Introduktion

Panda Antivirus

Panda Antivirus är en komplett och effektiv lösning för att hålla Din dator fri från alla typer av virus. Versioner av programmet för Windows 95/98, Windows NT Workstation, Windows 3.1x, DOS och OS/2 är inkluderade för att skydda Dig oavsett vilket operativsystem Du har. Hjälpen relaterar till **Panda Antivirus** för Windows 95/98.

Skyddsstrategier

Panda Antivirus innehåller flera typer av skydd mot virus:

- **Permanent skydd:** det permanenta skyddet svarar för att skydda Din dator hela tiden och kräver inget ingripande från användaren. Den stora fördelen med denna skyddsstrategi är att den skyddar Din dator helt automatiskt.
- **Manuell analys:** den manuella analysen låter Dig analysera alla områden på datorn när som Du så önskar. Välj bara område/enhet och programmet börjar genast analysera innehållet på jakt efter virus.
- **Borttagning:** när ett virus upptäcks finns det flera handlingsalternativ. Ett av dessa är borttagning (desinfektion) som innebär att programmet tar bort viruset från filen och lämnar den precis som den var innan den blev smittad.
- **Heuristisk analys:** den heuristiska analysmetoden är en alternativ analysmetod till de redan nämnda. Heuristisk analys sker på användarens begäran. Användaren måste ange vilket område som skall analyseras. Metoden inriktar sig på att upptäcka nya och okända virus.
- **Strängsökning:** precis som heuristisk analys är detta en alternativ analysmetod som sker på användarens begäran. Den används för att söka efter nya virus enligt data som tillhandahållits av Panda Softwares tekniska support.
- **Övriga fördelar:** Under denna rubrik har vi samlat vissa utmärkande funktioner hos programmet som är konstruerade för att ge information eller för att underlätta handhavandet av programmet. Som exempel kan vi nämna att det finns en rapportfil där Du kan se information om olika virusincidenter och uppgifter som utförts med antiviruset.

Panda Software Antiviruslösningar

Panda Software erbjuder följande antiviruslösningar:

- **24h-365d® Antivirus Insurance® för fristående PC**. Licenser.
- **24h-365d® Antivirus Insurance® för PC i nätverk** (automatisk distribution från servern).
- **24h-365d® Antivirus Insurance® för nätverksservrar** (Novell NetWare och Windows NT*).*
- **24h-365d® Antivirus Insurance® för lokala nätverk (Local Area Networks)**.
- **24h-365d® Antivirus Insurance® för e-mail- och Groupware-klienter**.
- **24h-365d® Antivirus Insurance® för e-mail- och Groupware Servers.**
- **24h-365d® Antivirus Insurance® för SMTP mailservrar.**
- **24h-365d® Antivirus Insurance® för PC anslutna till Internet.**
- **24h-365d® Antivirus Insurance® för Internet-servrar** (SMTP, FTP och HTTP).
- **24h-365d® Antivirus Insurance® för proxy-servrar.**

Vad är 24h-365d® Panda Software Antivirus Insurance®?

24h-365d® Panda Software Antivirus Insurance® är nytt och revolutionernade koncept för antivirusskydd som erbjuder Dig högsta möjliga säkerhet. **24h-365d® Panda Software Antivirus Insurance®** är en ypperlig kombination av produkter och service som erbjuder de högsta nivåerna av virusskydd. **24h-365d® Panda Software Antivirus Insurance®** kan köpas med olika licenstid och antal uppdateringar.

Produktens namn är **Panda Antivirus**, ett antivirus som har erhållit de mest krävande certifieringarna för denna typ av produkter, inkluderande:

- **ICSA:** beviljas av det ansedda amerikanska ICSA (International Computer Security Association) till antivirusprodukter som återkommande upptäcker 100% av *In the Wild*-viruses (de vanligast förekommande virusen vid varje givet tillfälle) och mer än 90% av virusen i *Zoo Collection* (en samling av tusentals mindre kända virus).

- **CheckMark:** beviljas av den brittiska datasäkerhetstidningen *Secure Computing*.

Om Du inte redan har **24h-365d® Panda Software Antivirus Insurance®**, kan Du beställa det med hjälp av formuläret på registreringskortet. Servicen som ingår i **24h-365d® Panda Software Antivirus Insurance®** är följande:

- **Hot-Line:** under ETT år, löser vi Dina virusproblem via telefon, fax, Internet och e-mail. När Du än ringer, dag som natt, kommer Du att få tala med mycket kvalificerad personal helt till Din tjänst 24 timmar om dygnet, 365 dagar om året. Detta är en exklusiv **Panda Software**-service.

- **S.O.S. Virus:** Om Du upptäcker ett virus som **Panda Antivirus** inte upptäcker eller tar bort kommer vi på snabbast möjliga sätt att inhämta ett prov på det nya viruset och inom 24 timmar ta fram en ny version som klarar av att upptäcka och ta bort viruset. Vi kommer sedan att skicka Dig den nya versionen helt utan kostnad.

- **Uppdateringar levereras direkt:** Ditt antivirus kommer alltid att uppdateras. Du får till angiven postadress varje månad eller kvartal uppdateringar på CD eller disketter om Du köpt vår **24h-365d® Panda Software Antivirus Insurance®**. Du kan också uppdatera produkten via vår WEB-sida så ofta du önskar under ett år, med löfte om minst en uppdatering varje dag.

- **WEB Service:** virusinformation och svar på de vanligaste frågorna.

Installation

Systemkrav

För att installera **Panda Antivirus** för Windows 95/98, krävs följande:

- IBM-kompatibel dator med minst 386-processor.
- 4 MB RAM.
- 4 MB hårddiskutrymme.
- Windows 95 eller högre.
- Mus.

Installationsprocedur

Panda Antivirus för Windows 95/98 levereras både på disketter och CD-ROM. För att installera från diskett sätter Du i disk 1 av **Panda Antivirus** och kör SETUP-programmet.

För att installera från CD-ROM, kör Du programmet CDMENU.COM. Progammet ger Dig en enkel meny att välja från. Först måste Du välja önskat språk och sedan vilken version Du önskar installera. I det här fallet väljer Du **Panda Antivirus** för Windows 95/98. Du skall alltid installera den version som motsvarar Ditt operativsystem, då varje version är speciellt utformad för att fungera med respektive operativsystem.

Installationsproceduren består av följande steg:

1. Först visas en välkomstbild.
2. Som steg två får Du möjlighet att analysera minnet och/eller hårddisken för att vara säker på att systemet är fritt från virus och att installationen blir riktigt gjord.
3. Du skall sedan skriva in Ditt namn och företag.
4. Du får en fråga om i vilken katalogen programmet skall installeras.
5. Du får sedan en fråga om vad programgruppen med ikonerna på Start-menyn skall kallas.
6. Du får möjlighet att installera det permanenta skyddet (**Sentinel**). Du kan också välja om Du vill att programmet skall analysera datorn vid uppstart.
7. Kopieringen av filer till hårddisken påbörjas.
8. När filerna är kopierade får Du möjlighet att skapa två reparationsdisketter, mycket användbara för att ta bort boot-virus eller i situationer när ett virus har upptäcks i minnet. Den första disketten som **Safedisk** skapar är en bootdiskett. Den andra innehåller **Pavcl**, vårt kommandoradsprogram. Vi rekommenderar bestämt att Du utnyttjar **Safedisk** för att skapa dessa disketter.
9. När disketterna är klara blir Du rekommenderad att starta om datorn för att aktivera det permanenta skyddet.

Uppdatera antiviruset

För att uppdatera den nuvarande versionen med den uppdatering Du får, installerar Du helt enkelt den nya över den gamla.

Avinstallation

Avinstallationen av **Panda Antivirus** görs med *Lägg till/Ta bort program* i *Kontrollpanelen*. Markera **Panda Antivirus Windows 95/98** från listan av program och klicka på *Lägg till/Ta bort*. För att slutföra avinstallationen måste Du starta om datorn.

Försök inte att avinstallera genom att radera mappen som programmet installerades i. Använd alltid metoden som beskrivs ovan.

Vad är permanent skydd?

Permanent skydd är ett program som så fort datorn startas, övervakar alla processer som riskerar att sprida virus för att därigenom garantera att inga virus kommer in i systemet.

Det permanenta skyddet är helt automatiskt och kräver inget ingripande från användaren. Trots den ständiga övervakningen påverkas inte systemets prestanda. Installation av det permanenta skyddet är därför alltid att rekommendera då det ökar säkerhetsnivån avsevärt.

Hur man använder det permanenta skyddet

Permanent skydd är ett av alternativen när Du installerar. Om Du markerar det alternativet kommer det permanenta skyddet (**Sentinel**) att laddas så fort Du startar datorn.

Sentinel visas som en ikon bredvid klockan på Aktivitetsfältet. Genom att dubbelklicka på den öppnas ett fönster där Du kan konfigurera hur **Sentinel** skall arbeta.

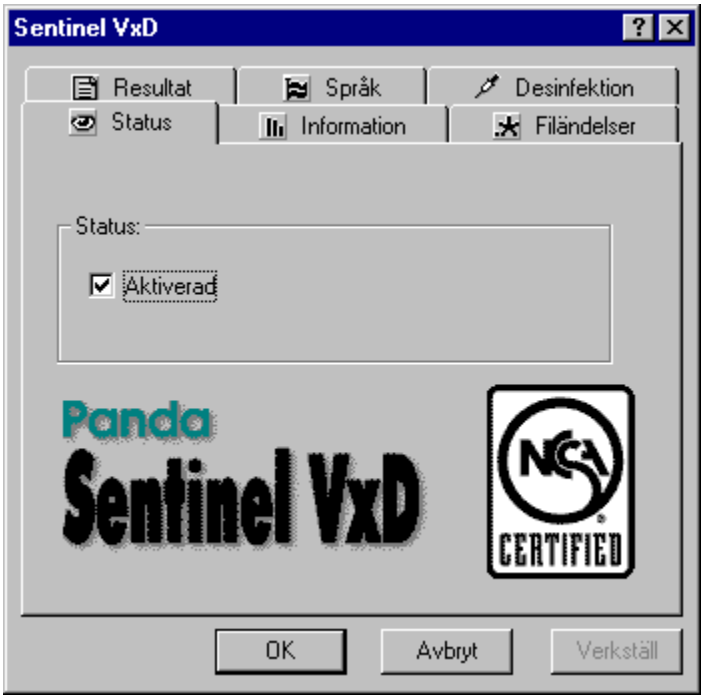
Det permanenta skyddet arbetar helt automatiskt. Om ett virus upptäcks vid en speciell operation kommer **Sentinel** att varna Dig om detta och vidta lämplig åtgärd.

Hur man ställer in det permanenta skyddet

Det permanenta skyddet kan ställas in (konfigureras) för att passa användarens behov. Genom att dubbelklicka på **Sentinel**-ikonen öppnas ett fönster med ett antal flikar. Varje flik hör till en speciell del av **Sentinels** konfiguration. Alternativen för inställningarna är följande:

Status

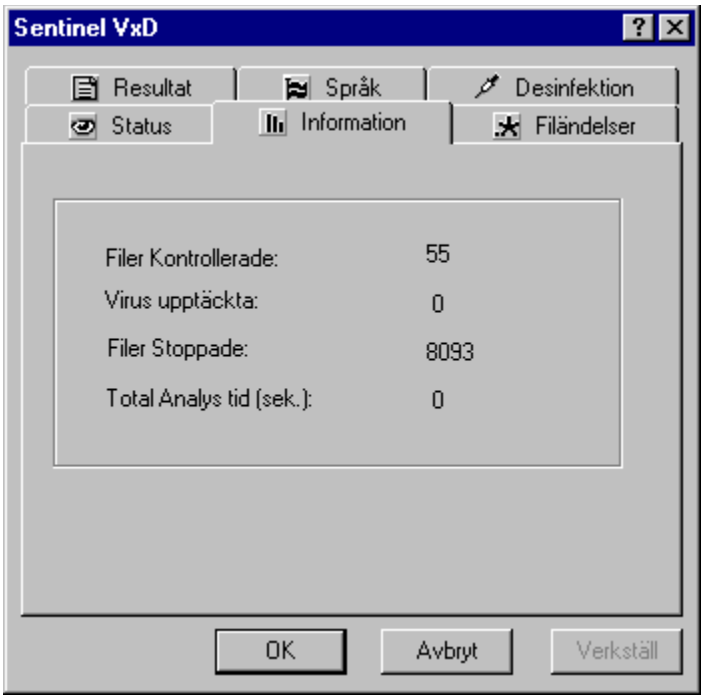
Denna flik visar statusen på det permanenta skyddet.



- **Aktiverad:** Detta alternativ låter Dig aktivera eller avaktivera det permanenta skyddet. Tänk på att om Du avaktiverar det permanenta skyddet kommer datorn att vara oskyddad mot virus.

Information

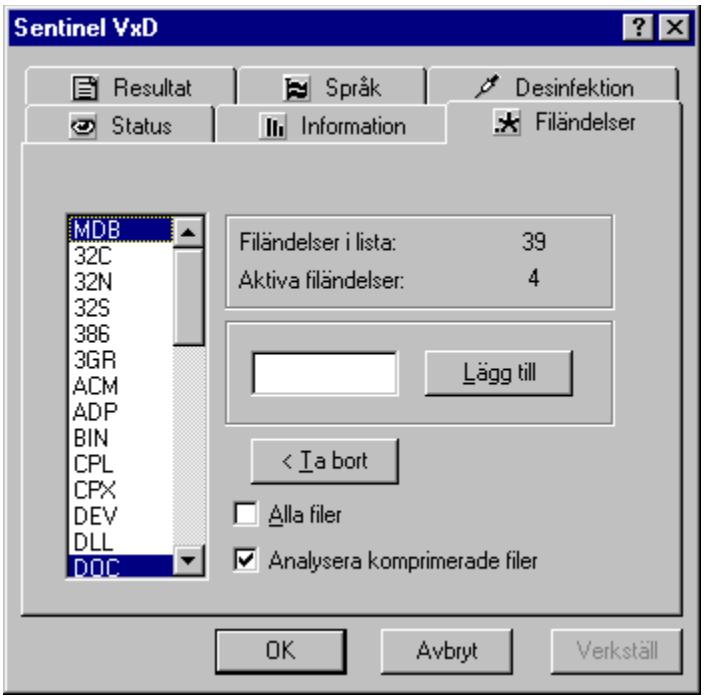
Denna flik visar diverse information om aktiviteten på det permanenta skyddet.



- **Analyserade filer:** Här visas antalet filer som analyserats av det permanenta skyddet sedan datorn startades.
- **Upptäckta virus:** Här visas antalet virus som upptäckts.
- **Övervakade filer:** Här visas antalet filer som övervakats av **Sentinel** sedan datorn startades.
- **Total analystid:** Här visas den totala tid som **Sentinel** använt för att analysera filerna.

Filändelser

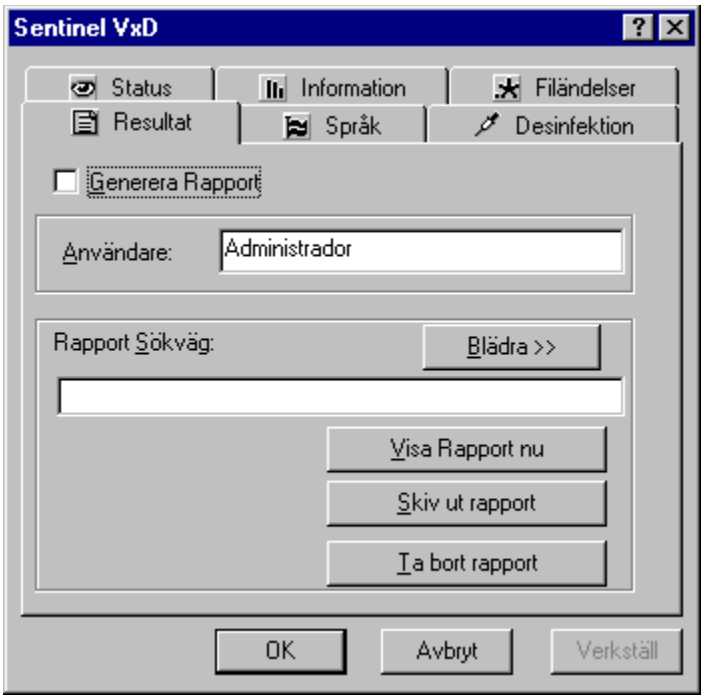
Denna avdelning låter Dig ställa in vilka filtyper som det permanenta skyddet skall analysera.



- **Lista på filtyper:** I listan över filtyper kan Du markera så många filtyper som Du önskar analysera. Det permanenta skyddet övervakar alla filer som öppnas, men kommer bara att analysera de filer vilkas filändelser är markerade i listan. Förutom de markerade filtyperna analyseras alltid COM- och EXE-filer.
- **Filändelser i lista:** Siffran motsvarar antalet filändelser i listan.
- **Aktiva filändelser:** Här visas antalet markerade filändelser.
- **Lägg till:** För att lägga till en filändelse till listan, skriver Du in ändelsen i rutan och klickar på *Lägg till*.
- **Ta bort:** För att ta bort en filtyp ur listan, markerar Du filändelsen och klickar på *Ta bort*.
- **Alla filer:** Om detta alternativ är markerat, kommer alla filer att analyseras oavsett vilken filtyp det är.
- **Analysera komprimerade filer:** Om detta alternativ är markerat kommer alla komprimerade filer som öppnas att analyseras.

Resultat

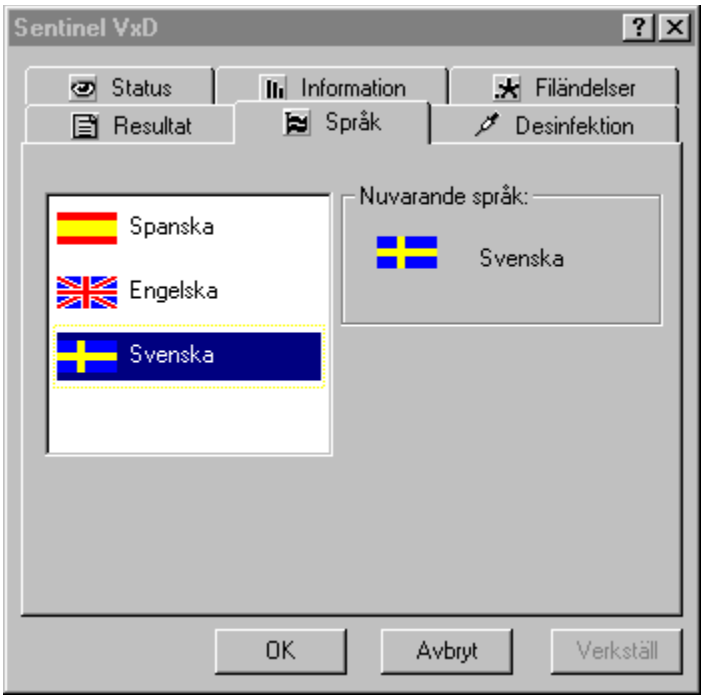
Här kan Du ställa in hur det permanenta skyddet skall hantera rapportfilen.



- **Skapa rapport:** Om detta alternativ är markerat, kommer en rapport att skapas med de olika incidenter som det permanenta skyddet upptäckt.
- **Användare:** Datorns användares namn visas här.
- **Rapport Sökväg:** Den här rutan låter Dig ange var Du vill att rapporten skall sparas.
- **Bläddra:** Knappen *Bläddra* låter Dig söka efter önskad plats för rapportfilen. Den valda platsen visas i rutan *Rapport Sökväg*.
- **Visa rapport nu:** Knappen visar Dig rapporten med hittills påträffade incidenter.
- **Skriv ut rapport:** Knappen låter Dig skriva ut rapporten.
- **Ta bort rapport:** Knappen låter Dig radera rapporten.

Språk

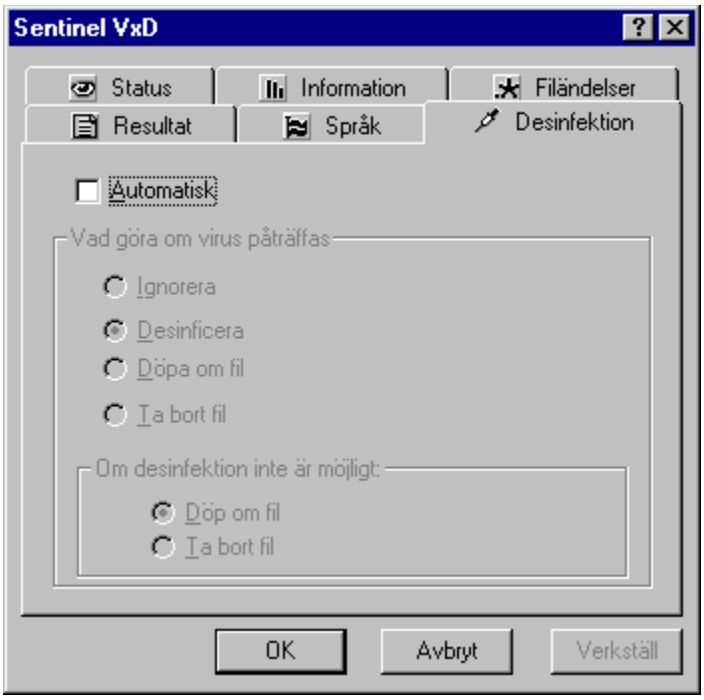
Du kan se vilket språk det permanenta skyddet för närvarande använder samt välja ett annat språk från listan över tillgängliga språk.



- **Tillgängliga språk:** En lista visas över de olika tillgängliga språken för det permanenta skyddet. För att välja ett språk markerar Du det i listan och klickar på *OK* eller *Verkställ*.
- **Nuvarande språk:** Här visas vilket språk det permanenta skyddet för närvarande använder.

Desinfektion

Denna flik låter Dig konfigurera hur borttagningen av virus sker med det permanenta skyddet.

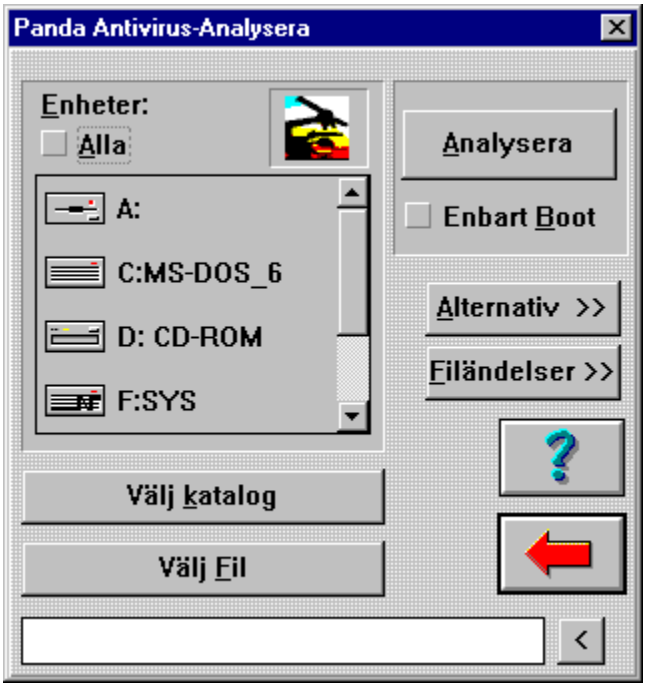


- **Automatisk:** Om detta alternativ är markerat kommer borttagningen av virus att ske automatiskt. Om **Sentinel** upptäcker ett virus och är inställd på automatik kommer programmet inte att varna när det upptäcker ett virus utan att reagera så som det är konfigurerat. Om Du har ställt in **Sentinel** på Desinfektion kommer filkommandot att avbrytas och filen desinficeras. På så sätt kommer filen nästa gång den skall öppnas att vara virusfri och kommandot kan utföras utan problem.
- **Ignorera:** Om detta alternativ är markerat kommer programmet inte att göra någonting om det upptäcker ett virus.
- **Desinfektion:** Om detta alternativ är markerat och det permanenta skyddet upptäcker ett virus kommer programmet att desinficera den smittade filen och lämna den i samma skick som den var innan den blev smittad.
- **Byt namn:** Om detta alternativ är markerat och ett virus upptäcks kommer **Sentinel** att byta namn på filen genom att ge den ändelsen VIR.
- **Ta bort fil:** Om detta alternativ är markerat och **Sentinel** upptäcker ett virus i en fil kommer filen att tas bort.
- **Om borttagning ej möjlig, byt namn:** Om detta alternativ är markerat och **Sentinel** upptäcker ett virus som inte kan tas bort tillfredsställande kommer filen att döpas om.
- **Om borttagning ej möjlig, ta bort fil:** Om detta alternativ är markerat och **Sentinel** upptäcker ett virus som inte kan tas bort tillfredsställande kommer filen att tas bort.

Vad är manuell analys?

Den manuella analysen låter Dig när som helst undersöka valfritt område på datorn. Alla dessa analyser kan konfigureras genom en serie med enkla alternativ.

Hur man använder den manuella analysen



För att genomföra en manuell analys gör man följande:

1. **Starta programmet:** För att starta programmet går man till programgruppen som innehåller ikonen för antiviruset (*Start: Program: Panda Antivirus Windows 95 & 98*). Klicka på *Panda Antivirus*-ikonen.
2. **Gå till analyssektionen:** För att komma dit klickar Du på *Analys*-knappen i knappraden. Ett fönster öppnas där Du kan bestämma vad som skall analyseras och hur det skall göras.
3. **Välj område:** Du måste välja vilket område som skall analyseras. De enheter som är anslutna till systemet visas i en lista. Du kan också välja en speciell katalog eller fil genom att använda respektive knappar.
4. **Ställa in filtyper/-ändelser:** Detta är ett valfritt alternativ. Programmet sparar inställningarna för de filtyper Du önskar analysera. Därför behöver Du bara göra dessa inställningar en gång.
5. **Ställa in alternativ för analys:** Detta är också ett valfritt alternativ. Programmet sparar inställningarna för dessa alternativ. Därför behöver Du inte upprepa detta mer än en gång. Konfigurationen behöver bara ändras då Du vill välja andra alternativ. En mer ingående beskrivning av dessa alternativ finns i dokumentationen till avsnittet om konfiguration.
6. **Markera om Du endast vill analysera boot-sektorn:** Detta är ett valfritt alternativ. Om Du markerar detta alternativ kommer endast boot-sektorn på de markerade enheterna att analyseras, inte filerna. Om detta alternativ inte är markerat kommer både boot-sektorn och filerna på de markerade enheterna att analyseras.
7. **Påbörja analysen:** Knappen *Analysera* påbörjar en analys av de valda områdena i enlighet med de alternativ Du har valt.

Hur man konfigurerar en manuell analys

Som nämnts tidigare måste följande uppgifter anges för en analys:

- Vilket område Du vill analysera.
- Vilka filtyper som skall analyseras.
- Hur analysen skall utföras.

Konfigurationen av en analys tar hänsyn till de filtyper som har valts samt alternativen för analys.

Filtyper

Genom att klicka på knappen *Filtyper* öppnar Du ett fönster där Du kan markera vilka filtyper Du vill analysera.

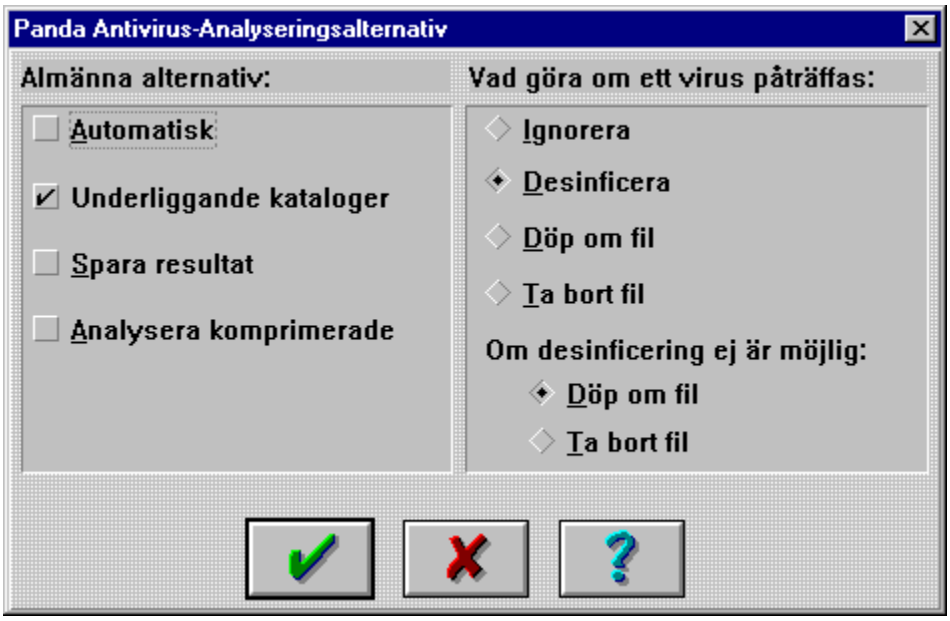
Genom att markera rutan *Alla* ovanför listan på filtyper kommer alla filer oavsett filtyp att analyseras. Om rutan inte är markerad kommer endast de filtyper som är markerade i listan att analyseras.

Två knappar låter Dig lägga till och ta bort filtyper ur listan. Förinställt så innehåller listan de vanligaste filtyperna såväl som ett urval av de filtyper som oftast innehåller virus.

Förutom de filtyper Du väljer kommer COM- och EXE-filer alltid att analyseras.

Analysalternativ

Genom att klicka på knappen *Alternativ* öppnar Du ett fönster där Du göra följande inställningar:



- **Automatisk:** Om detta alternativ är markerat kommer analysprocessen att gå helt automatiskt. Om ett virus upptäcks kommer Du att få en varning om detta, men processen kommer att fortgå utan avbrott. Detta är framför allt användbart om datorn innehåller många smittade filer.
- **Underkataloger:** Om detta alternativ är markerat kommer programmet att analysera filer även i underkataloger till de enheter Du har valt. Om rutan inte är markerad kommer endast filer i enhetens rotkatalog att analyseras.
- **Spara resultat:** Om detta alternativ är markerat kommer informationen från analysen att sparas i en resultatfil.
- **Analysera komprimerade filer:** Om detta alternativ är markerat kommer alla komprimerade filer att analyseras.
- **Ignorera:** Om detta alternativ är markerat och ett virus upptäcks kommer programmet att varna men inget mer.
- **Desinficera:** Om detta alternativ är markerat och ett virus upptäcks kommer programmet att försöka ta bort viruset.
- **Byt namn:** Om detta alternativ är markerat och ett virus upptäcks kommer programmet att döpa om filen med ändelsen VIR.
- **Ta bort:** Om detta alternativ är markerat och ett virus upptäcks kommer programmet att ta bort den smittade filen.
- **Om desinfektion ej är möjlig, byt namn:** Om detta alternativ är markerat och ett virus upptäcks som programmet ej kan ta bort, kommer filen att döpas om.
- **Om desinfektion ej är möjlig, ta bort:** Om detta alternativ är markerat och ett virus upptäcks som programmet ej kan ta bort, kommer filen att tas bort.

Vad är en heuristisk analys?

Heuristisk analys är en kompletterande analys utformad för att upptäcka okända virus.

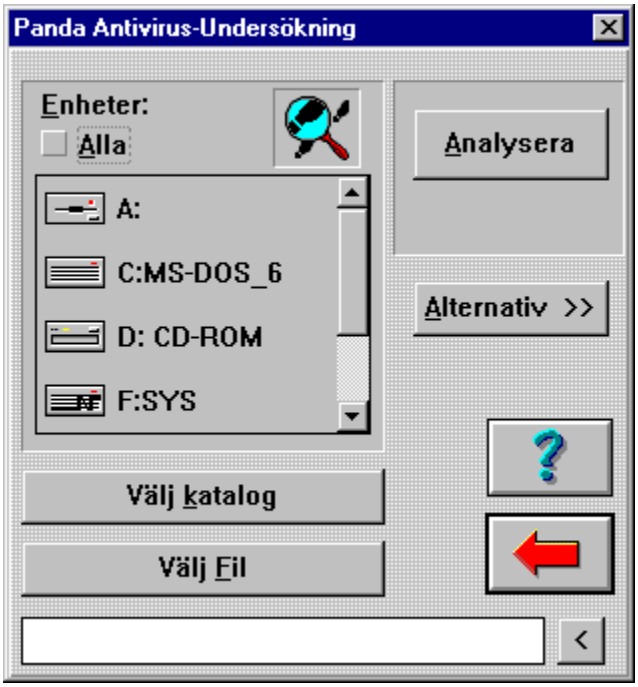
På samma sätt som den vanliga manuella analysen, sker analysen direkt och på användarens begäran. Metoden som används är dock helt annorlunda från den som används vid den vanliga analysen. Den senare försöker hitta virus som programmet känner igen, medan den heuristiska analysen försöker upptäcka virus utifrån kriterier eller generella kännetecken för virus.

Eftersom den heuristiska analysen endast kan misstänka att det finns virus i en fil, men inte har tillräckligt kunskap om viruset, är det inte möjligt att ta bort det.

Det är viktigt att inse att den heuristiska analysen endast är ett komplement till den vanliga analysen.

Arbetsgången för den heuristiska analysen liknar den för vanlig analys.

Hur man använder den heuristiska analysen



För att utföra en heuristisk analys, gör man följande:

1. **Starta programmet:** För att starta programmet, går Du till programgruppen som innehåller ikonen för Panda Antivirus (*Start: Program: Panda Antivirus Windows 95 & 98*). Klicka på ikonen.
2. **Gå till avdelningen för heuristisk analys:** För att komma till dit klickar Du på knappen *Undersök* i knappraden. Ett fönster öppnas där Du kan välja område och alternativ.
3. **Välj område:** Du måste välja vilket område som skall undersökas. De tillgängliga enheterna visas i en lista. Du kan även välja en speciell katalog eller fil med hjälp av respektive knappar.
4. **Konfigurera alternativen för heuristik:** Detta alternativ är valfritt. Programmet sparar inställningarna för heuristisk analys, så detta behöver Du bara göra en gång. Det är alltså endast när Du behöver ändra inställningarna som Du går in i den här menyn. Alternativen beskrivs mer ingående i dokumentationen till avdelningen för konfiguration.
5. **Påbörja analysen:** Med knappen *Analysera* startar Du en heuristisk analys på de valda enheterna för att upptäcka tecken på virus.

Hur man konfigurerar den heuristiska analysen

Som vi nämnt måste följande uppgifter anges för den heuristiska analysen:

- Vilket område Du önskar undersöka.
- Hur undersökningen skall utföras.

Konfigurationen av den heuristiska analysen beror på vilka alternativ som är markerade.

Alternativ för analys

Genom att klicka på knappen *Alternativ* öppnar du ett fönster som låter göra följande inställningar:

- **Minimum-nivån:** Om detta alternativ är valt kommer känsligheten att vara mycket låg, d v s endast filer som med hög sannolikhet innehåller virus kommer att markeras som misstänkta.
- **Medium-nivån:** Om detta alternativ är valt kommer känsligheten att vara medel. Härigenom kommer endast de filer som troligtvis innehåller virus att markeras som misstänkta.
- **Maximum-nivån:** Om detta alternativ är valt kommer känsligheten att vara mycket hög. Detta innebär att alla filer som verkar innehålla virus markeras som misstänkta. Även på denna nivå kommer dock chansen att en ren fil markeras som misstänkt att vara minimal.
- **Rapportera inkorrekt datum och tid:** Om detta alternativ är valt kommer Du att få en varning varje gång programmet upptäcker en fil med felaktigt datum/tid.
- **Rapportera komprimerade filer:** Om detta alternativ är valt kommer Du att informeras varje gång programmet upptäcker en komprimerad fil.
- **Rapportera vaccinerade filer:** Om detta alternativ är valt kommer Du att informeras varje gång programmet upptäcker en vaccinerad fil.

Vad är strängsökning?

Den manuella analysen letar efter virus som programmet har i sin databas. Då det dagligen kommer nya virus blir denna metod gradvis inaktuell.

Strängsökning använder samma metod som den manuella analysen, men låter Dig skriva in en söksträng (en del av ett virus) för programmet. **Panda Software** tekniska support kan på så sätt bistå Dig med en söksträng som matchar ett nytt virus och få programmet att upptäcka viruset även om det inte har någon annan information om det.

Liksom den manuella analysen är strängsökningen omedelbar och utförs på användarens begäran.

Hur man använder strängsökningen

För att utföra en strängsökning, gör Du följande:

1. **Starta programmet:** För att starta programmet, går Du till programgruppen som innehåller ikonen för Panda Antivirus (*Start: Program: Panda Antivirus Windows 95 & 98*). Klicka på ikonen.
2. **Gå till avdelningen för strängsökning:** För att komma till dit klickar Du på knappen *Sök* i knappraden. Ett fönster öppnas där Du kan ställa in vad som skall undersökas och hur det skall göras.
3. **Välj område:** Du måste välja ett område för strängsökningen. De tillgängliga enheterna visas i en lista. Du kan även välja en speciell katalog eller fil med hjälp av respektive knappar.
4. **Markera de strängar Du vill söka efter:** Skriv in de strängar Du vill att programmet skall söka efter eller välj redan inmatade strängar från en lista. Då programmet sparar angivna strängar behöver Du inte skriva in samma sträng mer än en gång.
5. **Starta sökningen:** Knappen *Sök* startar sökningen efter de valda strängarna i de valda områdena. Genom att klicka på knappen *Genomsök minnet* söker programmet efter strängarna i minnet.

Hur man konfigurerar strängsökningen

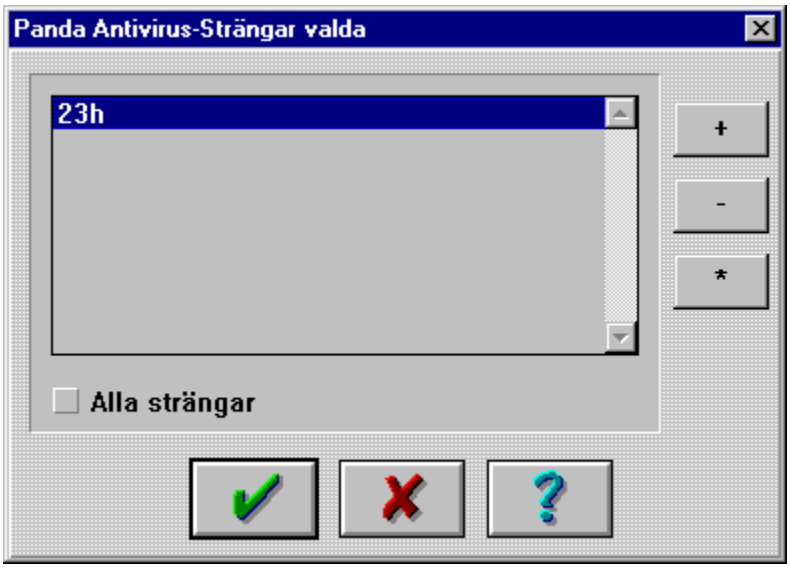
Som redan nämnts måste följande uppgifter anges i strängsökningen:

- Vilket område Du vill analysera med denna metod.
- Vilka strängar som programmet skall söka efter.

Konfigurationen av strängsökningen består i att ange vilka strängar programmet skall söka efter.

Strängar

Genom att klicka på knappen *Strängar* öppnar Du ett fönster där Du kan välja de strängar Du önskar söka efter.



Fönstret visar en lista strängar som skrivits in. Med hjälp av knapparna kan Du lägga till eller ta bort strängar. Du kan också redigera redan inmatade strängar.

Programmet kommer inte att söka efter alla inmatade strängar såvida inte rutan *Alla strängar* är markerad. Om den inte är markerad kommer programmet endast att söka efter de strängar som är markerade i listan.

Hur man tar bort virus med Panda Antivirus

Panda Antivirus innehåller inte någon speciell "desinfektions-sektion", utan borttagningen är integrerad med analysen eller det permanenta skyddet. Om ett virus upptäcks av analysprogrammet eller permanentskyddet, kommer programmet att försöka ta bort det (om det är inställt att göra så).

Alternativen för inställningarna låter Dig ange att alla smittade filer som ej kan rensas skall tas bort eller döpas om.

Virus kan påträffas i minnet, i bootsektorn eller i filer. I vart och ett av fallen skall man gå tillväga på olika sätt. Läs mera i respektive sektion för att få mer information.

Borttagning av boot-virus

För att ta bort ett boot-sektorvirus från enhet C: gör Du så här:

1. Stäng av datorn. Sätt in en virusfri bootdiskett (om Du skall göra borttagningen från en CD måste disketten innehålla drivrutiner för CD-läsaren) och starta om datorn. Om Du har skapat säkerhetsdisketter med hjälp av **Safedisk**, använder Du den första Safedisken som bootdiskett.
2. När väl datorn startat om kör Du kommandoradsversionen av antiviruset (PAVCL) enligt nedanstående instruktioner:

   - Om Du vill köra **Pavcl** från diskett, sätter Du i disk 1 av **Panda Antivirus** för DOS/Windows 3.1x eller den andra Safedisken och skriver:

     ```
     PAVCL C: /CLV
     ```

   - Om Du vill köra **Pavcl** från CD-ROM, sätter Du i CD-skivan och ställer Dig i katalogen DOSWIN3X och önskad "språkkatalog" och skriver:

     ```
     PAVCL C: /CLV
     ```

     Om Du får ett meddelande att enheten är ogiltig skriver Du:

     ```
     PAVCL /HD0 /CLV
     ```

Borttagning av filvirus

Om Du har virus i Dina filer rensar Du Ditt system genom att ställa in programmet enligt följande:

- I *Analysera/Alternativ/Filtyper* aktiverar Du *Alla filtyper, Desinficera* och *Automatisk*.
- Gå till analysdelen och markera alternativet *Enheter: Alla*. När analysen utförs kommer smittade filer att rensas.

Borttagning av virus via permanentskyddet

Sentinel klarar av att ta bort de virus den upptäcker. Om **Sentinel** upptäcker ett virus och är inställd på att ta bort det, kommer programmet att ta bort viruset innan filen tillåts gå vidare. För att **Sentinel** skall ta bort virus automatiskt måste Du ställa in programmet på *Automatisk* och *Desinficera*.

Borttagning av minnesresident virus

Om Du misstänker att Du har ett virus i minnet stänger Du av datorn, sätter i en ren bootdiskett (som måste innehålla drivrutiner för CD-läsaren om Du tänker köra programmet från CD) och startar om datorn.

Om Du använde **Safedisk** för att skapa disketter använder Du disk 1 som bootdiskett. **Pavcl**, vårt kommandoradsprogram, finns på diskett 2.

När väl datorn startat om kör Du kommandoradsversionen av antiviruset (PAVCL) enligt nedanstående instruktioner:

- Om Du vill köra **Pavcl** från diskett, sätter Du i disk 1 av **Panda Antivirus** för DOS/Windows 3.1x eller den andra Safedisken och skriver:

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

- Om Du vill köra **Pavcl** från CD-ROM, sätter Du i CD-skivan och ställer Dig i katalogen DOSWIN3X och önskad "språkkatalog" och skriver:

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

Kommandot kommer att analysera alla enheter efter virus och försöka ta bort de virus det hittar utan ingripande från användaren. Det finns utförligare information om de olika **Pavcl** kommandona på annat ställe i den här dokumentationen. **Pavcl** är kommandoradsversionen av **Panda Antivirus**. Den upptäcker och tar bort samma antal virus som alla andra versioner av **Panda Antivirus**. Med det här kommandot kan Du ta bort alla virus som upptäcks och sedan starta om datorn som vanligt utan problem.

Analys från kommandoraden

Panda Antivirus innehåller ett program som heter **Pavcl** och som körs från kommandoraden i MS-DOS. Analysverktyget upptäcker och tar bort samma virus som alla andra versioner av programmet.

Pavcl är ett snabbt analysverktyg som upptar väldigt lite minnesutrymme. Det behövs dock en viss kunskap om de parametrar som programmet måste ha för att kunna köras. **Pavcl** finns i installationskatalogen för **Panda Antivirus** för Windows 95/98. Det finns också på disk 1 i DOS/Win3.x-versionen, samt i motsvarande språkkatalog i katalogen DOSWIN3X på CD-skivan.

Pavcl Parametrar

Uppgift

`/NOM` Analysera inte minnet.

`/NOB` Analysera inte boot-sektorn.

`/NOF` Analysera inte filer.

`/ALL` Analysera alla enheter (disketter, hårddiskar etc).

`/INVx` Undersök enhet ”x” för att hitta okända virus.
Exempel: /INVA undersöker enhet A: (diskettstationen).

`/CLV` Ta bort de virus som hittas.

`/LIS` Visa en lista på de virus som upptäcks i den här versionen.

`/HEU` Aktivera en heuristisk sökmetod.

`/CMP` Analysera komprimerade filer.

`/CDR` Visa **PAVCL**s svarskoder.

`/SAV` Spara de nuvarande parametrarna i en fil. Vid nästa körning kommer de sparade parametrarna att ligga till grund för de som eventuellt skrivs in i den nya körningen.

`/IB+` Lägger till ett internt vaccin i boot-sektorn.
`/IB-` Tar bort ett internt vaccin från boot-sektorn.
`/IB*` Verifierar internt vaccin i boot-sektorn.

`/EB+` Lägger till ett externt vaccin i boot-sektorn.
`/EB-` Tar bort ett externt vaccin från boot-sektorn.

`/EB*` Verifierar externt vaccin i boot-sektorn.

`/IF+` Lägger till ett internt vaccin i en fil.
`/IF-` Tar bort ett internt vaccin från en fil.
`/IF*` Verifierar internt vaccin i en fil.

`/EF+` Lägger till ett externt vaccin i en fil.
`/EF-` Tar bort ett externt vaccin från en fil.
`/EF*` Verifierar externt vaccin i en fil.

`/B+` Lägger till ett internt och externt vaccin i boot-sektorn.
`/B-` Tar bort ett externt och externt vaccin från boot-sektorn.
`/B*` Verifierar externt och externt vaccin i boot-sektorn.

`/F+` Lägger till ett internt och externt vaccin i en fil.
`/F-` Tar bort ett internt och externt vaccin från en fil.
`/F*` Verifierar internt och externt vaccin i en fil.

Alternativ

`/NSB` Analysera inte underkataloger.

`/PTH` Analysera de kataloger som finns i PATH-variabeln.

`/ISO` Aktivera isolerat läge.

`/NOS` Avaktivera ljud.

`/AEX` Analysera alla filer oavsett filtyp (filändelse).

`/AUT` Analysera utan ingripande från användaren.

`/OVR` Skriv över innan borttagning.

`/NOR` Skriv ingen resultatfil.

`/DEL` Ta bort infekterade filer även om det går att ta bort endast viruset.

`/LOC` Analysera alla lokala enheter.

`/NBR` Tillåt inte att analysprocessen avbryts.

`/ITW` **Pavcl** kommer endast att söka efter virus i *In The Wild*. Denna parameter skall bara användas under speciella omständigheter.

Du kan också använda alternativet ”/?”, en DOS-standard, för att få en lista över tillgängliga parametrar. Du ser också vilka alternativ Du kan använda för de olika språk denna version av **Pavcl** stödjer.

De förinställda åtgärderna är:

- Analysera minnet.
- Analysera boot-sektorn.
- Analysera filer.

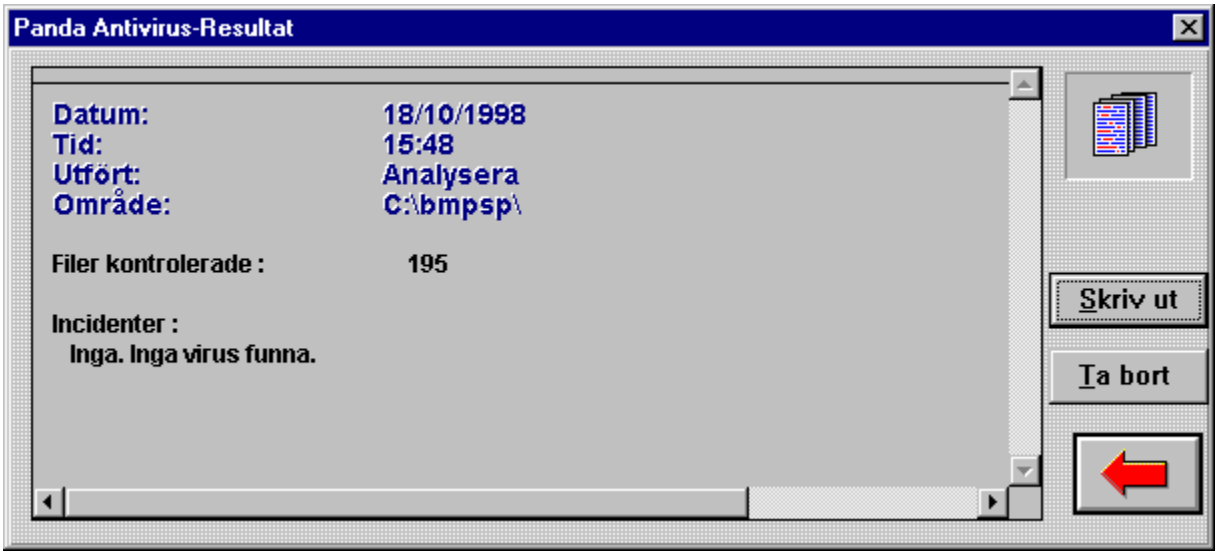
Och de förinställda alternativen är:

- Analysera underkataloger.
- Desinficera inte (ta inte bort virus).
- Aktivera ljud.
- Analysera bara programfiler.
- Skapa en resultatfil.

Växlarna /?, /LIS och /INVx är exkluderande, d v s de kan inte kombineras med någon annan uppgift. Efter att ha utfört den valda uppgiften återvänder programmet till DOS. Sökvägen för de filer man vill analysera skrivs på vanligt DOS-sätt:

```
[Enhet:][Sökväg][Filnamn]
```

Resultatrapport



Resultatrapporten visar alla de uppgfiter som har utförts med antiviruset såväl som alla incidenter som inträffat.

Informationen sparas mellan de olika körningarna. Den kan därför användas för att när som helst undersöka alla uppgifter utförda med antiviruset.

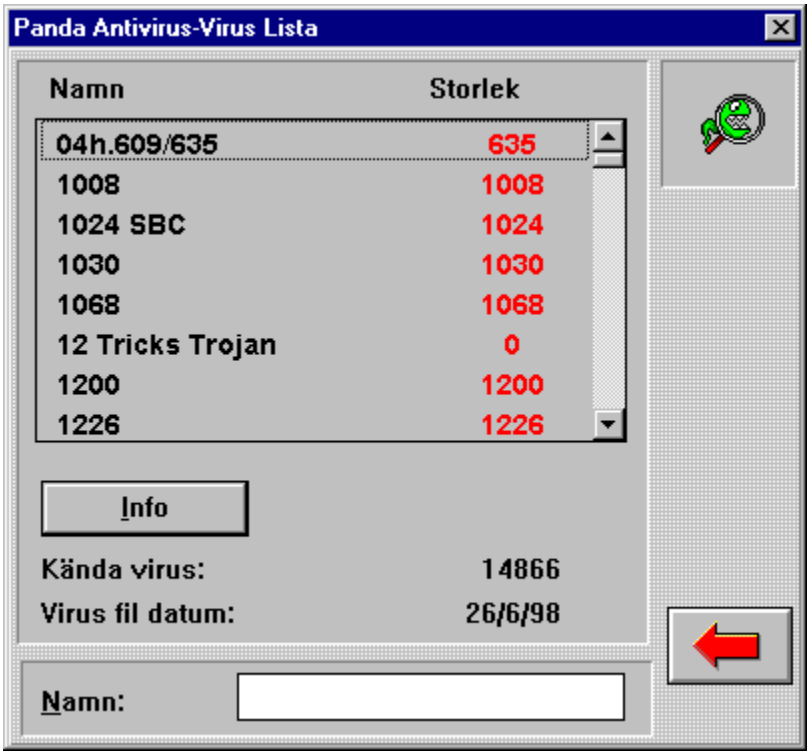
För alla operationer loggas följande data:

- Datum och tid.
- Typ av uppgift.
- Område där uppgiften utfördes.
- Antal filer som kontrollerats.
- Alla virusrelaterade incidenter.

För att informationen skall sparas i resultatrapporten måste man ha kryssat för rutan *Spara resultat* i fönstret *Analys/Alternativ*.

Innehållet i resultatrapporten kan skrivas ut för att vara lätt tillgängligt. Det går också att radera rapporten när som helst för att hindra den från att bli alltför omfattande.

Viruslista



Viruslistan visar de vanligaste virusen som **Panda Antivirus** kan upptäcka. Namn och storlek på varje virus visas i listan.

Antalet virus som denna version av **Panda Antivirus** kan upptäcka visas under listan. Datum då listan skapades visas också så att man kan se om den är uppdaterad eller inte.

Du kan skriva in namnet på ett virus i den vita rutan för att hitta ett virus snabbare och enklare. Listan är av samma anledning sorterad i alfabetisk ordning.

När Du har valt ett virus kan Du klicka på knappen *Info* för att öppna ett fönster med följande information:

- Namn.
- Ursprung.
- Storlek.
- Alias.
- Datum då det först upptäcktes.
- Om det går att ta bort.
- Områden som kan smittas av viruset.
- Egenskaper hos viruset.

Här nedan följer en förklaring av de olika egenskper ett virus kan ha:

- **Resident:** När viruset startas reserverar det ett litet minnesutrymme där det installerar sig själv och varifrån det kan spridas.
- **Stealth:** Detta är en teknik som en del residnta virus använder. Den består av att dölja de förändringar viruset orsakar i de filer det smittar. När användaren begär information om filen kommer viruset att fånga upp anropet och returnera information från innan filen smittades.
- **Krypterad:** Virus som har denna egenskap kan kryptera sig själva på olika sätt varje gång de smittar en fil. Därför kan man inte söka efter dessa virus med hjälp av en söksträng.
- **Skriver över:** Virus, residenta eller inte, som skriver över programkod. Smittade filer blir därför oanvändbara. Filstorleken ökar inte, såvida viruset inte är större än själva filen. Enda sättet att ta bort dessa virus är att radera filen och ersätta den med en ren och osmittad kopia.
- **Polymorfiskt:** Polymorfiska virus är avancerade varianter av krypterade virus. Polymorfiska virus kan ändra sin krypteringsmetod från smittotillfälle till smittotillfälle. På så sätt förblir ingen del av viruset oförändrad.

Allmänna funktioner

Panda Antivirus för Windows 95/98 erbjuder ett enkelt användargränssnitt. I huvudfönstret är de vanligaste alternativen lätt tillgängliga via stora knappar.

Genom att klicka på knapparna kommer Du åt de olika funktionerna i programmet. Läs mera under respektive avdelning för en utförlig genomgång av de olika funktionerna.