárnu kontrolu).

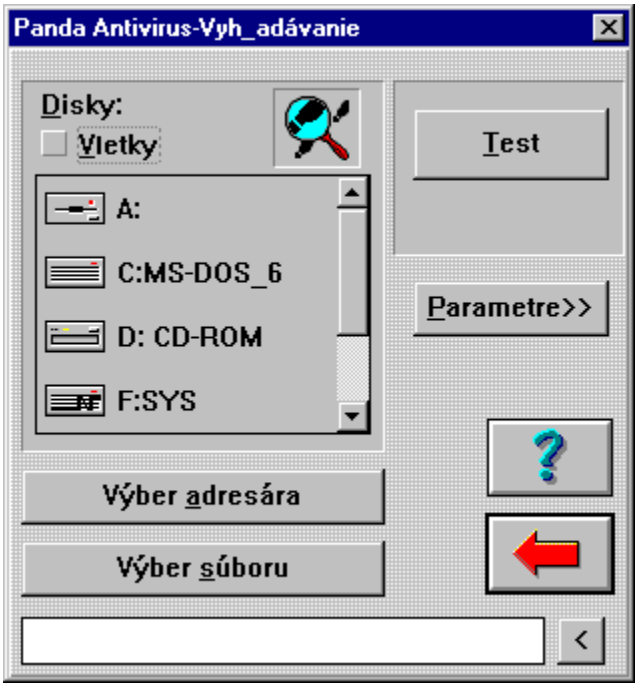
Podozrivé súbory detekované s touto technikou nemusia byt dezinfikovatelné.

Na druhej strane je však bezné, ak anti-vírus nájde niekolko programov (súborov) napríklad na pevnom disku a oznací ich ako "ciastocne podozrivé" (minimally suspicious). Nemusí však íst o infekciu. Ak sa však na danom médiu nachádza viac ciastocne podozrivých súborov, môze to tiez znamenat nakazenie vírusovou infekciou a je nevyhnutné zaslat vzorky výrobcovi anti-vírusu (pozri: HOTLINE).

Analýza umoznuje zistit správanie a detekovat podozrivú cinnost rezidentných programov (trvalo zavedených v pamäti) v systéme, ktorá nemôze byt zaznamenaná regulárnou kontrolou, ak cinnost vírusu nie je dokumentovaná. Poskytuje pouzívatelovi monitorovanie správania:

- boot vírusov a
- vírusov, ktoré infikujú súbory (obsahujú podozrivé inštrukcie pre operácie s inými súbormi a vykonávajú ich).

Pouzitie heuristickej analýzy



Kontrolu na poziadanie mozno uskutocnit realizáciou nasledovných krokov:

Pred aktiváciou regulárnej kontroly je nevyhnutné nastavit tieto parametre:

- **Vybrat cast z pocítacového systému, ktorá sa má kontrolovat.** Pouzívatel má nasledovné moznosti:
  - **Všetky (All)** - Ak pouzívatel zvolí túto moznost, anti-vírus kontroluje celý systém pocítaca, t.z. boot systém všetkých médií a diskov, obsah root adresárov a podadresárov na médiách a všetky súbory podla konfigurácie.
  - **Disky (Drives)** - Pouzívatel si musí zvolit aspon jedno z mozných médií (disk, disketa, CD-ROM), ktoré sa má kontrolovat. **Vzdy sa kontroluje boot systém zvoleného disku (média)**.
  - **Výber adresára (Select Directory)** – Pouzívatel špecifikuje adresár, v ktorého obsah sa má preverit. Ak zvolíme túto polozku, budú kontrolované zvolené adresáre a jeho príslušné podadresáre.
  - **Výber súboru (Select File)** – Pouzívatel špecifikuje súbor, v ktorý sa má kontrolovat.
- **Špecifikovat parametre analýzy**

Citlivost (Level) heuristickej analýzy môze byt upravená nastavením úrovne v hlavnom menu analýzy. Pouzívatel má moznost nastavit jednu z troch úrovní (Minimum, Medium, Maximum). Okrem toho mozno v pravej casti okna nastavit zobrazovanie hlásenia pri vyhladaní súborov (Report on – Upozornit na):

- **Komprimované súbory** (Compressed Files),

- **Ockované súbory** (Vaccinated Files),
- **Nesprávny dátum a cas** (Incorrect date and time).

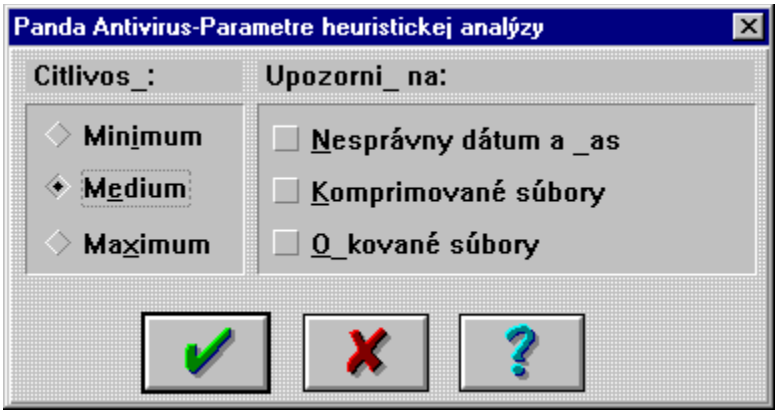
Komprimované súbory (sprostredkované napr. zo siete Internet) môzu byt potenciálnymi nositelmi infikovaných súborov. Nesprávne dátumy a casy môzu zvycajne signalizovat nakazenie vírusom, ktorý takýmto spôsobom mení parametre súborov (mení štruktúru súboru a tým môze menit aj dátum a cas poslednej zmeny súboru).

Konfigurácia parametrov heuristickej analýzy

Citlivost (Level) heuristickej analýzy môze byt upravená nastavením úrovne v hlavnom menu analýzy. Pouzívatel má moznost nastavit jednu z troch úrovní (Minimum, Medium, Maximum). Okrem toho mozno v pravej casti okna nastavit zobrazovanie hlásenia pri vyhladaní súborov (Upozornit na - Report on):

- **Komprimované súbory (Compressed Files),**
- **Ockované súbory (Vaccinated Files),**
- **Nesprávny dátum a cas (Incorrect date and time).**

Komprimované súbory (sprostredkované napr. zo siete Internet) môzu byt potenciálnymi nositelmi infikovaných súborov. Nesprávne dátumy a casy môzu zvycajne signalizovat nakazenie vírusom, ktorý takýmto spôsobom mení parametre súborov (mení štruktúru súboru a tým môze menit aj dátum a cas poslednej zmeny súboru).



Hladanie retazcov

Kontrola na poziadanie prehladáva súbory a detekuje casti vírusov. Databáza vírusov musí byt pravidelne doplnaná.

Metóda hladania retazcov pouzíva obdobný systém prehliadania súborov, ale na rozdiel od kontroly na poziadanie umoznuje pouzívatelovi zadat jednotlivé retazce manuálne.

Týmto spôsobom mozno vyhladat nový vírus – Technická podpora Panda Software zašle pouzívatelovi jednotlivé retazce korešpondujúce s novým vírusom a pouzívatel si má moznost okamzite otestovat ci sú súbory nakazené alebo nie.

Pouzitie hladania retazcov

Retazce mozno vyhladávat realizáciou nasledovných krokov:

Pred hladanie je nevyhnutné nastavit tieto parametre:

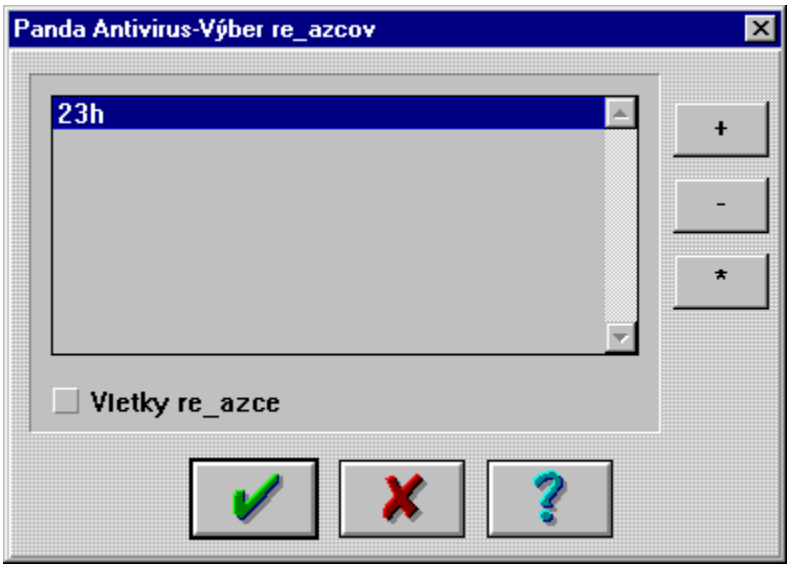
- **Vybrat cast z pocítacového systému, ktorá sa má kontrolovat.** Pouzívatel má nasledovné moznosti:
  - **Všetky (All)** - Ak pouzívatel zvolí túto moznost, anti-vírus kontroluje celý systém pocítaca, t.z. boot systém všetkých médií a diskov, obsah root adresárov a podadresárov na médiách a všetky súbory podla konfigurácie.
  - **Disky (Drives)** - Pouzívatel si musí zvolit aspon jedno z moznych médií (disk, disketa, CD-ROM), ktoré sa má kontrolovat. **Vzdy sa kontroluje boot systém zvoleného disku (média)**.
  - **Výber adresára (Select Directory)** – Pouzívatel špecifikuje adresár, v ktorého obsah sa má preverit. Ak zvolíme túto polozku, budú kontrolované zvolené adresáre a jeho príslušné podadresáre.
  - **Výber súboru (Select File)** – Pouzívatel špecifikuje súbor, v ktorý sa má kontrolovat.
- **Špecifikovat parametre hladania (co hladat)**

Ak pouzívatel pozaduje len prehladanie pamäti, postacuje aktivovat tlacítko Prehladat pamät (Explore Memory).

Výber retazcov

Používatel musí mat zvolenú oblast, ktorá sa má prehliadat a zvolené retazce, ktoré sa majú hladat.

Pomocou volby má pouzívatel moznost vyhladat ASCII, desiatkovo alebo šestnástkovo zapísané znaky v špecifikovaných súboroch, boot systéme alebo v pamäti. Retazce zadáva pouzívatel. Byty musia byt oddelené ciarkou (,).



Jednotlivé zadané retazce môzu byt hladané súcasne (All strings – Všetky retazce).

Pouzívatel môze pouzit túto metódu pre vyhladanie lubovolných znakov v súboroch ulozených na médiu.

Na obrázku je uvedený príklad zadania retazca. Retazce mozno pridat stlacením „+“, odobrat stlacením „-“, editovat oznacený retazec stlacením „*“.

Dezinfekcia

Úlohou kontroly súborov (Test - Scan) bolo vyhladat infekciu. Dezinfekcia je funkcia, ktorá je aktivovaná v iba v prípade detekcie vírusov v súboroch a je úzko viazaná na kontrolu na poziadanie alebo neustálu kontrolu. Ak niektorá z týchto metód detekuje vírus, program sa pokúsi súbor dezinfikovat (podla konfigurácie).

V takomto prípade sa zobrazí na monitore upozornenie, ze anti-vírus zistil prítomnost vírusov. Po skoncení danej operácie sa zobrazí na monitore informácia o úspešnosti procesu, ako aj prípadné problémy, ktoré sa mohli pocas neho vyskytnút. Niektoré vírusy, ktorých výskyt je minimálny, nemusia byt daným spôsobom odstránené. V takomto prípade program ponúka moznost daný súbor vymazat alebo zmenit meno napadnutého súboru. Koncovka názvu príslušného súboru sa zmení na `VIR`.

Vírusy môzu byt objavené v pamäti, boot sektoroch diskov alebo v súboroch.

Dezinfekcia boot vírusov

Na dezinfekciu boot vírusov z disku C: vykonajte nasledujúce kroky:

1. Vypnite (reštartujte) pocítac. Vlozte neinfikovanú štartovaciu disketu s operacným systémom do mechaniky (ak chcete pouzit dezinfekciu z CD-ROM, na štartovacej diskete musia byt ovládace k CD-ROM). Ak máte vytvorený SAFEDISK (Záchrannú disketu), pouzite SAFEDISK 1, vytvorený programom SAFEDISK ako štartovaciu.
2. Po reštarte pocítaca spustite riadkovo orientovanú verziu anti-vírusu (PAVCL.EXE):

```
PAVCL C: /CLV
```

alebo:

```
PAVCL /HD0 /CLV
```

Dezinfekcia vírusov v súboroch

Ak sa vyskytli vírusy v súboroch na disku, mozno ich vycistit dodrzaním nasledovného:

- V casti hlavného okna stlacte tlacítko Test/Prípony (Scan/Extens.).Zvolte moznost *Všetky prípony (All extensions), Dezinfikovat súbor (Disinfect)* and *Automatická (Automatická kontrola - Automatic)*.
- V okne Kontrola (Scan – Test) zvolte moznost All Drives (Všetky disky) a spustite kontrolu – Test (Scan). Po skoncení procesu budú všetky súbory dezinfikované (ak to bolo mozné).

Dezinfekcia prostredníctvom neustálej ochrany

Program SENTINEL umoznuje dezinfekciu súborov. Ak pouzívatel aktivuje polozku Automatic (Automatická dezinfekcia), infikované súbory môzu byt dezinfikované bez zásahu pouzívatela.

Riešenie situácie v prípade zistenia vírusu (What to do if a virus is found):

- **Ignorovat** (Ignore) - v prípade napadnutia vírusom program zaznamená do výsledného hodnotenia dané zistenie, ale nevykoná ziadne opatrenia.
- **Dezinfikovat** (Disinfect) - v prípade napadnutia vírusom program dezinfikuje napadnuté súbory, ak je to mozné.
- **Premenovat súbor** (Rename file) - premenovanie infikovaných súborov.
- **Vymazat súbor** (Erase file) - vymazanie infikovaných súborov.

  Ak nie je mozná dezinfekcia súborov (If no disinfection possible):

  - **Premenovat súbor** (Rename file) – premenovanie infikovaných súborov.
  - **Vymazat súbor** (Erase file) – vymazanie infikovaných súborov.

Dezinfekcia pamätovo rezidentných vírusov

Ak máte podozrenie, ze vírus môze byt zavedený v pamäti, vlozte štartovaciu disketu a vypnite (reštartujte) pocítac.

1. Vypnite (reštartujte) pocítac. Vlozte neinfikovanú štartovaciu disketu s operacným systémom do mechaniky (ak chcete pouzit dezinfekciu z CD-ROM, na štartovacej diskete musia byt ovládace k CD-ROM). Ak máte vytvorený SAFEDISK (Záchrannú disketu), pouzite SAFEDISK 1, vytvorený programom SAFEDISK ako štartovaciu.
2. Po reštarte pocítaca spustite riadkovo orientovanú verziu anti-vírusu (PAVCL.EXE):

```
PAVCL /ALL /CLV /AEX /AUT
```

Tento príkaz skontroluje všetky disky v systéme, všetky súbory na nich a pokúsi sa dezinfikovat všetky infikované súbory bez zásahu pouzívatela.

S produktami Panda je dodávaný program, ktorý je riadkovo orientovanou verziou anti-vírusového programu – pavcl.exe.

Program detekuje a dezinfikuje rovnaké mnozstvo vírusov ako ostatné verzie anti-vírusu. Podrobnosti nájdete v dalŠej dokumentácií.

Kontrola prostredníctvom príkazového riadku

S produktami Panda je dodávaný program, ktorý je riadkovo orientovanou verziou anti-vírusového programu – pavcl.exe. Táto sa pouzíva pri štarte pocítaca na kontrolu systému pred tým, ako sa štartuje operacný systém (Windows 95/NT). Je pouzitelná i samostatne ako prostriedok na detekciu a eliminációu vírusov i v prípade, ze Váš operacný systém je nefunkcný. Program detekuje a dezinfikuje rovnaké mnozstvo vírusov ako ostatné verzie anti-vírusu.

PAVCL sa nachádza adresári, kde ste inštalovali anti-vírus. Dalej ho mozno ho nájst na diskete c. 1 verzie pre DOS/Windows 3.x alebo na CD-ROM médiu (adresár DOSWIN3X).

Parametre programu Pavcl

/NOM bez kontroly pamäti
/MEM kontrola pamäti
/NOB bez kontroly BOOT systému
/NOF bez kontroly súborov
/ALL test všetkých diskov v pocítaci
/LOC test lokálnych diskov
/ITW test "In the wild" vírusov
/NBR zákaz prerušenia cinnosti programu s ESC alebo Ctrl-Break
/INVA vyhladávanie neznámych vírusov na diskete A:
/INVB vyhladávanie neznámych vírusov na diskete A:
/CLV odstránenie nájdených vírusov
/LIS zoznam vírusov, ktoré sú známe tejto verzií
/SAV ulozí parametre do súboru
/NSB bez kontroly vnorených podadresárov
/PTH test adresárov špecifikovaných v DOS (resp. Windows) PATH
/ISO izolácia
/HEU aktivácia heuristickej analýzy
/CMP hladanie vírusov v komprimovaných súboroch typu ZIP, ARJ, LZEXE, MS Compress
/NOS bez zvukového upozornenia
/AEX test všetkých súborov nezávisle od ich prípon
/AUT test bez zásahu pouzívatela
/OVR prepísat pred odstránením
/NOR bez vytvorenia záznamu o kontrole
/ENG po anglicky
/MSF:meno_súboru - výpis textového súboru, v ktorom môzu byt informácie a inštrukcie pre pouzívatela
/CDR

Ockovanie: /xyz
x: F alebo B z 'F'ile (súbor) alebo 'B'oot
y: I alebo E z 'I'nternal (interné) alebo 'E'xternal (externé). Parameter je nepovinný.
z: '+' pridat, '-' odstránit or '*' overit ockovanie
Napr.: /FI+ príkaz pridá internú vakcínu do súborov
/B+ príkaz pridá internú a externú vakcínu do súborov

Parametrom “/?” si mozno zobrazit uvedené parametre.
Programom PAVCL mozno kontrolovat nasledujúce casti systému:

- Kontrola pamäti.
- Kontrola boot sektorov.
- Kontrola súborov.

Implicitne sú nastavené tieto parametre:

- Kontrola podadresárov.
- Bez dezinfekcie.
- Zvukové efekty.
- Kontrola len spúštatelných súborov.
- Záznam kontroly a vytvorenie hlásenia a vykonanej kontrole (Results file).

Ak spustíte program pavcl.exe s parametrami “/?”, “/LIS” alebo ”/INVx”, ziadna iná funkcia programu nebude aktivovaná. Po skoncení zadanej úlohy sa program vráti do DOS-rezimu.

Cesta (cesty) sa pod DOS-om uvádzajú podla nasledovného syntaxu:

```
[DISK:]\[CESTA][MENO_SUBORU]
```

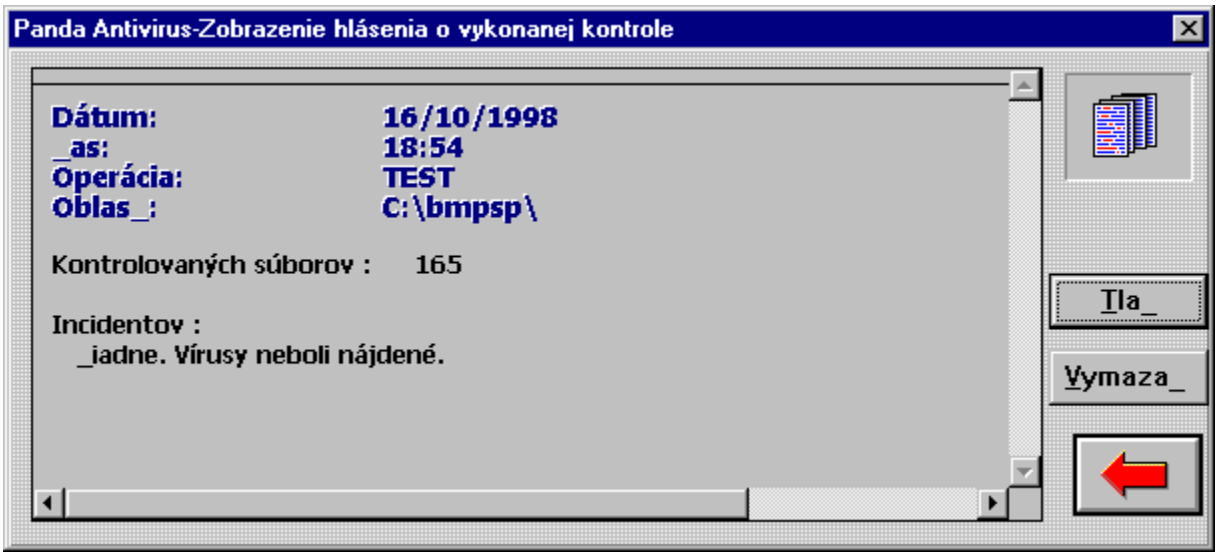
Hlásenia o vírusových infekciách

Aktiváciou tlacítka **Hlásenia** (Reports) sa zobrazí zoznam anti-vírusom vykonaných operácií a ich vyhodnotenie. V hlásení sú všetky typy operácií, cas vykonania, priebehu a rozlicných udalostí v priebehu kontroly a dezinfekcie, napríklad ci boli vírusy nájdené a kde boli nájdené. Tento súbor je ulozený na disku a kedykolvek si mozno jeho obsah pripomenút alebo vytlacit.

Obsah súboru mozno sledovat nasledujúcimi spôsobmi:

§ kliknutím na polozku **Hlásenia** (Reports) v hlavnom okne programu (panel nástrojov)
§ vyhladaním v hlavnom roletovom menu (Súbor (File)/ Vyhodnotenie kontroly (Results))
§ vyhladaním súboru ap.rpt v adresáry, v ktorom je inštalovaný anti-vírus

Všetky operácie programu sa chronologicky zaznamenávajú v tomto súbore.



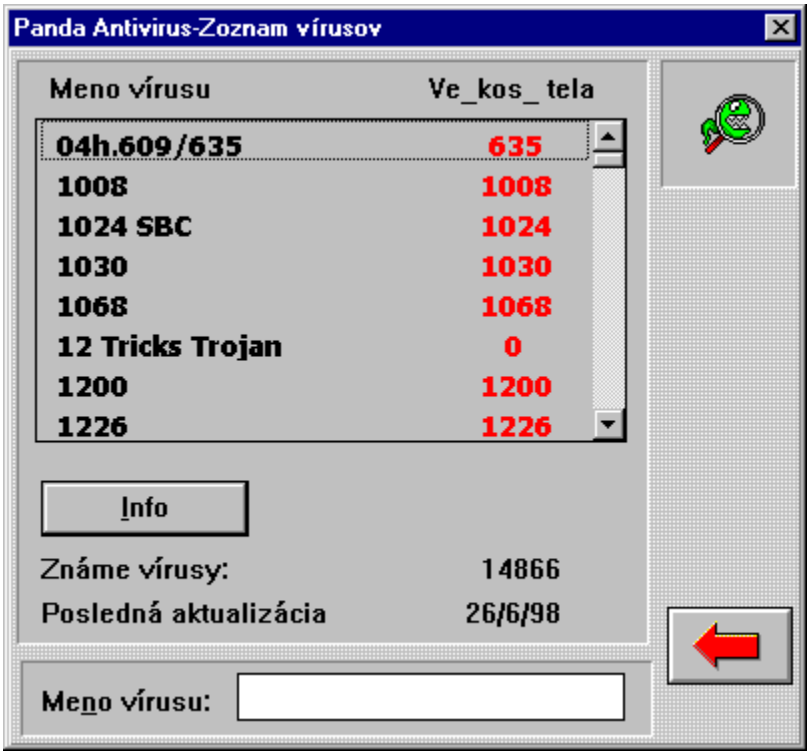
Do súboru sa zaznamenávajú nasledovné operácie alebo údaje:

- Dátum a Cas kontroly (Date and time)
- Vykonaný proces (Operation)
- Oblast, v ktorej bola operácia vykonaná (Area)
- Pocet kontrolovaných súborov (Files checked)
- Pocet vírusových konfliktov (Incidents)

Informácie sa zaznamenávajú do vyhodnotenia kontroly ak v všeobecných parametroch kontroly je aktivovaná polozka *Save results* (Ulozit hlásenie)

Vyhodnotenie kontroly mozno kedykolvek vytlacit (Print) alebo vymazat (Erase). Pred tlacou súboru je nevyhnutné pripravit tlaciaren.

Zoznam vírusov



V tejto casti programu si mozno zobrazit aktuálnu databázu všetkých známych vírusov (Virus Report) a informácie o nich (dvojitým poklikaním alebo stlacením klávesy Enter na názov zvolené vírusu).

V zozname vírusov (Zoznam vírusov - Virus List) sú uvedené všetky známe vírusy a ich pocet (Total). Zoznam obsahuje informácie o mene (Name) a velkosti tela vírusu (Size).

Ak chcete vyhladat špecifický vírus podla jeho názvu, vpíšte zaciatocné písmená jeho mena do casti okna Meno vírusu (Name) a pomocou šípok ho vyhladajte. V zozname vyznacte ziadaný vírus a stlacte Enter (alebo dva krán nan poklikajte).

Okno Podrobné informácie o víruse (Virus Information) obsahuje nasledovné informácie o víruse: Meno (Name), Pôvod (Source), Velkost (Size), Vlastnosti (Characteristics) (Rezidentný - Resident, Maskovaný - Stealth, Kódovaný - Encrypted, Prepisujúci - Overwrites, Polymorfný - Polymorfic), Dátum -prvá lokalizácia (resp. vzniku) (Date) a informáciu, ktoré typy súborov alebo casti PC napáda - Infikuje (Infects) - (Tabulka partícií disku - Partition table, Boot sektory - Boot sectors, *.COM, *.EXE, COMMAND.COM, *.SYS, Dalšie súbory (Other files). V okne je aj informácia o moznej dezinfekcií – Mozno dezinfikovat (Disinfection possible).

Typy vírusov

Rezidentný - Resident: - rezidentný vírus v pamäti - pocas behu pocítaca si vírus rezervuje cast pamäti a obsadí ju. Infikuje ostatné spustené programy.

Maskovaný - Stealth: Túto techniku vyuzívajú niektoré rezidentné vírusy. Technika pozostáva z maskovania prítomnosti vírusu pred pouzívatelom. Vírus zakrýva akúkolvek zmenu komponentov systému, napríklad dátum, cas, dlzku súboru, zmenu zavádzacieho sektoru. Vírus simuluje neinfikované prostredie operacného systému a predkladá systému údaje, ktoré zodpovedajú správaniu

neinfikovaného systému. Ak sa napríklad vyskytne poziadavka na cítanie sektoru, kde si však vírus ulozil svoje telo, vírus presmeruje poziadavku na miesto, kde sa momentálne nachádza obsah originálneho sektoru. Systému sa však javí všetko v poriadku. Podmienka existencie stealth vírusov je ich zavedenie v operacnej pamäti. Ak pouzívatel naštartuje systém z cistej diskety, nemôze dôjst k aktivácii vírusu, ktorý je ulozený na pevnom disku.

Kódovaný - Encryption: Tieto typy vírusov sa bránia detekcií tým spôsobom, ze ziadna z kópii vírusového tela nie je rovnaká (kódovanie tela vírusu). Tieto druhy vírusov nemozno vyhladat prostredníctvom metódy, ktorá vyhladáva retazce, ktoré zodpovedajú urcitému vírusu. Naštastie vírus potrebuje aj dekódovacie rutiny, ktoré mu umoznia dekódovanie do pôvodnej podoby. Tieto rutiny mozno vyhladat a zabránit šíreniu vírusov.

Prepisujúci - Overwrites: Tieto vírusy môzu byt rezidentné i nerezidentné. Premazávajú casti súborov, ktoré infikovali a to bud vlastným telom alebo "zhlukmi" retazcov, ktoré narúšajú pôvodnú štruktúru programu. Dlzka súboru sa však nemení. Tým sa stáva súbor nepouzitelný. Jediná moznost dezinfekcie je vymazat takýto súbor a nahradit ho neinfikovaným. Anti-virus však musí zabezpecit úplnú likvidáciu a prevenciu voci takýmto vírusom v celom pocítaci.

Polymorfný - Polymorphic: Polymorfné vírusy sú "zveladené" samokódované (Encryption) vírusy. Tieto vírusy sa bránia voci antivírusovej kontrole tým, ze ziadne dve kópie ich vírusového tela nie sú totozné. Tým je úplne obmedzená kontrola prostredníctvom metódy, ktorá vyhladáva retazce, ktoré zodpovedajú urcitému vírusu. Vírus je zvycajne tvorený dekódovacou rutinou, ktorá dekóduje zakódované telo vírusu v pamäti po jeho spustení. Úvodná dekódovacia rutina však umoznuje v prípade semipolymorfných vírusov jeho lokalizáciu (pouzívajú statickú dekódovaciu rutinu). Plne polymorfné vírusy majú aj dekódovacie rutiny generované rôznymi spôsobmi, pricom aj dlzka týchto rutín môze byt rôzna. Vírus dalej môze svoje telo rozdelit na niekolko castí, ktoré sú náhodne umiestnované do súboru, co stazuje jeho detekciu.

Hlavné funkcie programu

Prostredníctvom tohto obrázku mozno zobrazovat informácie o rôznych prvkoch hlavného okna. Stací nastavit kurzor myši na príslušnú aktívnu oblast a aktivovat ju.