Antivírus a vírus

Antivírus

- Je softvér ktorého cieľom je identifikovať a eliminovať počítačové vírusy
- Prvý antivírusový systém, schopný ničiť viacero vírusov vznikol v roku 1988
- Najznámejšie AV : NOD32, Avast!, Avira, AVG, Kaspersky, Norton

Zdroje obrázkov : http://www.sharkycomputer.hu/blog/wp-content/uploads/2009/08/NOD32v2logo.jpg, http://softmania.sk/data/stahnu.cz/uploadimages/avast%20-%20navod/Logo.jpg

- **Druhy antivírusov**
- **Jednoúčelové antivírusy**: Sú to antivírusové programy, ktoré sa zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu.
- **On-demand antivírusy:** Zaraďujú sa sem aj internetové on-line skenery. Obvykle sú to rôzne aplety, ktoré v spojení s internetovým prehliadačom dokážu prehľadať pevný disk používateľa.

- **Komplexné antivírusové balíky:** Je väčšinou zložené tak, aby jednotlivé produkty dokázali dohromady kontrolovať vstupné/výstupné miesta siete, ktoré sú pre infiltráciu populárne. Často sa v balení vyskytuje:
- Antivírusový systém pre stanice
- Antivírus pre poštové servery – antispam
- Antivírus pre súborové servery
- Firewall
- Antispyware

- Vírusová databáza je súhrn informácií, na základe ktorých dokáže antivírusový skener vyhľadávať známe vírusy. Vírusová databáza je obvykle označená dátumom vydania. Vďaka nej dokáže antivírusový skener detegovať väčšinu známych vírusov, ktoré vznikli pred dátumom vydania vírusovej databázy. Pravidelnou aktualizáciou je možné zaistiť, že rozdiel medzi súčasným dátumom a dátumom vydania bude čo najmenší a budú tak detegované aj najnovšie prírastky medzi vírusmi.

Zdroj obrázka: http://d2nwkt1g6n1fev.cloudfront.net/helpmax/wp-content/uploads/sub/nod32/sk/source/sshots/ea_update_main.png

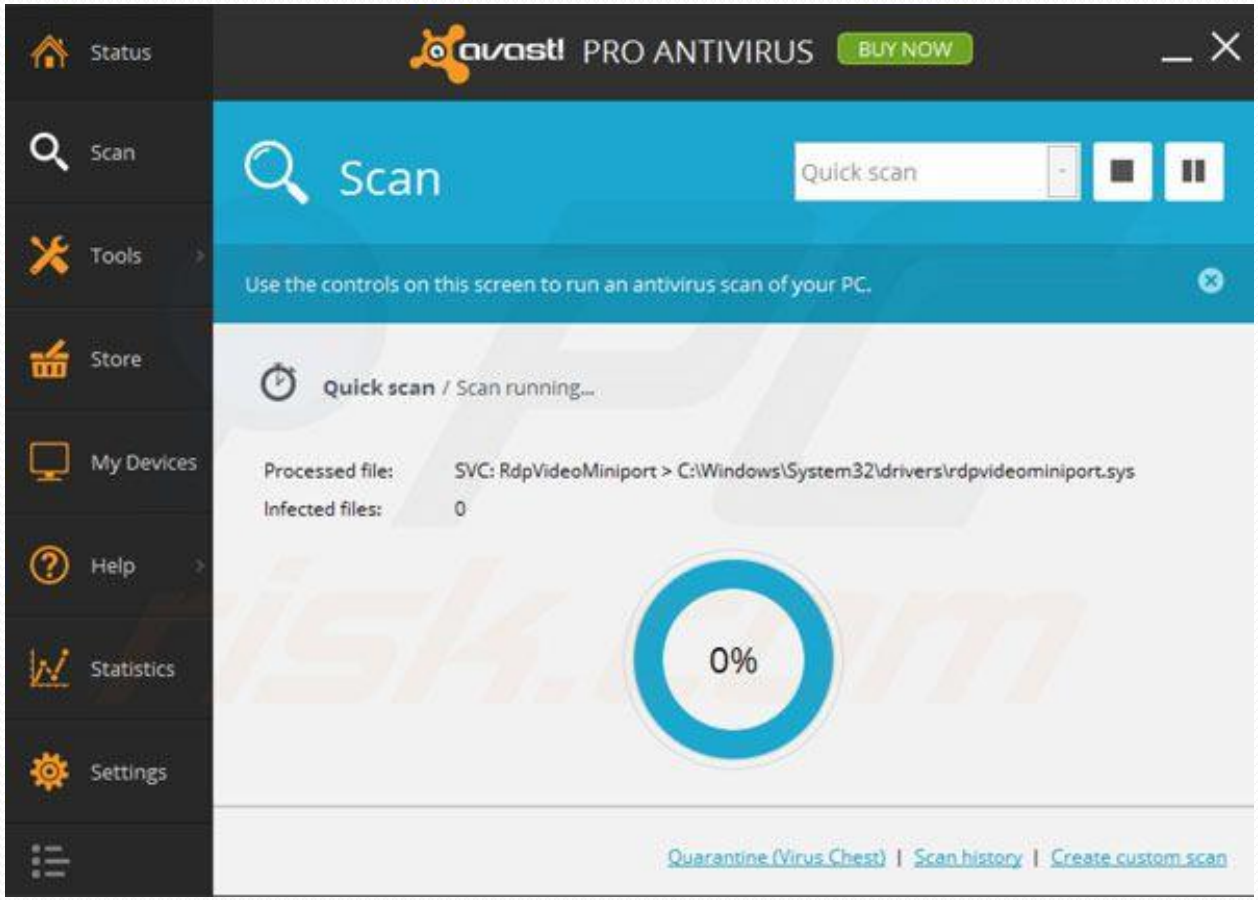
- Hlásenia antivírusov pri zachytení vírusov

Zdroje obrázkov: http://www9.pcmag.com/media/images/235708-comodo-antivirus-5-0-false-positive.jpg
https://security.intuit.com/images/trojanhorse.jpg

- Heuristická analýza je rozbor kódu hľadajúc postupy pre činnosť typickú pre vírusy. Takto možno odhaliť aj dosiaľ neznáme vírusy. Zatiaľ čo zástancov tejto analýzy tešila možnosť detekcie neznámych vírusov, odporcovia sa obávali zvýšeného počtu falošných poplachov. Dnešná heuristická analýza je natoľko prepracovaná, že výskyt falošného poplachu je skôr náhodou.

Zdroj obrázka: http://www.freecomputermaintenance.com/wp-content/uploads/2012/01/virus-detected.jpg

- Falošné poplachy – false positive
- Za falošný poplach označujeme situáciu, keď antivírus deteguje vírus aj keď v skutočnosti o žiadny nejde. Okolnosti, ktoré môžu viesť k falošným poplachom a zároveň k znehodnoteniu celého antivírusu:
- Použitie krátkych sekvencií na detekciu vírusov.
- Použitie nesprávnych sekvencií na detekciu vírusov.
- Zvýšenie citlivosti antivírusu za účelom zvýšenia úspešnosti detekcie môže mať aj opačný efekt. Príkladom je „precitlivená“ heuristická analýza.



- Ukážka skenu vírusov v Avast! Antivirus

Zdroj obrázka: http://images.pcrisk.com/stories/av2014/avast-2014-quick-scan.jpg

Ďakujem za pozornosť

Zdroj textu: http://sk.wikipedia.org/wiki/Antiv%C3%ADrusov%C3%BD_softv%C3%A9r