STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ
Plzenská 1, 080 47 Prešov

tel.: 051/7725 567
fax: 051/7732 344

spse@spse-po.sk
www.spse-po.sk

Vírusy a antivírové programy

Tatiana Varadyová

2008

TENTO PROJEKT JE SPOLUFINANCOVANÝ EURÓPSKOU ÚNIOU

Predhovor

Tento učebný text je určený pre tematický celok *Vírusy a antivírové programy* v predmete Výpočtová technika v 1. ročníku odboru Elektrotechnika.

Je členený na kapitoly podľa logického obsahu náplne tohto celku. V závere kapitoly alebo skupiny kapitol, čo je prevažne vždy v spodnej časti strany, je grafickým spôsobom vytvorený „Prehľad“ - zhrnutie obsahu tejto kapitoly, ktoré môže byť vodítkom pri príprave na uvedenú časť témy alebo pri jej opakovaní.

Obsah

Úvod **5**

1 Škodiace programy **6**

1.1 Základné pojmy 6
1.2 Prejavy napadnutia systému 6
1.2.1 Prejavy nedeštruktívnych škodiacich programov 7
1.2.2 Prejavy deštruktívnych škodiacich programov 7
1.3 Prenos škodiacich programov do počítača 8
1.4 Prečo sú škodiace programy vytvárané 8

2 Rozdelenie škodiacich programov **9**

2.1 Trójske kone 9
2.2 Vírusy 10
2.2.1 Makrovíry 10
2.2.2 Červy 10
2.3 Ďalšie delenia 12
2.3.1 Bootovacie vírusy 12
2.3.2 Rezidentné vírusy 12
2.3.3 Polymorfné vírusy 12
2.3.4 Stealth vírusy 12
2.4 Iné formy útokov 12
2.4.1 Spyware 13
2.4.2 Adware 13
2.4.3 PopUp 13

3 Ako sa brániť **14**

3.1 Zálohovanie systému 14
3.2 Prenos údajov 14
3.3 Originálny softvér 14
3.4 Internet 14
3.5 Aktívna ochrana 15

4 Antivírový softvér **16**

4.1 Vlastnosti antivírových programov 16
4.2 Metódy vyhľadávania infiltrácií 16
4.2.1 Metóda kontrolných súčtov 17
4.2.2 Metóda vyhľadávania typických reťazcov 17
4.2.3 Heuristická analýza 17
4.3 Delenie antivírových softvérov 18
4.3.1 Jednoúčelové programy 18
4.3.2 Programové balíky 18
4.4 Súčasti antivírového balíka 20

5 Antivírusový program NOD32 ..... **21**

5.1 Popis prostredia aplikácie 21
5.1.1 Nastavenie prostredia aplikácie 22
5.1.2 Profil 23

5.2 Testovanie 23
5.2.1 Konkretizovanie testovania 23
5.2.2 Výsledky testovania 24
5.3 Liečenie 25
5.4 NOD32 Control Center 25
5.4.1 Archív protokolov 25
5.4.2 Aktualizácia vírusovej databázy 25
5.4.3 Moduly NOD32 26
5.4.4 Nástroje systému NOD32 28
Záver 29
Zoznam literatúry 30

Úvod

Súčasná spoločnosť sa čoraz častejšie označuje prívlastkom informatická. Informácie majú stále väčšiu cenu. Preto sú zraniteľné a je potrebné ich chrániť.

Jedným z množstva nebezpečí, ktoré číhajú na údaje sú škodiace programy. Vírusy sú najznámejšou kategóriou škodiacich programov. Keďže v dnešnej dobe je ich hrozba reálna, aj bežný používateľ by mal byť informovaný o nebezpečenstve, ktoré mu zo strany škodiacich programov hrozí.

TENTO PROJEKT JE SPOLUFINANCOVANÝ EURÓPSKOU ÚNIOU

1 Škodiace programy

1.1 Základné pojmy

Škodiace programy sú **krátke programové celky**, ktoré sú schopné spôsobiť používateľovi istú záškodnícku činnosť. Tá môže byť dvojaká:

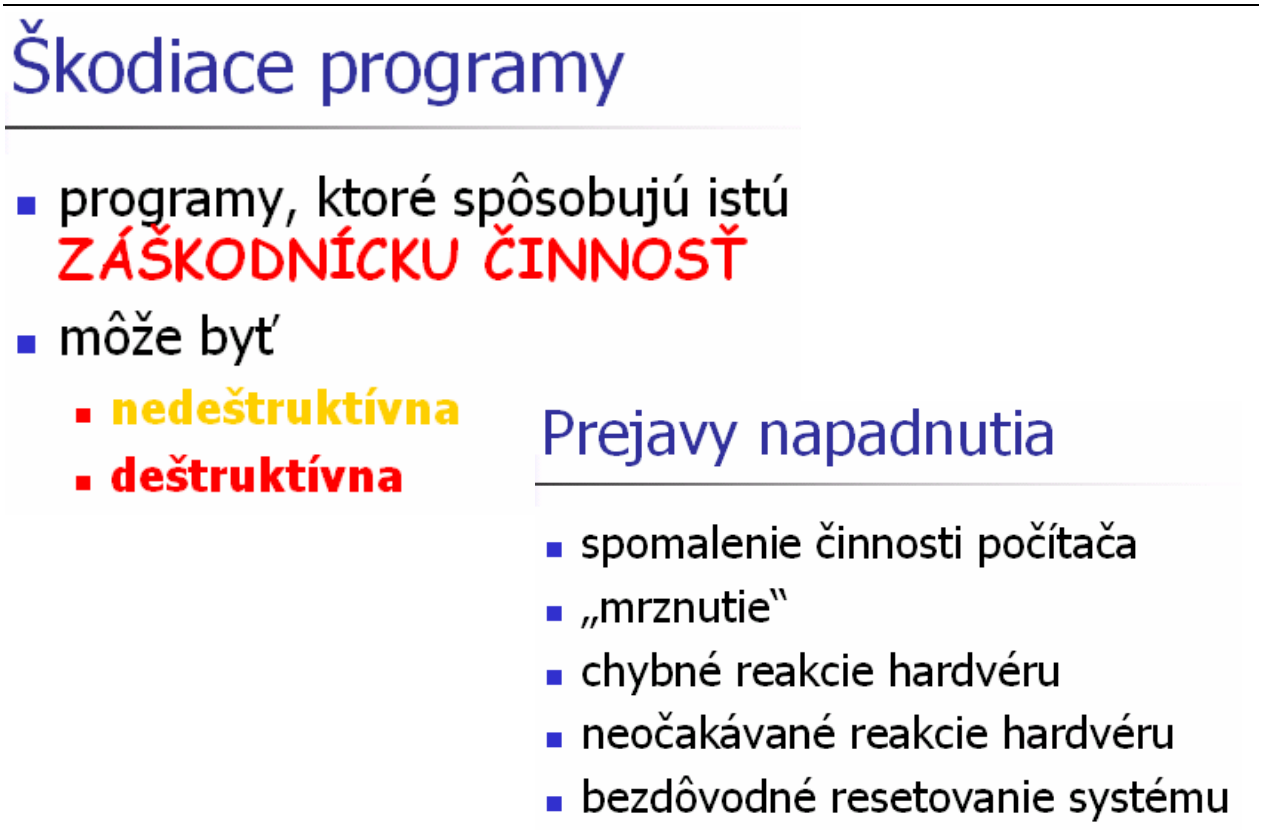
- **nedeštruktívna**, teda nespôsobí trvalé poškodenie systému,
- **deštruktívna** – poškodenia systému sú trvalé.

1.2 Prejavy napadnutia systému

Ako sa môže správať počítačový systém, ktorý je napadnutý niektorým zo škodiacich programov:

- môže sa uňho objaviť spomalenie činnosti celého počítača,
- môže sa prejaviť „mrznutie“ systému,
- niekedy sa dostavuje bezdôvodné resetovanie systému,
- chybné či neočakávané reakcie hardvéru, napr.
  - čudná reakcia myši,
  - nezvyčajná reakcia tlačiarne či iného zariadenia.

Prehľad



1.2.1 Prejavy nedeštruktívnych škodiacich programov

Kategória nedeštruktívnych škodiacich programov v zásade nespôsobuje fatálne škody. Tieto programy väčšinou len otravujú používateľovi život. Môže sa to prejavovať napríklad rozsypávaním obrazu, miznutím písmen, prípadne vyžadovaním stláčania nejakých klávesov nato, aby systém pokračoval vo svojej činnosti.

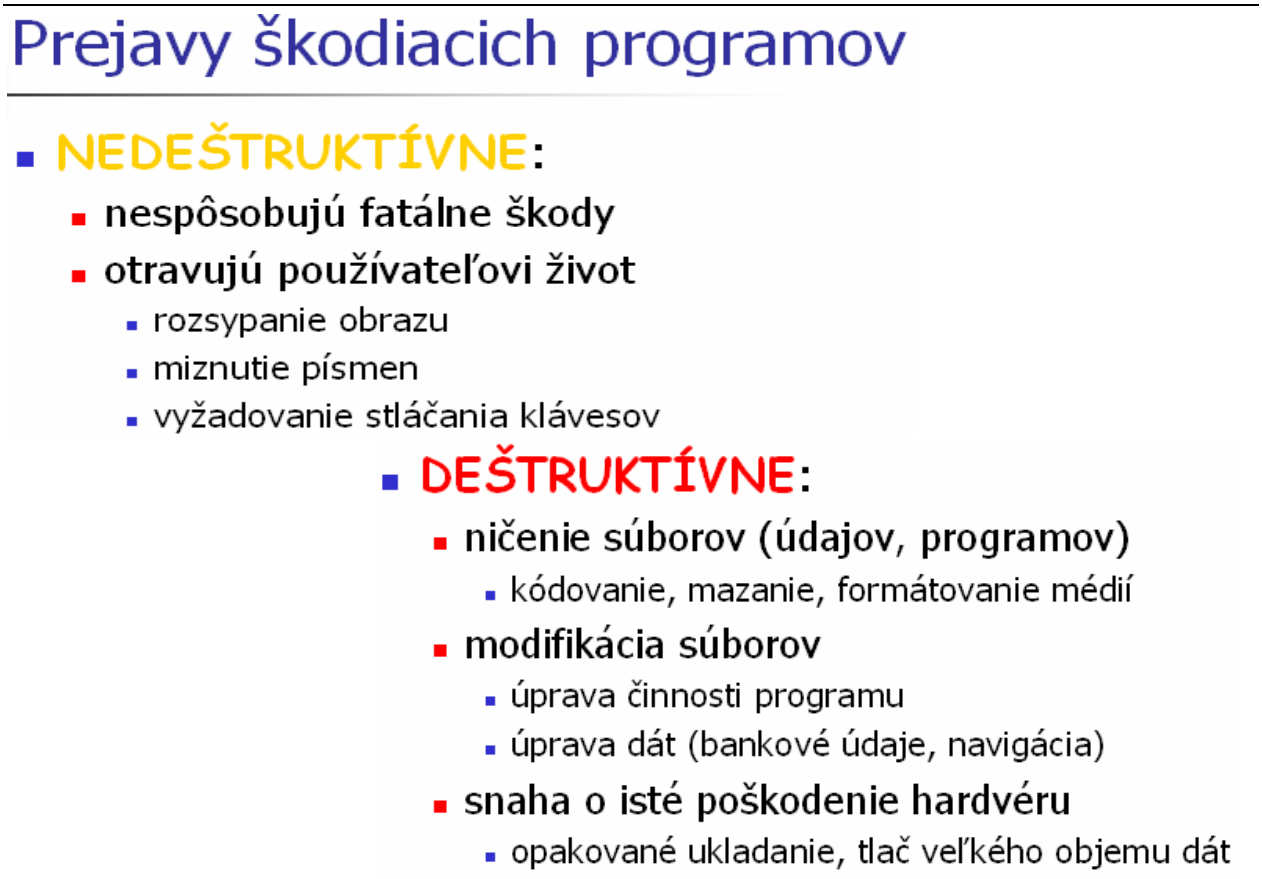
1.2.2 Prejavy deštruktívnych škodiacich programov

Horšie sú však pôsobenia deštruktívnych škodiacich programov. Môžu sa prejaviť napr. **ničením súborov**, či už súborov s údajmi alebo s programami. Samotné ničenie môže byť pri plnom formátovaní médií alebo mazaním len niektorých súborov, prípadne ich kódovaním.

Druhou kategóriou deštruktívnych činností je **modifikácia súborov**. Môže dôjsť k úprave činnosti programu alebo k úprave dát. Pokiaľ dochádza k modifikácii údajov, nie k ich trvalému odstráneniu, táto činnosť je veľmi nebezpečná. Ak sa takýto škodiaci program dostane napr. do bankového systému a bude iba posúvať desatinnú čiarku, alebo takýto program začne upravovať údaje v navigačnom softvéri. Škodiace programy z tejto kategórie sú veľmi ťažko odhaliteľné a čím dlhšie pôsobia v systéme, tým môžu napáchať väčšie škody. V tom sa prejavuje ich veľká zákernosť.

Treťou kategóriou sú škodiace programy, ktoré majú snahu istým spôsobom **poškodiť hardvér**. Môže sa jednať o zapisovanie bezvýznamných dát na voľné miesto pamäťových médií alebo tlačenie veľkého objemu dát na tlačiareň, čím sa zlikviduje všetok papier či všetok toner.

Prehľad



1.3 Prenos škodiacich programov do počítača

Ako sa škodiaci program dostane do nášho počítača? Vždy si ho prenesieme **s nejakým súborom**. Buď pomocou **prenosných médií**: diskety, CD, DVD médiá, USB kľúče, alebo **počítačovou sieťou** – škodiaci program sa dostane do počítača pomocou jej bezpečnostných dier. Často si ho tiež zanesieme z internetu, ak využívame jeho služby, napr. službu www alebo e-mail.

1.4 Prečo sú škodiace programy vytvárané

Možno sme si položili otázku – prečo sú škodiace programy vytvárané? Vytvárajú ich šikovní programátori s pochybnou morálkou. Prevláda u nich možno túžba po sláve, túžba zviditeľniť sa, niekedy si chcú iba vyskúšať svoje schopnosti a takýmto spôsobom sa sebarealizovať, v niektorých prípadoch je v popredí túžba pomstiť sa - ak sú napríklad prepustení z práce alebo majú pocit, že sú nedocenení. Každopádne u nich prevláda snaha škodiť alebo ničiť. Občas sa objavuje v literatúre aj zmienka o tom, že pomocou týchto programov môže dochádzať v niektorých prípadoch aj k ekonomickému zisku. Nie je to podložené a ťažko posúdiť, nakoľko je to skutočne realitou.

Prehľad

Prenos škodiacich programov

- **prenosnými médiami**
  - diskety, CD, DVD, flash, ...
- **počítačovou sieťou**
- **internetom** (jeho službami), napr.
  - www
  - e-mail

Prečo sú vytvárané

- šikovní programátori s pochybnou morálkou
  - zviditeľniť sa – túžba po sláve
  - vyskúšať si svoje možnosti - sebarealizácia
  - pomstiť sa
  - snaha škodiť, ničiť
  - ekonomický zisk (?)

2 Rozdelenie škodiacich programov

Dostávame sa k rozdeleniu škodiacich programov. Menej znalí používatelia považujú všetky škodiace programy za vírusy. Avšak okrem vírusov existujú aj iné skupiny, ktoré majú svoje pomenovania. Sú to trójske kone, makrovíry a červy.

2.1 Trójske kone

Tieto škodiace **programy** sa prejavujú tým, že okrem svojej **pozitívnej** (potrebnej) činnosti, vďaka ktorej si ich používateľ do svojho počítača aj nainštaluje, vykonajú tiež **nedokumentovanú činnosť**, o ktorej klient nevie a pravdepodobne by s ňou nesúhlasil (napr. vymazanie súboru). Pokiaľ ide o tú dokumentovanú – pozitívnu činnosť, musí byť taká, aby presvedčila používateľa, že práve tento program je pre neho potrebný a práve tento program chce mať vo svojom počítači. Môže to byť napríklad nejaký veľmi pekný šetrič obrazovky, veľmi dobrý súborový manažér alebo iný program, po ktorom používateľ zatúži.

Základnou vlastnosťou trójskych koní je však skutočnosť, že **nemajú schopnosť replikácie**, teda nerozmnožujú sa. Nevytvárajú svoje kópie, ktoré by sa pridávali k ďalším doteraz čistým súborom. Ak si zavlečieme do počítača jeden napadnutý súbor, tak aj po čase tam naďalej bude iba jeden „nečistý“ súbor - nebude ich viac.

Trójske kone môžu napr. vytvárať aj tzv. „zadné dvierka“ do systému – umožnia prevziať ovládanie nad počítačom ľuďom z radov hackerov, ktorí o to majú záujem.

Trójske kone môžeme členiť na kategórie. Medzi nimi nájdeme aj tzv. bomby či míny.

Míny

Sú to škodiace programy, ktoré po vykonaní svojej záškodníckej činnosti **likvidujú samé seba**. Zlikvidovaný je teda ten program, ktorý bol nositeľom tejto nežiadúcej činnosti. Z toho dôvodu sa dosť ťažko odhaľujú - po istej dobe vlastne samé prestanú existovať v počítači.

Míny sa niekedy zvyknú pridávať k demoverziám programov. Zabezpečí sa tým, že program (demoverzia plnej komerčnej verzie programu) po istej dobe prestane existovať a teda nie je možné naďalej ho používať.

Bomby

Touto kategóriou sa označujú škodiace programy, ktoré sú aktivované pri istej podmienke. **Podmienka** je

- logická
- časová.

Logickou podmienkou môže byť napríklad

- počet odštartovaní programu,
- prítomnosť konkrétneho hardvéru – napr. grafickej karty alebo disku,

a pokiaľ definovaná logická podmienka nie je splnená, tak sa tento škodiaci program vôbec neaktivuje, čiže neukáže svoju činnosť resp. prítomnosť. Môže sa preto pokojne stať, že na jednom počítači takýto program vôbec nezistíme, pričom na inom áno, pretože tam požadovaná logická podmienka splnená bola.

Časové bomby sú zase závislé na nejakom časovom intervale alebo časovom okamihu. Sú to teda škodiace programy, ktoré sa spúšťajú napríklad: v piatok trinásteho, prvého apríla, alebo po uplynutí nejakého časového obdobia (napr. tridsiatich dní od inštalácie) a pod.

2.2 Vírusy

Dostávame sa ku kategórii škodiacich programov, označovanej ako vírusy. Vírusy sú trójske kone, ktoré **majú navyše schopnosť replikácie**. Replikácia je samokopírovanie, teda **nekontrolované rozmnožovanie sa**.

Vírusy potrebujú ku svojej existencii hostiteľa - štartovateľný súbor (súbor s príponou ***.exe***, ***.com***), podobne, ako trójske kone. Aktivujú sa jeho odštartovaním. Okrem vykonania svojej naprogramovanej záškodníckej činnosti vytvoria zo seba kópiu, a tú pripoja ku vhodnému súboru, ktorý nájdu. Ten sa stáva následne prostriedkom na ďalšiu aktiváciu vírusu.

Tým, že sa vírusy replikujú, teda vytvárajú zo seba svoje vlastné kópie, tie sa pripájajú k iným štartovateľným súborom. A teda - ak sme si do svojho počítača zaniesli jeden jediný vírus na jednom štartovateľnom súbore, za nejakú dobu budeme mať tento vírus niekoľko násobne viac krát vo svojom počítači, prilepený ku iným štartovateľným súborom. Pomocou tohto mechanizmu je zabezpečené, že sa vírus mnohonásobne častejšie rozšíri do iných počítačov na jednom výskyte programu, ako to robí trójsky kôň.

2.2.1 Makrovíry

Dlhú dobu sa nebezpečnými v súvislosti s prenosom škodiacich programov, javili iba štartovateľné – teda vykonateľné súbory. Sú to tie, ktoré po svojom odštartovaní priamo vykonávajú svoju naprogramovanú činnosť. Majú príponu ***.exe*** či ***.com***. Dátové súbory boli z tohto hľadiska bezpečné – nepredstavovali žiadne nebezpečenstvo pre zavlečenie škodiacich programov do počítača. Dnes však už táto výsada neplatí. Aj dátové súbory, hlavne tie, ktoré boli vytvorené v aplikáciách balíka ***MS Office*** môžu byť nositeľmi škodiacich aktivít. Zabezpečujú to tzv. makrovíry.

Makrovíry sú škodiace programy, ktoré sa viažu na dátové súbory, najčastejšie tie, ktoré sú produktmi aplikácií balíka ***MS Office*** (***.doc***, ***.xls***, ***.pps***). Súbory s dátami za normálnych okolností nemôžu byť nositeľmi bežných vírusov, pretože samé osebe nič nevykonávajú. Pri práci s takýmito súbormi je však k dispozícii tzv. makrojazyk. Zabezpečí napr. vykonávanie opakovaných činností v súvislosti s úpravou dokumentov.

Otvorením dokumentu aplikáciou, pokiaľ boli použité, tak sa príkazy makrojazyka vykonajú. Sú zamerané na dáta a činnosti s nimi. Pokiaľ pomocou príkazov makrojazyka dokážeme v dokumente vykonať zmysluplnú činnosť, ktorá je pre používateľa pozitívna, je možné naprogramovať aj postupnosť negatívnych činností. A na tomto princípe fungujú makrovíry. Využívajú makropríkazy na príslušnú škodiacu činnosť. Makrovíry sa môžu vyskytnúť v súvislosti so súbormi obsahujúcimi dokumenty aplikácie ***MS Word***, zošit aplikácie ***MS Excel***, či prezentácie aplikácie ***MS PowerPoint***. Sú to štatisticky tak často používané aplikácie, že má zmysel pre tvorcov, zapodievať sa vytváraním škodiacich postupností práve nástrojom makrojazyka. Hostiteľskými súbormi makrovírov sú teda dokumentové súbory.

2.2.2 Červy

Ďalšou kategóriou sú škodiace programy, ktoré nazývame červy. Červy sú vírusy, ktoré nepotrebujú ako hostiteľa štartovateľný súbor, ale **šíria sa prostredníctvom počítačovej siete**. Najčastejšie využívajú elektronickú poštu, pomocou ktorej sa rozšíria na počítače v sieti zapojené.

Červy môžu pre svoju činnosť využívať aj bezpečnostné diery v sieťovom operačnom systéme a prostredníctvom nich sa rozšíriť na počítače, ktoré sú vzájomne prepojené bez ohľadu na pripojenie k internetu.

Dôsledky činnosti červov sú rôzne. Skutočnosť, že sa replikujú a rozširujú na počítače v sieti, zabezpečí ich veľmi rýchle množenie, ktoré spôsobuje napr.

- **citeľné spomalenie** prenosu dát v počítačovej sieti, ktoré môže viesť až k jej zahlteniu,
- **zapĺňanie diskového priestoru** nežiadúcimi dátami.

Teda aj keď červ nič iné nevykonáva, iba sa množí, vzhľadom na to, že funguje v sieti, môže spôsobiť obrovské škody z dôvodu straty priechodnosti prostriedkov IKT v danom čase.

Ďalšou činnosťou sieťových škodiacich programov je ale tiež zisťovanie prístupových hesiel ku kontám používateľov, najlepšie administrátorov. Tiež rôzne pokusy o prevzatie kontroly nad počítačom prípadne nad celou miestnou počítačovou sieťou.

Rôzne formy takýchto škodiacich programov sa šíria či už priamo v správe elektronickej pošty alebo pomocou súborov, ktoré tvoria jej prílohu. Je preto veľmi nebezpečné otvárať správy prípadne pripojené súbory, ktoré

- sú od neznámych či nedôveryhodných odosielateľov,
- majú čudný a nepravdepodobný obsah (napr. anglický text od slovenského odosielateľa, stačí aj nepravdepodobný predmet správy),
- v prílohe je súbor so zvláštnou príponou,
- súbor v prílohe má viacero prípon, a pod.

Sieťové vírusy sú nepríjemné hlavne tým, že majú vysoký potenciál šírenia v podobe uložených kontaktov v schránkach elektronickej pošty. Z tohto hľadiska je napr. e-mail klient ***MS Outlook*** nebezpečný svojou funkciou náhľadu správy, ktorá sa vďaka tomu otvára automaticky bez pokynu používateľa, a tým sa škodiaci program zanesie do počítača bez jeho vedomia. Následne môže využiť e-mail kontakty a okamžite sa rozošle ďalej.

Prehľad



2.3 Ďalšie delenia

Škodiace programy je však možné rozdeliť do rôznych iných skupín podľa ďalších iných kritérií. Uvedieme si len pomenovania, ktoré súvisia najčastejšie s vírusmi a môžeme sa s nimi stretnúť pri označovaní rôznych kategórií škodiacich programov.

2.3.1 Bootovacie vírusy

Pojem „boot“ predstavuje štart operačného systému. Pojem bootovací vírus označuje škodiaci program, ktorý sa štartuje súčasne **s odštartovaním operačného systému**. Neaktivuje ich teda ľubovoľný súbor ***.exe***, ale priamo zapnutie počítača.

2.3.2 Rezidentné vírusy

Rezidentný znamená trvalo bežiaci, teda umiestnený v operačnej pamäti. Pokiaľ hovoríme o rezidentných vírusoch, jedná sa o také škodiace programy, ktoré po svojom odštartovaní umiestnia sa do operačnej pamäte, trvalo v nej bežia a čakajú na vhodnú príležitosť, kedy môžu prejaviť svoju činnosť.

2.3.3 Polymorfné vírusy

Jedna a tá istá činnosť sa môže vykonať rôznymi spôsobmi. Práve túto skutočnosť využívajú polymorfné vírusy. Sú typické tým, že sa snažia **skryť pred odhalením** antivírovým programom. Schovávajú sa pomocou maskovania, ktoré spočíva v tom, že menia svoj kód pri každej kópii jedného a toho istého vírusu.

Skutočnosť, že je možná zmena kódu, vyplýva práve z variability postupov pri dosiahnutí toho istého cieľa. Daná činnosť môže byť zapísaná viacerými spôsobmi, a môže byť vykonaná viacerými postupmi. Vírus teda môže jednu a tú istú škodiacu činnosť vykonávať pomocou rôznych postupov. Žiadne dve kópie polymorfného vírusu nemajú presne identický kód a tým sú veľmi ťažko odhaliteľné pomocou antivírových programov.

2.3.4 Stealth vírusy

Vírusy označované stealth sa rovnako snažia **zamaskovať svoju prítomnosť** v systéme. Využívajú na to však iné mechanizmy, ktorými zneviditeľnia svoju prítomnosť (napr. zmena prípon súborov).

V literatúre či na internete sa môžeme stretnúť s mnohými ďalšími deleniami škodiacich programov a rôznymi inými kategóriami vírusov, pretože každý deň vznikajú nové, a snažia sa čo najúspešnejšie dosiahnuť svoj cieľ.

2.4 Iné formy útokov

S masívnym rozvojom používania internetu sa stretávame s ďalšími nástrahami, ktoré číhajú na počítače používateľov. Môžu byť zavlečené pomocou vírusov, trójskych koní či červov, podstatný je dôsledok, ktorý spôsobia.

2.4.1 Spyware

Spyware je tzv. špiónsky program. Zisťuje – „kradne“ dáta z cieľového počítača, aby ich odovzdal záujemcovi. Môžu to byť osobné údaje, využijú sa napr. pre potreby agresívnej reklamy, ale tiež napr. heslá k finančným účtom, či počítačovým kontám za účelom zneužitia.

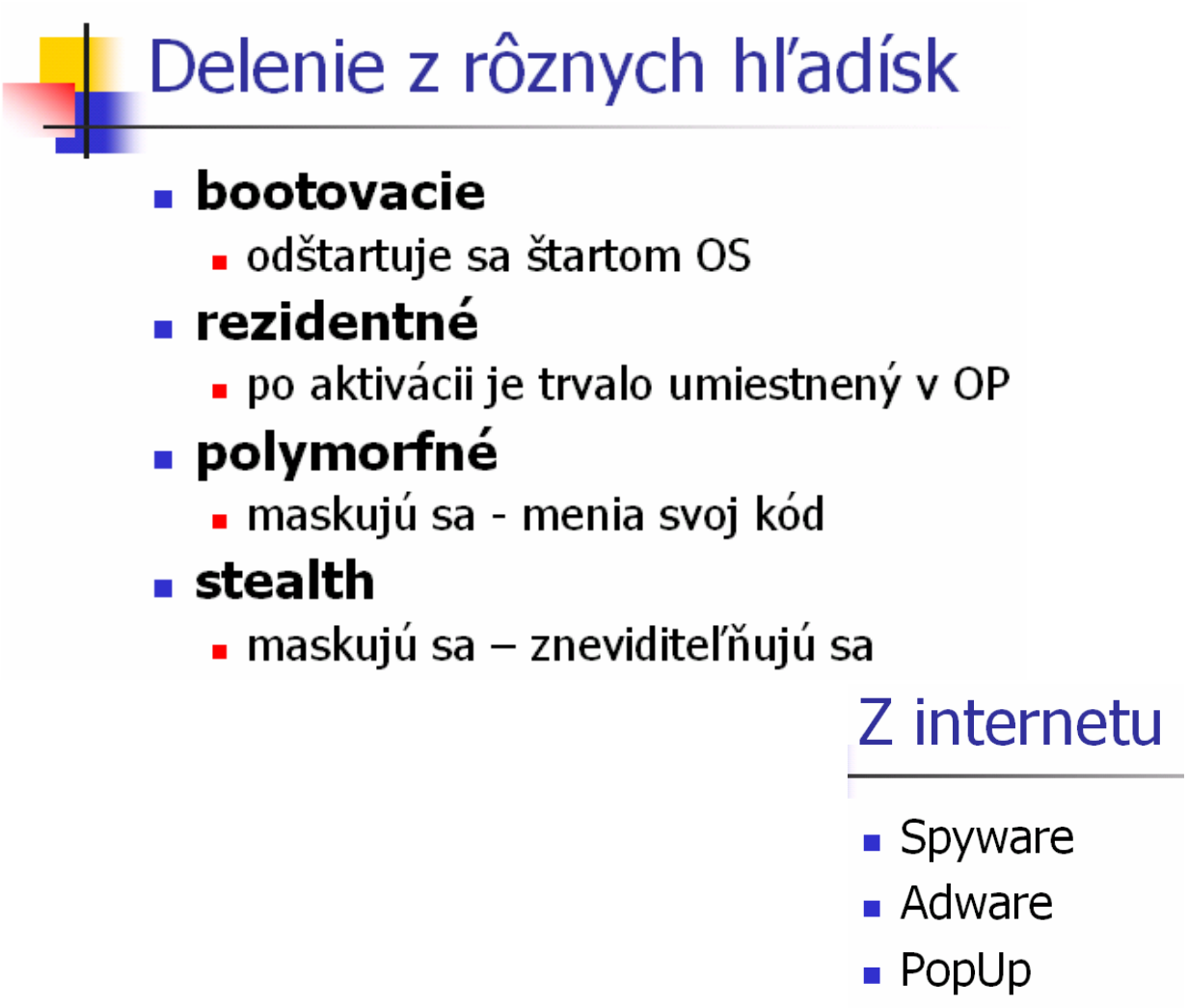
2.4.2 Adware

Adware je určitá forma špiónskeho programu, ktorý získava informácie o používateľovi, ktorý surfuje po www stránkach špeciálne pre potreby reklamy. Následne otvára bez jeho pokynu nevyžiadané okná s reklamnými informáciami. Snažia sa prispôsobiť jeho zvyklostiam, robiť reklamu cielenou. Adware môže zhromažďovať osobné údaje bez vedomia používateľa. Spomaľuje prácu a je to pre používateľa obťažujúce.

2.4.3 PopUp

Programy, ktoré otvárajú okná nevyžiadané okná s reklamou bez vôle používateľa služby www . Nezhromažďujú osobné údaje, sú však obťažujúce.

Prehľad



3 Ako sa brániť

Používateľ by mal aspoň rámcovo vedieť, ako sa brániť pred stratou údajov, ktorú nám môžu spôsobiť škodiace programy.

3.1 Zálohovanie systému

V prvom rade je veľmi dôležité vykonávať zálohovanie systému, s ktorým pracujeme. Pravidelné zálohovanie si vyžadujú hlavne **dátové súbory**, ktoré sme počas činnosti s počítačom vytvorili resp. upravili. Zálohovanie programov nie je až takou veľkou nutnosťou, pretože je predpoklad, že máme vždy k dispozícii originálne nosiče, na ktorých tieto programy sú, a my si ich môžeme z týchto originálnych nosičov kedykoľvek do nášho počítača znova nainštalovať. Vytvorené dáta však zostávajú len v našom počítači. To je dôvod, prečo práve ich treba ukladať aj na záložné médiá.

Niekto by mohol namietať, že na záložné médium sa nám pri zálohovaní môže uložiť aj napadnutý súbor, a teda máme uložený súbor s nákazou. Je to pravda. Je však výhodou, ak máme uložené na záložnom médiu hoci aj zavírené dáta, ktoré z neho môžeme kedykoľvek obnoviť. V prípade, že sa škodiaci program prejavil a zničil dáta v počítači, pravdepodobne získame vhodný program, ktorým si dokážeme túto nákazu odstrániť. A rovnako ju odstránime aj zo zálohovaných dát, resp. z dát obnovených zo zálohy. Máme teda šancu, dostať sa späť k svojim údajom. V prípade, že žiadnu zálohu nemáme, nemáme z čoho dáta obnoviť.

3.2 Prenos údajov

Prenos údajov nesie vysoké riziko z hľadiska možnosti nákazy počítača. Samozrejme, že sa nevyhneme prenosu dát z počítača na počítač, v dnešnej dobe to jednoducho nie je možné. Treba však mať na pamäti nebezpečenstvo, ktoré je s tým spojené.

Tiež si treba uvedomiť nebezpečenstvo použitia podozrivých zdrojov či médií, alebo neznámych nosičov informácií (diskety, CD médiá). Jednoducho nevkladajme takéto médiá bez rozmyslu do našich počítačov. A hlavne - nezabúdajme ich v mechanikách pred štartom operačného systému (nebezpečné môžu byť zabudnuté diskety v mechanike po vypnutí počítača – z hľadiska jeho následného zapnutia a zotrvaní napadnutej diskety v nej pri zavádzaní operačného systému).

3.3 Originálny softvér

Ďalším odporúčaním pre ochranu proti infiltráciám do počítačov je používať iba originálny softvér. Naozaj sa neodporúča sťahovať si programy z rôznych stránok nelegálneho softvéru, alebo kupovať ich od priekupníkov, kde nie je zaručená jeho pravosť. Podobne je to aj s kopírovaním programov medzi používateľmi vzájomne. Nikde nie je zaručené, že kamarátov počítač je naozaj čistý.

3.4 Internet

Internet je najväčším zdrojom informácií ale bohužiaľ aj najväčším zdrojom škodiacich programov. Preto neodporúča sa navštevovať webové sídla, ktoré sú pochybného rázu. Či už sú

to webové stránky, ktoré ponúkajú nelegálny softvér, nelegálnu hudbu alebo www stránky iného charakteru (napr. so sexuálnou tematikou).

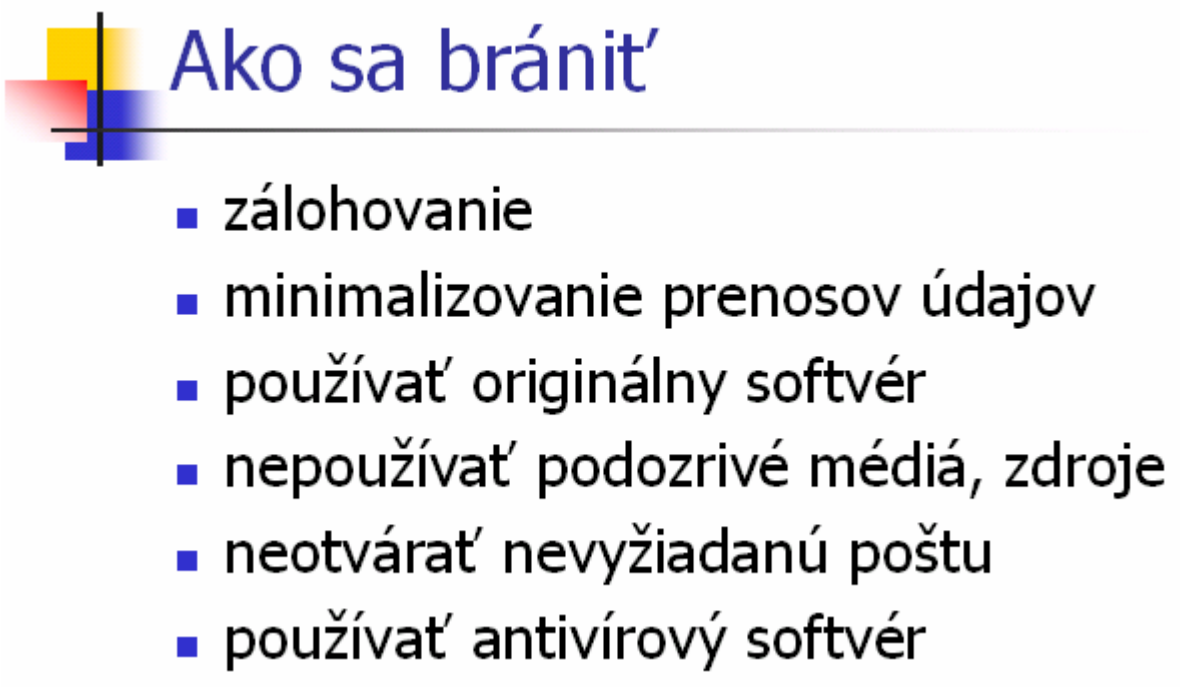
Podobne je to aj s nevyžiadanou poštou. Každý deň sme zavalení množstvom mailov, z ktorých ale veľká väčšina je z kategórie nevyžiadaná pošta. Neodporúča sa otvárať všetky správy, ktoré sú do našej schránky doručené. Pokiaľ je nám odosielateľ správy neznámy, pokiaľ nám nič nehovorí predmet správy, či správa je v cudzom jazyku, nemusíme ju vôbec otvárať. Ak správu otvoríme a tá obsahuje ako prílohu štartovateľný súbor, a navyše nám správa nie je ničím povedomá, neodporúča sa tento súbor vôbec ukladať na disk.

Škodiaci program sa môže do počítača zaniesť niekedy len samotným otvorením správy elektronickej pošty, prípadne uložením prílohy, ktorú táto správa nesie (napr. ak je prílohou štartovateľný alebo skomprimovaný súbor).

3.5 Aktívna ochrana

Ak aj budeme dodržiavať všetky predchádzajúce odporúčania, nebezpečenstvo nákazy nie je znížené úplne na nulu, pretože prenosu dát sa nevyhneme rovnako ako spamom. Každopádne existuje ďalší prostriedok ochrany nášho počítača, ktorý môže účinne chrániť počítačový systém pred nepríjemnosťami, ktoré vyplývajú zo zavlečenia infiltrácie. Dôrazne sa odporúča používať antivírový softvér.

Prehľad



4 Antivírový softvér

Antivírový program je aplikácia, ktorá vysokým spôsobom chráni náš počítač pred účinkami škodiacich programov. Existuje veľká škála ponuky tohto softvéru. Sú z kategórie komerčných aj nekomerčných a používateľ si vyberá podľa vlastností, ako napr.

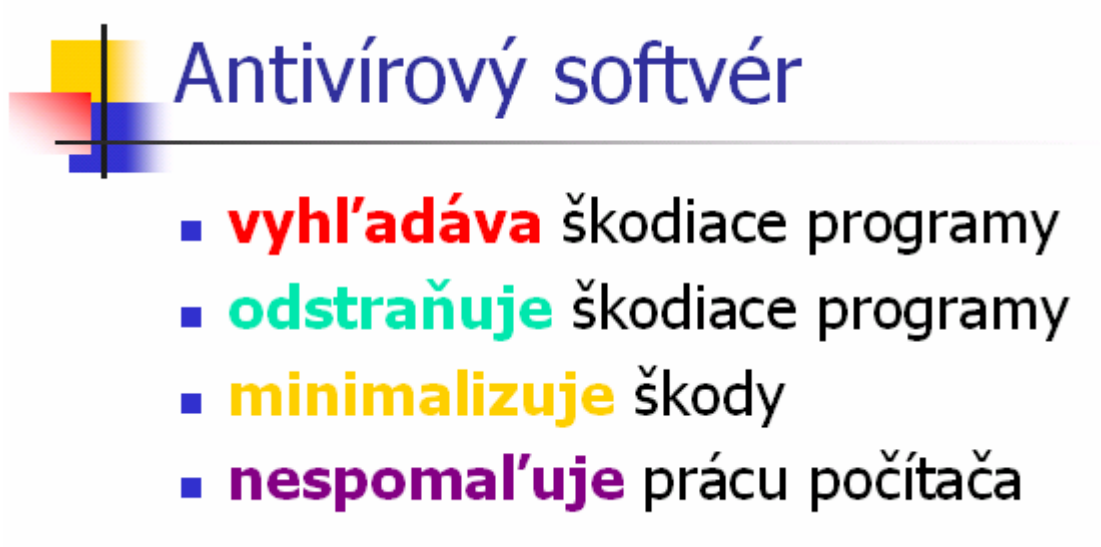
- dostupnosť,
- účinnosť ochrany systému,
- jednoduchosť ovládania programu.

4.1 Vlastnosti antivírových programov

Antivírový softvér by mal spĺňať štyri nasledujúce vlastnosti:

1. má vyhľadávať škodiace programy, ktoré eventuálne sú v našom počítači,
2. ak sa škodiaci program v počítači nachádza, úlohou antivírového softvéru je odstrániť ho,
3. pokiaľ škodiaci program napáchal škody na našom systéme, antivírový softvér sa snaží do najväčšej možnej miery tieto ujmy minimalizovať,
4. dobrý antivírový softvér však nesmie spomaľovať prácu počítača, aby tým nebrzdil prácu jeho používateľa.

Prehľad



4.2 Metódy vyhľadávania infiltrácií

Na vyhľadávanie škodiacich programov má každý antivírový program svoje vlastné metódy. Od ich účinnosti závisí účinnosť celého antivírového systému. Samozrejme, je to výrobným tajomstvom každej softvérovej firmy, ktorá vyrába antivírový program, ako sa ten dopracuje k požadovanému výsledku.

Existujú však niektoré všeobecne známe metódy, pomocou ktorých je možné škodiace programy v systéme odhaliť.

4.2.1 Metóda kontrolných súčtov

Jednou z metód, ktoré sa môžu využiť pri vyhľadávaní infiltrácií v počítači je napr. metóda kontrolných súčtov. Využíva sa pri nej skutočnosť, že súbory sú na disku zapísané ako postupnosti núl a jednotiek. Je veľmi jednoduché urobiť fyzický súčet obsahu – **spočítať nuly a jednotky**, pomocou ktorých je súbor na disku zapísaný.

Takéto kontrolné súčty sa vykonajú ihneď po nainštalovaní antivírového programu do systému. Pri opakovanej kontrole disku sa vykonávajú nové kontrolné súčty. Pokiaľ dôjde ku zmene súčtov tam, kde sa takáto zmena nepredpokladá, je predpoklad, že systém je napadnutý nejakou infiltráciou. Ktoré súbory nemajú dôvod meniť svoj kontrolný súčet: jedná sa o tie, v ktorých sa nachádzajú programy. V ich prípade nie je dôvod, aby sa menila dĺžka resp. obsah súboru – program sa iba vykonáva, nie modifikuje.

Táto metóda je však nepoužiteľná na dátové súbory, pretože dopĺňaním údajov do dátových súborov alebo ich vymazávaním, sa ich dĺžka mení a teda kontrolné súčty budú rôzne.

V aplikáciách je táto metóda ukrytá za skratku CRC (Count Round Control).

4.2.2 Metóda vyhľadávania typických reťazcov

Inou metódou pre detekciu infiltrácií je vyhľadávanie typických vírusových reťazcov pre konkrétne vírusy. Sú známe **postupy, ktoré konkrétne škodiace programy robia** a ktorými vytvoria ujmu svojmu hostiteľovi. Sú pre nich typické. Antivírový program vyhľadáva tieto charakteristické postupnosti a tým určí, ktorý konkrétny škodiaci program sa na disku nachádza. Touto metódou sa však dajú vyhľadať len tie škodiace programy, ktoré už sú dobre zdokumentované.

4.2.3 Heuristická analýza

Iná metóda, s názvom heuristická analýza, dokáže odhaliť aj škodiace programy, ktoré ešte zdokumentované nie sú. Spočíva v postupe, pri ktorom sa prezerajú jednotlivé programy na disku a zisťuje sa, čo robia. Pokiaľ obsahujú v sebe činnosti, ktoré môžu byť typické pre nejaký vírus alebo iný škodiaci program (napr. takouto činnosťou môže byť kopírovanie samého seba, či premenovávanie samého seba), heuristická analýza vyhlási, že v systéme **môže byť infiltrácia**.

Táto metóda sa neviaže na žiadne konkrétne škodiace programy. Vyhľadáva iba také činnosti, ktoré sú vo všeobecnosti typické pre akýkoľvek škodiaci program.

V prípade tejto metódy však môže byť spustený aj planý poplach. Môže sa stať, že činnosť, ktorú heuristická analýza považuje za prejav infiltrácie, je súčasťou korektného programu a je pre neho normálna. Je vždy na používateľovi, aby zvážil, či infiltrácia, ktorú našla heuristická analýza, je skutočne škodiacim programom, alebo je to len prejav normálnej činnosti konkrétneho programu.

Heuristická analýza však dokáže odhaliť aj také škodiace programy, ktoré ešte neboli zdokumentované. Nezáleží na tom, či sa už vyskytli, alebo je to prvý prejav ich existencie. Ak ale svet o nich ešte nevie a teda antivírové programy ich ešte nemajú zahrnuté do svojho zoznamu, správne nastavená heuristická analýza dokáže takejto infiltrácii do nášho počítača zabrániť.



4.3 Delenie antivírových softvérov

Existuje veľké množstvo antivírových softvérov. V zásade ich môžeme rozdeliť do dvoch kategórií.

4.3.1 Jednoúčelové programy

Jednoúčelové antivírové programy sú určené **proti konkrétnej infiltrácii**, proti konkrétnemu škodiacemu programu. Ich výhodou je **veľmi rýchla dostupnosť** po objavení sa škodiaceho programu. Rovnako sú výhodné vtedy, pokiaľ je **infiltrácia príliš zložitá**, a jej odstránenie vyžaduje vysoké nároky na antivírový program.

4.3.2 Programové balíky

Druhou kategóriou antivírového softvéru sú programové balíky. Tieto aplikácie poskytujú komplexné služby ochrany počítača proti infiltráciám. Ich súčasťou sú v zásade tri skupiny programov.

Skener

Program s označením **vyhľadávač** alebo skener má za úlohu na príkaz prezerať médiá a zisťovať, či sa na nich nenachádza infiltrácia.

Clean

Druhou skupinou programov v antivírových balíkoch sú tie, ktoré označujeme **liečiteľ** - cleaner. **Likviduje nájdenú infiltráciu**, a dokáže do čo najväčšej miery zlikvidovať aj jej dôsledky.

Pokiaľ si ale liečiteľ nevie so škodiacim programom poradiť, vykoná aspoň opatrenia na to, aby sa nemohol ďalej v systéme šíriť a robiť záškodnícku činnosť. Takáto situácia vôbec nemusí byť výnimočná, vzhľadom na obrovské množstvo novovznikajúcich infiltrácií.

Ak v čase odhalenia antivírový softvér nemá ešte prostriedky na to, aby infiltráciu odstránil, a zlikvidoval jej škody, premiestni ju do vymedzeného priestoru tak, aby zamedzil jej šíreniu alebo prejavom jej činností. Oblasť, do ktorej sa izolujú napadnuté súbory sa môže nazývať rôzne: napr. karanténa alebo vírusový trezor.

Rezidentný štít

Ďalšou časťou antivírového softvérového balíka je tzv. rezidentný štít. Zabezpečuje neustály dohľad nad počítačom tým, že trvale beží v operačnej pamäti a kontroluje všetky jeho činnosti. Pokiaľ by sa nejaká infiltrácia snažila do nášho počítača dostať, napr. z elektronickej pošty, alebo počas kopírovania dát z nejakého prenosného elektronického média, rezidentný štít tento pokus ohlási, prípadne zamedzí takejto činnosti.

Prehľad

Typy antivírových softvérov

- JEDNOÚČELOVÉ PROGRAMY
  - špeciálne proti konkrétnemu programu
  - okamžite dostupné pri objavení sa vírusu
  - pri zložitých infiltráciách účinnejšie
- PROGRAMOVÉ BALÍKY
  - komplexné služby ochrany počítača proti infiltráciám

Programové balíky

- **Vyhľadávač** – scanner
  - na príkaz prezerá médiá
- **Liečiteľ** – clean
  - likviduje škodiaci program, jeho dôsledky
  - pokiaľ nedokáže – zamedzí šíreniu a útokom (karanténa, trezor)
- **Rezidentný štít**
  - neustála kontrola činnosti počítača

4.4 Súčasti antivírového balíka

Antivírový softvérový balík je tvorený dvomi súčasťami. Prvou z nich je samotný **program**, ktorý si nainštalujeme na svoj počítač, a on zabezpečuje jeho ochranu. K svojej činnosti však potrebuje druhú súčasť, ktorá sa nazýva **vírusová databáza**. Tá obsahuje informácie o všetkých škodiacich programoch, ktoré sú v danom čase dostupné, a ktoré teda môžu ohroziť náš počítač.

Keďže škodiace programy vznikajú denne, je potrebné vírusovú databázu pravidelne obnovovať, aby mal antivírový program vždy aktuálne informácie o reálnych možných infiltráciách. Pokiaľ by obnova nebola vykonávaná dostatočne často, počítač nebude dostačujúco chránený pred možnou nákazou.

Ako často a kde je vírusová databáza dostupná na to, aby sa mohol vykonať upgrade, to závisí od konkrétneho výrobcu antivírového balíku. V niektorých prípadoch sa poskytujú vírusové databázy denne prípadne aj viac krát denne podľa potreby, pretože výskyt nových infiltrácií je naozaj veľmi častý. Pri niektorých aplikáciách sú dostupné v dlhších časových intervaloch. Vírusové databázy sú najčastejšie dostupné na stiahnutie na internete.

Príkladom u nás veľmi často využívaných antivírových balíkov sú programy

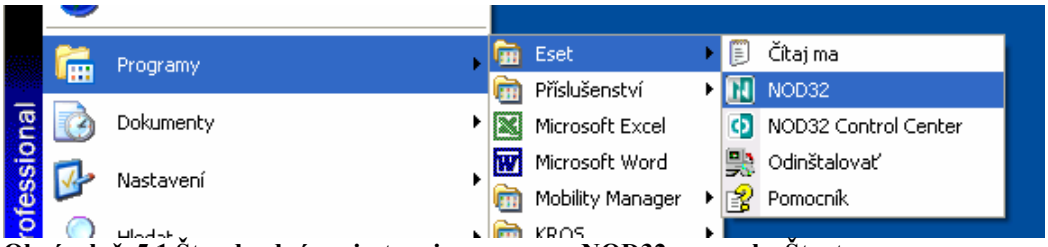
- NOD od firmy Eset,
- AVG od firmy Grisoft.

Prehľad

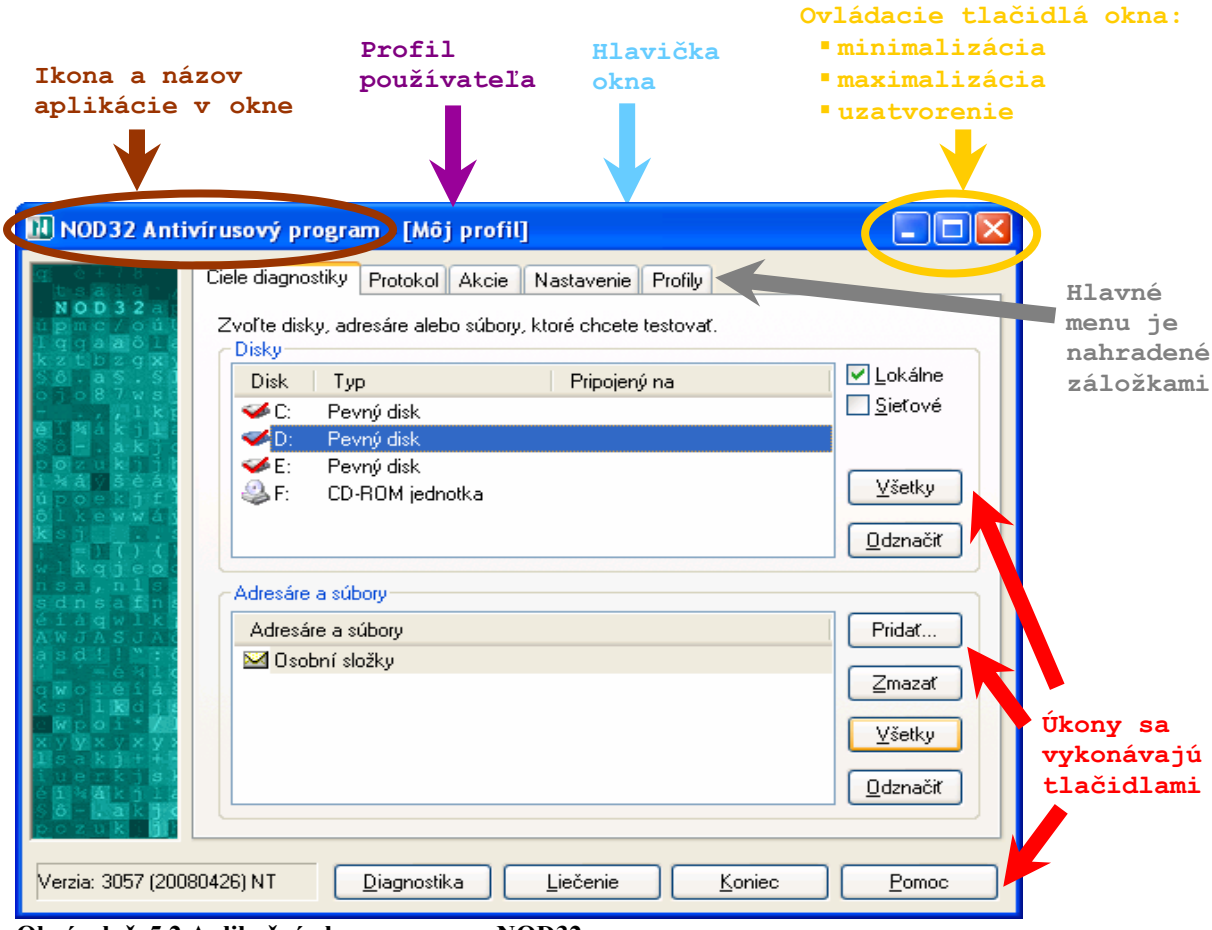


5 Antivírusový program NOD32

Komerčný softvér ***NOD32*** je balík programov, ktorý ochráni počítač od infiltrácií. Štandardnou inštaláciou sa vytvorí programová skupina ***Eset*** (Obrázok č. 5.1). V nej voľba ***NOD32*** štartuje prácu tohto systému (Obrázok č. 5.2).



Obrázok č. 5.1 Štandardné umiestnenie programu NOD32 v ponuke Štart



Obrázok č. 5.2 Aplikačné okno programu NOD32

5.1 Popis prostredia aplikácie

Aplikácia beží v klasickom okne. Využijeme znalosti z používania programov priamo od firmy Microsoft na to, aby sme sa aj v nej dokázali zorientovať. Je vytvorená pre prostredie ***MS Windows***, avšak je od úplne iného výrobcu.

V prípade takýchto aplikácií je dodržanie štandardných spôsobov pri prístupe k programu čiste len na jeho tvorcovi. Ak je ochotný prispôsobiť sa akýmsi - samozrejme nepísaným

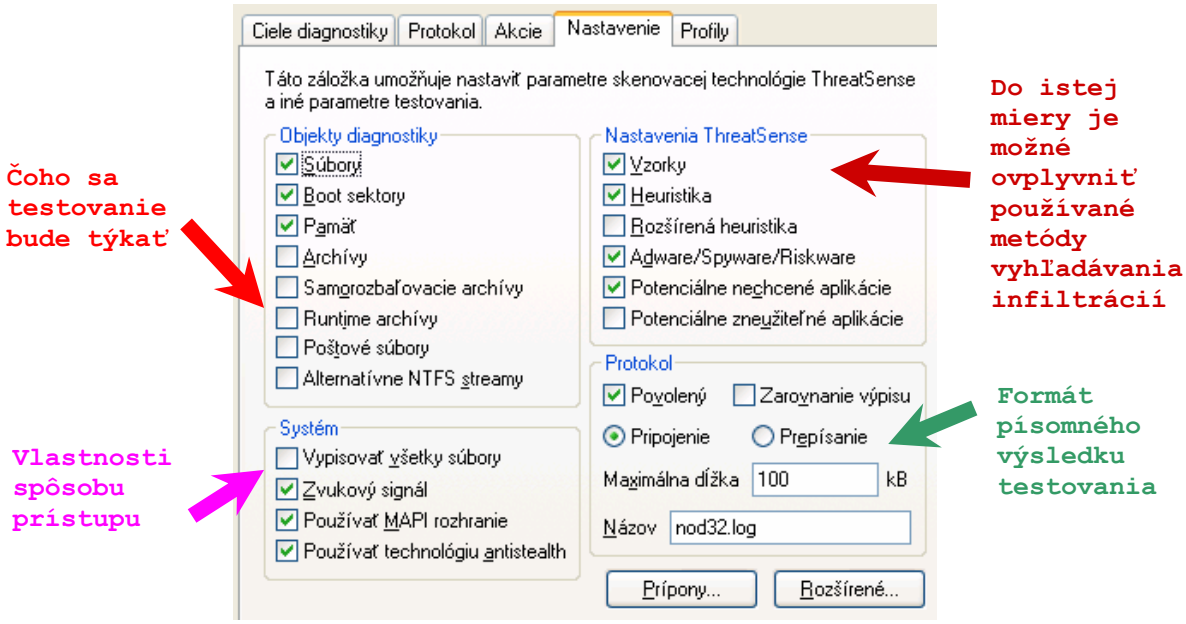
pravidlám, uľahčí používateľom svojich programov prístup k nim. Pokiaľ si vytvorí rýdzo vlastné spôsoby ovládania, môže to byť brzdou rozširovania tohto produktu. Či sa nám to páči alebo nie, produkty firmy Microsoft pokrývajú väčší podiel trhu, ako ktorékoľvek iné. Používatelia si teda prirodzene zvykajú na ich ovládanie. Pri stretnutí s iným programom intuitívne hľadajú známe spôsoby ovládania. Nie sú veľmi ochotní vracať sa do čias ***MS-DOS***u, kedy sa každá aplikácia riadi svojsky.

Z operačného systému teda už poznáme základné časti klasického (aplikačného) okna.

- Na hornom okraji okna rozlišujeme **hlavičku s trojicou tlačidiel** na minimalizáciu, maximalizáciu a uzatvorenie okna programu.
- **Hlavné menu aplikácie** je nahradené systémom záložiek. Ich názvy priamo sprístupňujú funkcie, ktoré zastupujú. Pracovnú plochu teda pokrýva vybraná záložka s jej funkciami.
- Vzhľadom na použitý systém záložiek, ovládanie je doplnené **tlačidlami** pre potvrdenie či doplnenie parametrov.

5.1.1 Nastavenie prostredia aplikácie

Skôr ako prvý krát použijeme program, je vhodné pozrieť sa, ako má nastavené svoje vlastné parametre, ktoré samozrejme ovplyvnia výsledok jeho činnosti. Nájdeme ich v záložke **`Nastavenie`** (Obrázok č. 5.3), ale tiež aj v záložke **`Akcie`** (Obrázok č. 5.4).



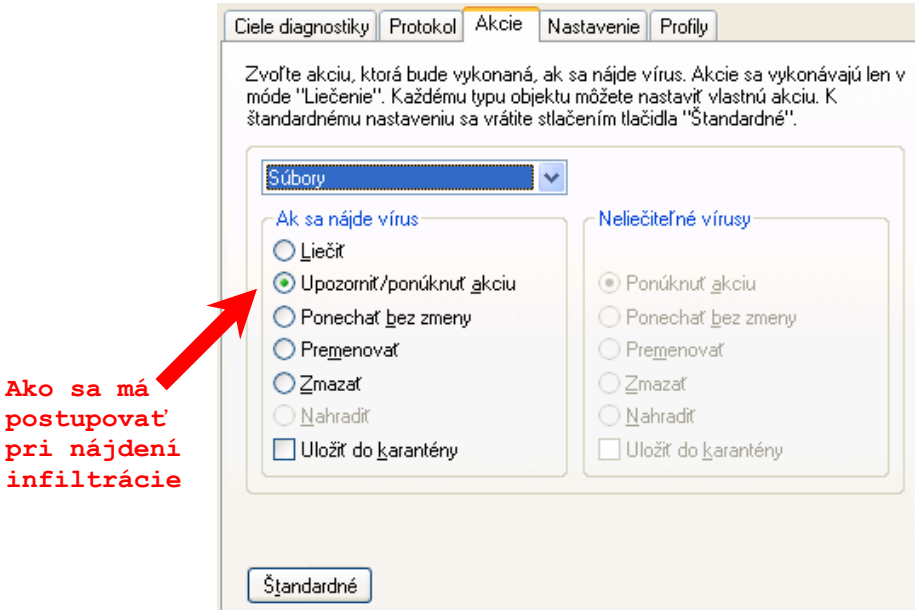
Obrázok č. 5.3 Nastavenie vlastností programu NOD32

- **`Nastavenia`**

V tejto záložke riadime v podstate účinnosť vyhľadávania infiltrácií. Ovplyvňujeme rozsah kontroly (ktorých súborov a kde umiestnených sa testovanie bude týkať) a do istej miery si volíme aj metódu vyhľadávania (napr. používanie heuristickej analýzy – čím môže dochádzať aj k falošným poplachom).

- **`Akcie`**

Ovplyvňujeme úkon, ktorý sa má vykonať s nájdenou infiltráciou. Pomocou tohto nastavenia riadime razanciu postupu – od nulového zásahu, po odstránenie bez výzvy. Treba si vždy uvedomiť dôsledky nastaveného prístupu.



Obrázok č. 5.4 Nastavenie úkonov programu NOD32

5.1.2 Profil

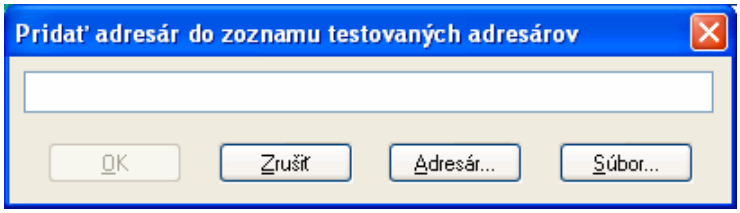
Požadované vlastnosti môžeme zoskupiť do jedného celku a označiť názvom, čím vytvoríme tzv. **profil**. Ten zrýchli a do istej miery zjednoduší prístup ku konkrétnej skupine nastavení. Môže sa využiť napr. pri nastavení automatického testovania.

5.2 Testovanie

5.2.1 Konkretizovanie testovania

Pri samotnom testovaní musíme zvoliť disk, ktorý chceme kontrolovať, výberom v hornej časti okna so záložkou **`Ciele diagnostiky`** (Obrázok č. 5.2). Bude kontrolovaný ten, ktorý má na svojej ikone červené zaškrtnutie. Jednotlivo sa označia alebo odznačia pomocou úkonu 2xĽT myši.

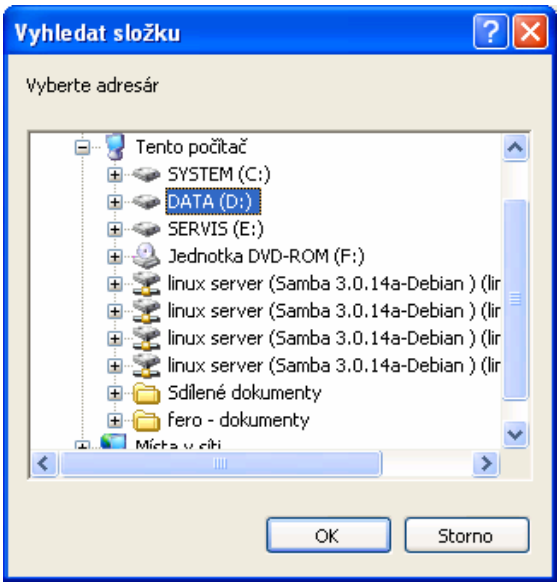
V rámci štruktúry dokážeme zvoliť pre potreby testovania iba konkrétny priečinok či súbor, pokiaľ nechceme kontrolovať celý obsah disku. Selekcia sa sprístupní prostredníctvom tlačidla **`Pridať...`**, ktoré vedie ku dialógovému oknu (Obrázok č. 5.5).



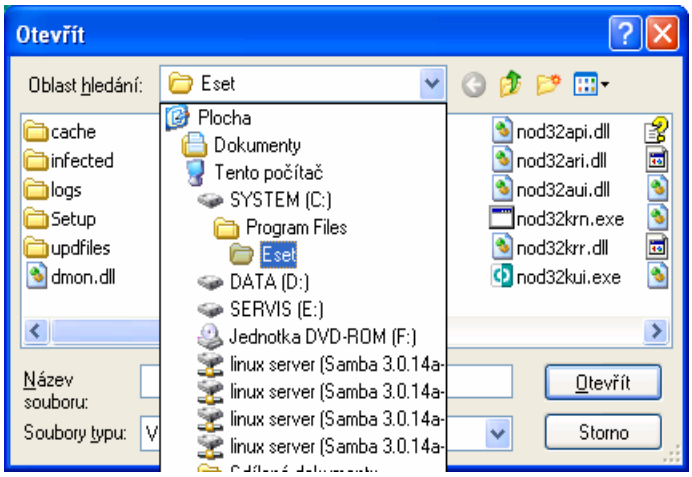
Obrázok č. 5.5 Možnosť výberu priečinku alebo súboru na testovanie

Tlačidlom **`Adresár...`** vykonávame selekciu priečinku, ktorého obsah chceme overiť voči možnej infiltrácii. Vedie ku dialógu (Obrázok č. 5.6), v ktorom sa preklikáme ku stanovenému cieľu.

Tlačidlom **Súbor...** si v prípade potreby vyberáme na testovanie súbor (Obrázok č. 5.7).



Obrázok č. 5.6 Výber priečinku na testovanie

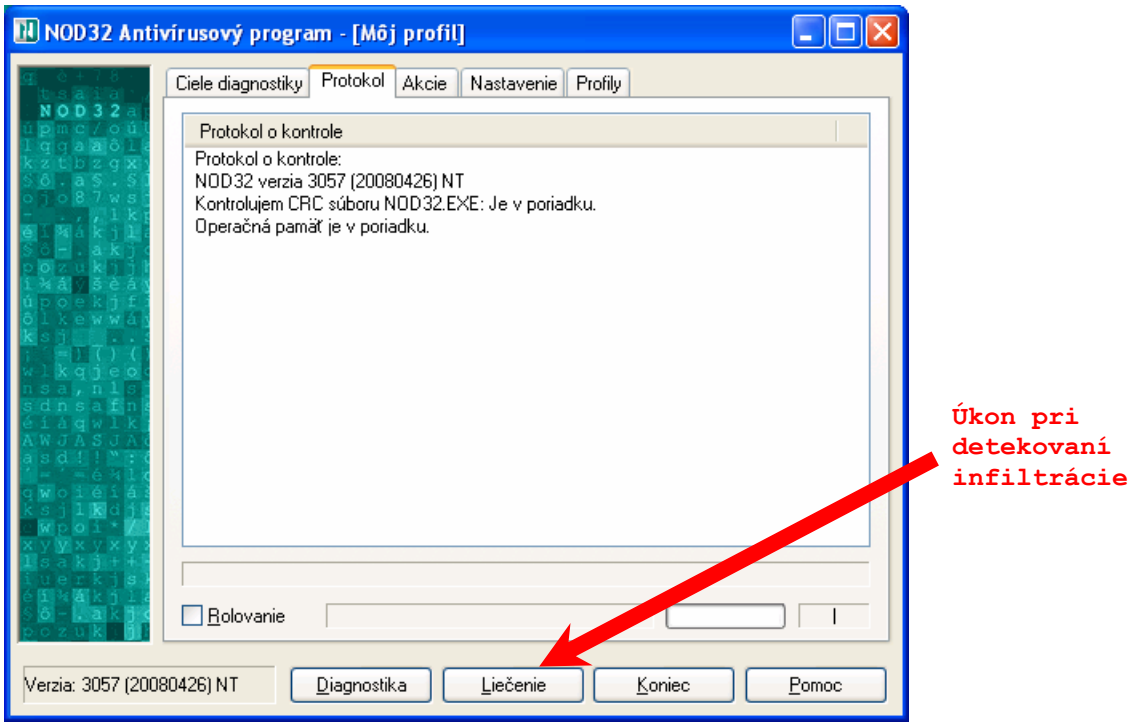


Obrázok č. 5.7 Výber súboru na testovanie

Testovanie sa štartuje tlačidlom **Diagnostika**. Môže trvať aj niekoľko minút – závisí to od množstva súborov, ktoré je nutné prekontrolovať.

5.2.2 Výsledky testovania

Výsledky testovania sa zobrazia na záložke **Protokol**. Po každom odštartovaní programu sa prekontroluje operačná pamäť, čo je uvedené aj v protokole (Obrázok č. 5.8).



Obrázok č. 5.8 Výsledok testovania

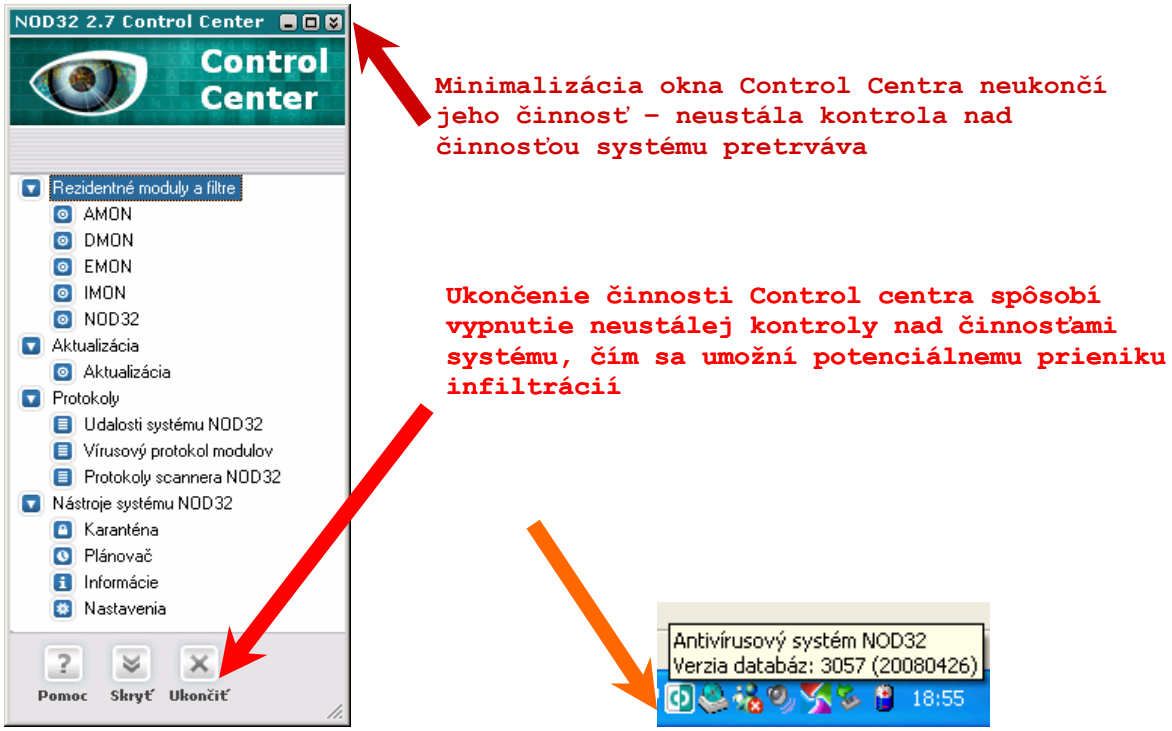
5.3 Liečenie

Ak testovanie odhalilo infiltráciu, liečenie sa pokúsi odstrániť ju. Ak je úspešné, systém sa vyčistí od škodiacich programov. Pri neúspešnom pokuse, máme k dispozícii karanténu (viď stranu 28).

5.4 NOD32 Control Center

Program ***NOD32 Control Center*** je rovnako dostupný z programovej skupiny ***Eset***. Je zvláštny tým, že okrem iného zabezpečuje činnosť rezidentných modulov v systéme, preto musí bežať neustále – ak má systém strážiť, a teda na mieste ukončovacieho tlačidla na hlavičke jeho okna je minimalizačné tlačidlo v inej podobe (Obrázok č. 5.9). Program je typický svojou ikonou na paneli aktívnych úloh vpravo (Obrázok č. 5.10).

Jeho ukončenie musí používateľ vykonať vedome tlačidlom v spodnej časti okna. Tým však vypne priebežnú ochranu systému proti infiltráciám.



Obrázok č. 5.9 Okno NOD32 Control Center

Obrázok č. 5.10 NOD32 v systéme beží rezidentne

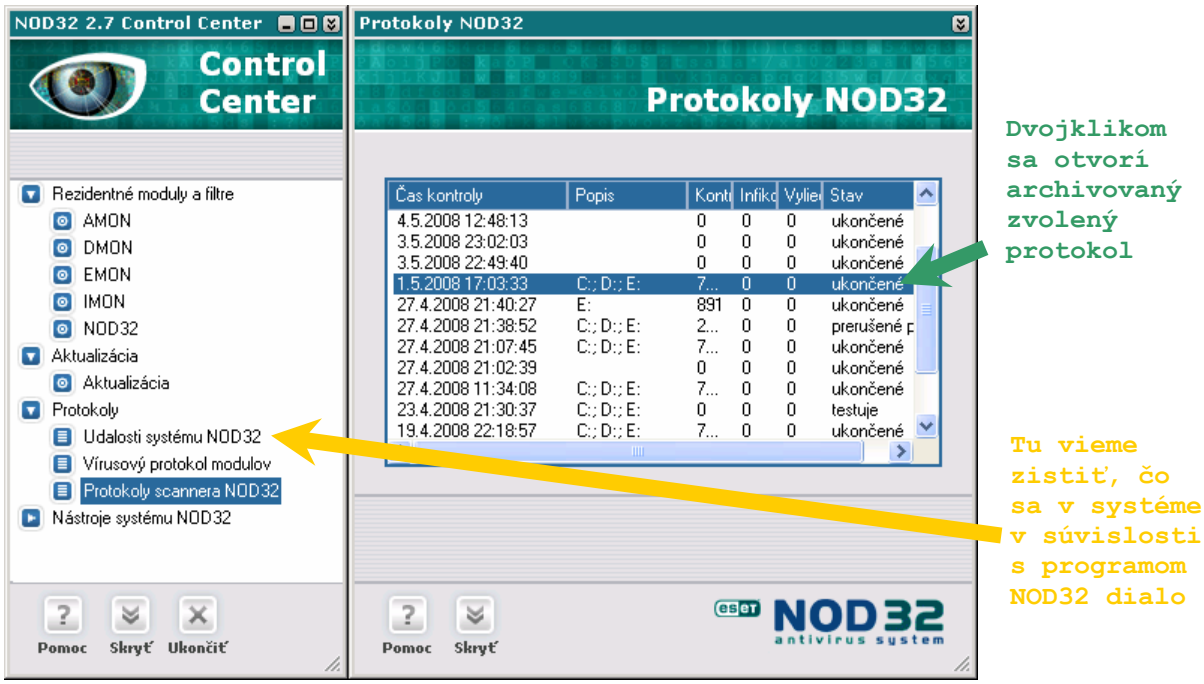
5.4.1 Archív protokolov

Protokoly o testovaní systému sa archivujú a dokážeme sa vrátiť ku výsledkom testov staršieho dáta (Obrázok č. 5.11) prostredníctvom ponuky **`Protokoly`**.

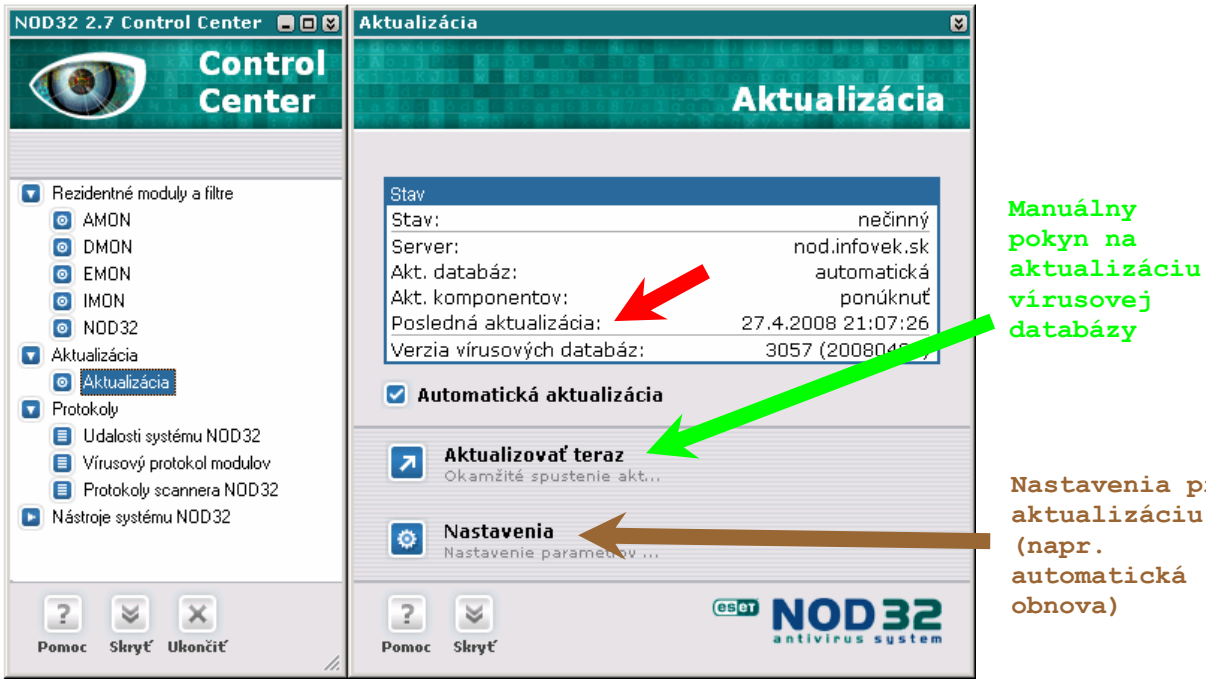
5.4.2 Aktualizácia vírusovej databázy

Je to dôležitá informácia hlavne vtedy, ak náš počítač nie je pripojený k internetu trvale. Vírusová databáza teda nie je aktualizovaná priebežne. Prenosu súborov sa však nedá zamedziť

(médiami, USB kľúčmi), kontrola systému je každopádne namieste aj v takomto prípade. Kontrolovať ho však so starou databázou nie je veľmi efektívne – nevychytajú sa najnovšie infiltrácie. Preto je zisťujeme dátum poslednej aktualizácie (Obrázok č. 5.12) a z tohto miesta môžeme vykonať aktualizáciu manuálne na pokyn.



Obrázok č. 5.11 Prístup k predchádzajúcim protokolom



Obrázok č. 5.12 Informácia o poslednej aktualizácii vírusovej databázy

5.4.3 Moduly NOD32

V časti **`Rezidentné moduly a filtre`** máme prístup k častiam, ktoré bežia nepretržite a kontrolujú príslušnú skupinu činností v systéme. Používateľa môžu obťažovať

spomaľovaním práce systému. Do istej miery je možné znížiť toto nepohodlie rozumným nastavením parametrov.

AMON

Zabezpečuje neustálu kontrolu systému. Sleduje všetky akcie pri prístupe k súborom (štartovanie, otváranie, kopírovanie, premenovanie súborov), čím odhalí už pokus o prienik infiltrácie. Patrí k modulom označovaným ako **on-access scanner** (automaticky spúšťaný pri prístupe k súboru).

DMON

Modul, ktorý kontroluje dokumenty pred pokusom o ich otvorenie. Je zameraný iba na dokumenty, vytvorené aplikáciami balíka ***MS Office*** (verzia 2000 a vyššia).

EMON

Modul je určený na kontrolu pokusu o infiltráciu pomocou niektorých klientov elektronickej pošty (napr. ***MS Outlook***).

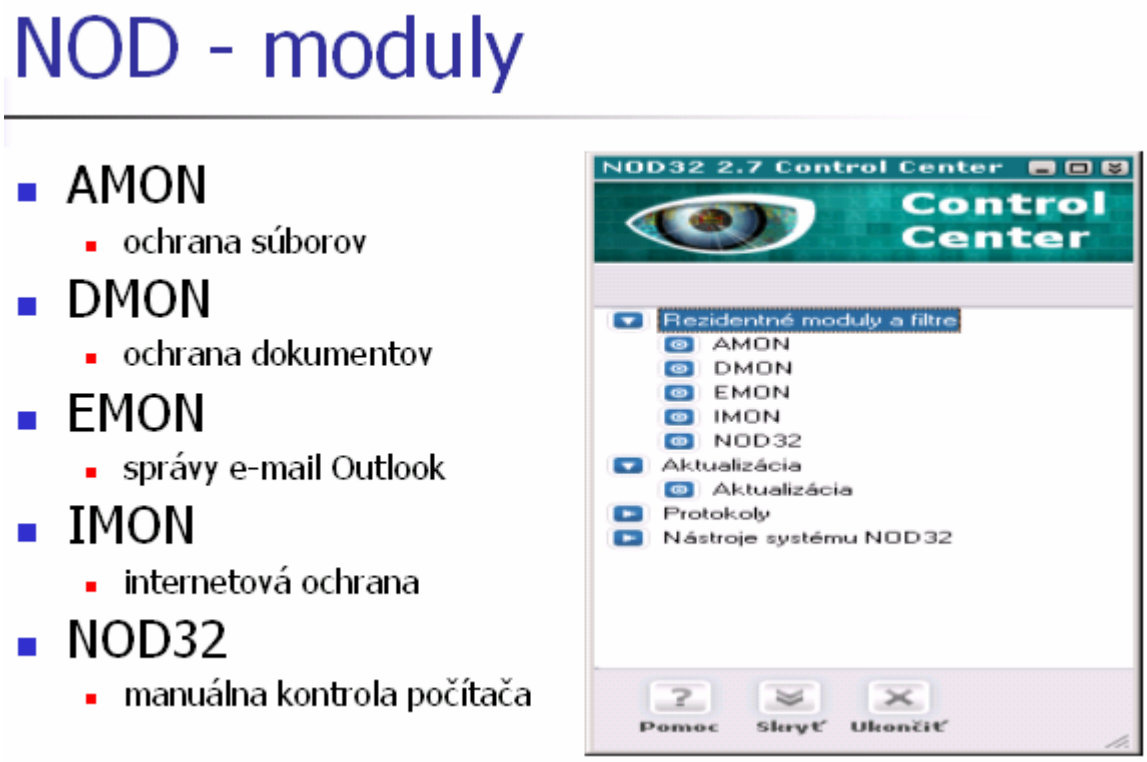
IMON

Internetový monitor sleduje komunikáciu počítača s internetom. Odhalí možné pokusy o prienik z webu či elektronickej pošty z ľubovoľného klienta.

NOD32

On-demand scanner – kontrola systému na pokyn používateľa. Otvára okno aplikácie NOD32 (Obrázok č. 5.2).

Prehľad



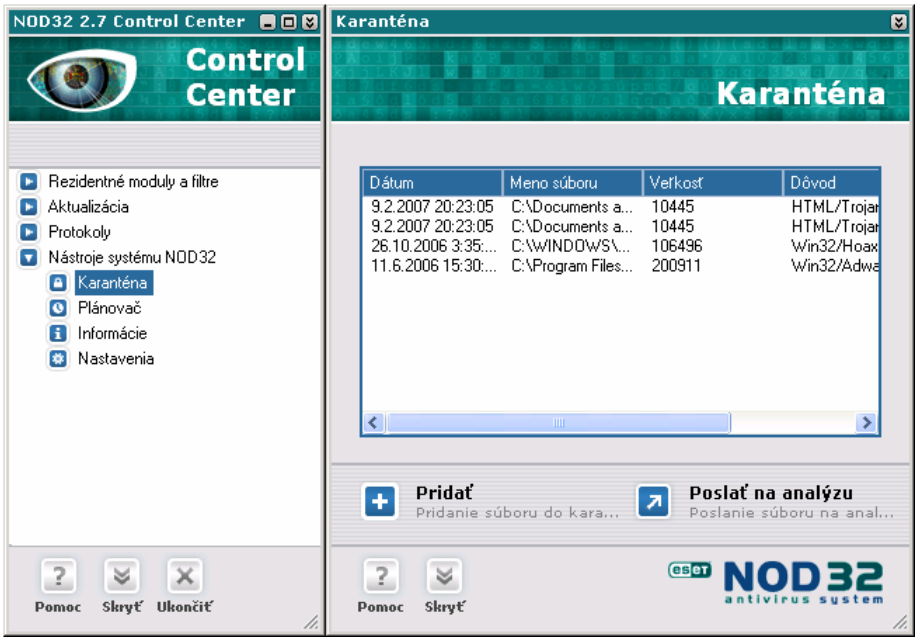
5.4.4 Nástroje systému NOD32

Ponúkajú prístup k častiam, ktoré nesú informácie o

- spôsobe a frekvencii testovania (**Plánovač**),
- podrobných informáciách a nastaveniach,
- karanténe.

Karanténa

Priestor, kam sa presúvajú súbory, ktoré nie je možné zbaviť infiltrácií v aktuálnej dobe sa nazýva karanténa (Obrázok č. 5.13). Tu môžu počkať na novú aktualizáciu vírusovej databázy, čím sa zvýši šanca na ich vyliečenie bez nebezpečenstva pre systém.



Obrázok č. 5.13 Informácia o soboroch v karanténe

Prehľad



Záver

Hrozbu zo strany škodiacich programov rozumný používateľ v žiadnom prípade nezľahčuje. Keďže internet je najväčším zdrojom informácií, je tiež najväčším zdrojom infiltrácií. Ak sa svojim počítačom k tejto rozsiahlej sieti pripájame, určite je rozumné používať účinný antivírus s pravidelne obnovovanou vírusovou databázou.

Zoznam literatúry

Elektronické zdroje

Antispyware. 2008. [online] : Antispyware, 2007 [cit. 2008-05-02]. Dostupné na internete: <http://www.antispyware.sk>

COTO.JE [online] : [cit. 2007-06-18]. Dostupné na internete: <http://coto.je>

Eset. 2008. [online]. [cit. 2008-05-02]. Dostupné na internete: <http://www.eset.sk/sk>

Virusy. 2008 [online] : MLK CompSoft, 2008 [cit. 2008-05-02]. Dostupné na internete: <http://www.virusy.sk/>

Wikipédia Slobodná encyklopédia [online] : 2007 [cit. 2006-11-05]. Dostupné na internete: <http://sk.wikipedia.org>