Jen „technická“ ochrana nestačí

Ing. Jindřich Hlaváč, CISA
hlavac@dcit.cz
DCIT, a.s., http://www.dcit.cz

Statistika nuda je…

Statistika „technologií“

- 98 % uživatelů PC používá antivirový program
- 70 % uživatelů používá personální firewall a antispyware
- 90 % firem používá antimalware SW
- 75 % firem a organizací v rámci IT řeší systematicky filtraci obsahu (web, pošta)

- 42 produktů bojuje v posledním testu Virus Bulletinu o VB100 ocenění (63 v databázi VB)
- 80 milionů registrovaných uživatelů free verze Avast!

Zdroj: Factum 2008, Skodlivysoftware.cz, www.virusbtn.com

… má však cenné údaje! (1)

- Proč se tedy situace stále zhoršuje?

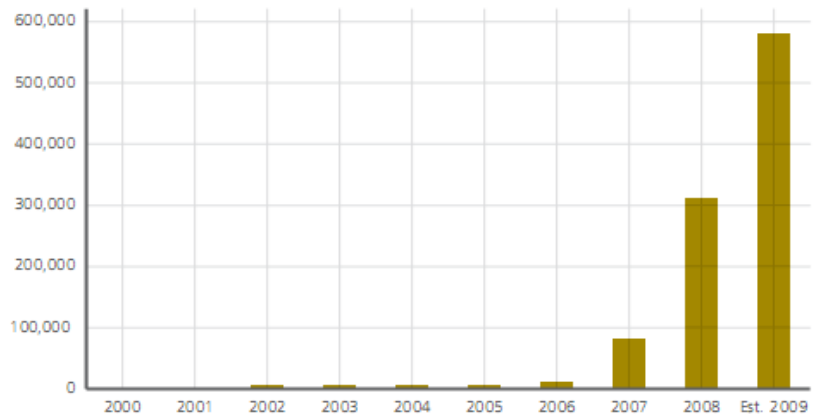


Figure 23: Growth in Password-Stealing Malware

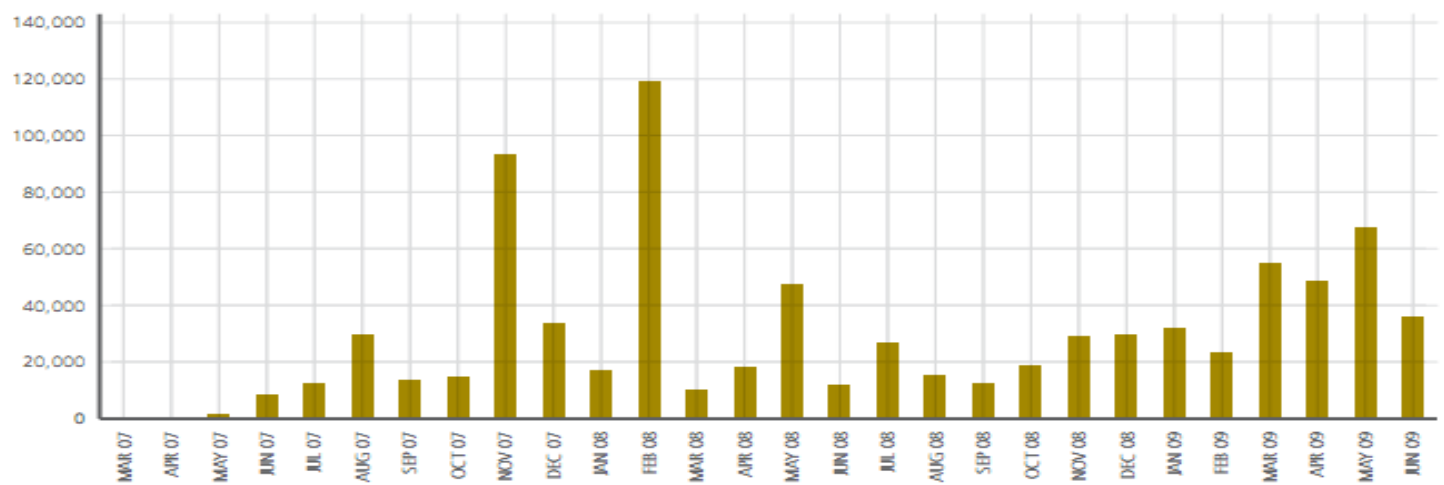
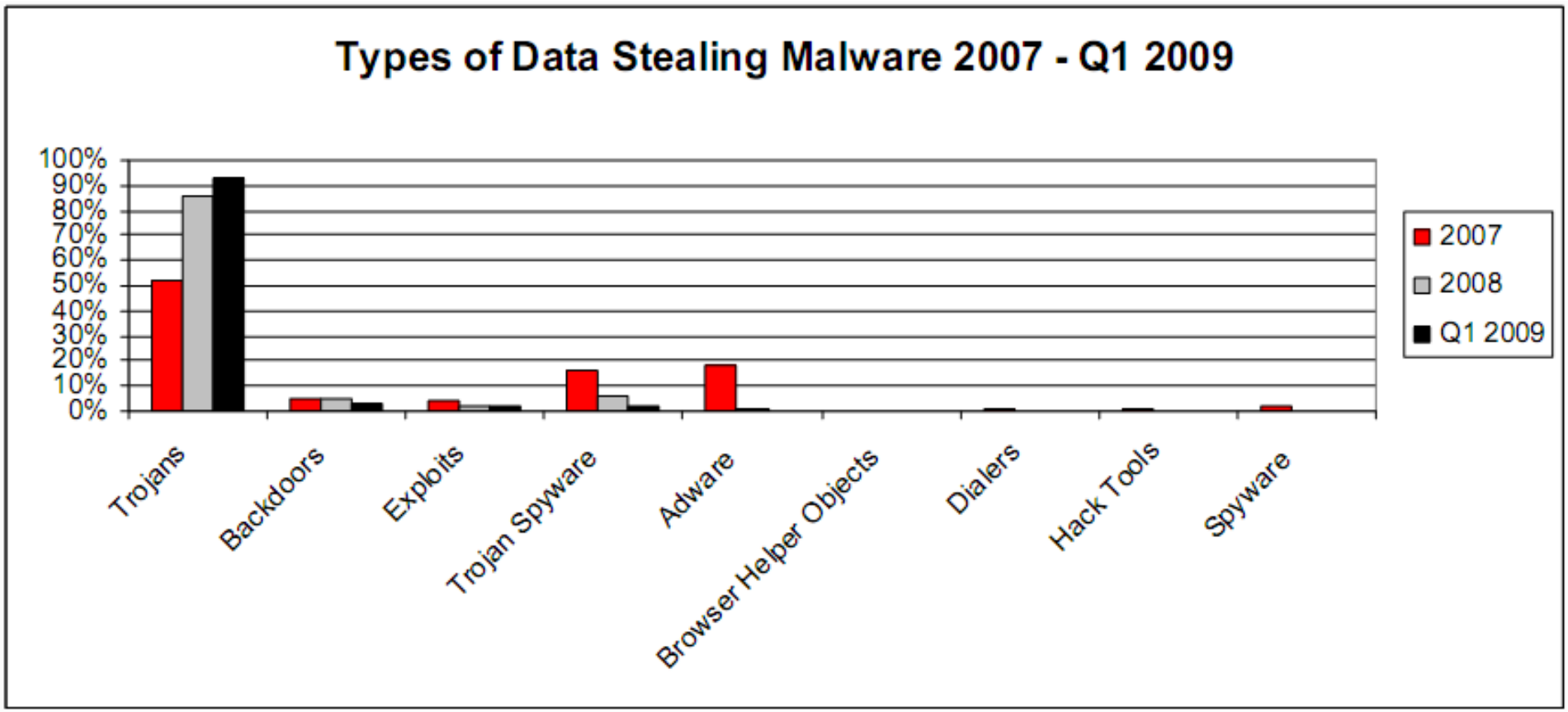


Figure 30: Unique AutoRun Malware Binaries Discovered, by Month.

Zdroj: http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709.pdf

… má však cenné údaje! (2)

- „Náklady firem na únik dat vzrostly průměrně na $ 202/záznam v roce 2008 (růst o 2,5 % oproti roku 2007 a o 11 % oproti roku 2006).“



Zdroj: Trend Micro (June 2009)

Hrubá síla technologií nestačí – o tom se bude snažit vás přesvědčit tento příspěvek.

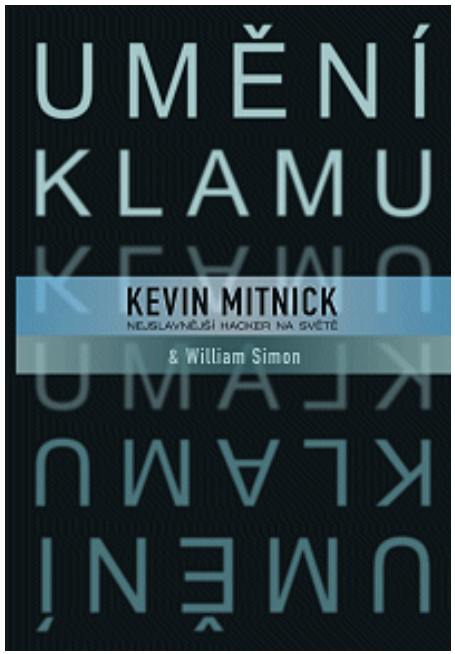
Sociální inženýrství

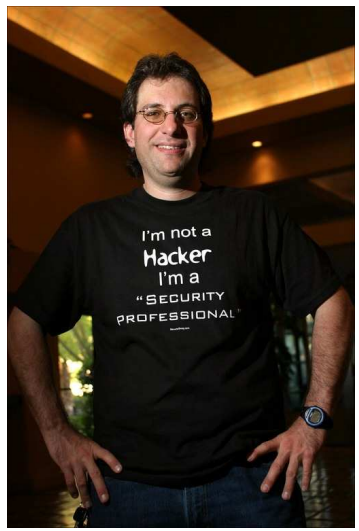
Sociotechnika = přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili že jste někdo jiný a zmanipulovat je k vyzrazení některých informací nebo provedení určitých úkonů.

- Termín „proslavil“ Kevin Mitnick (phreaking)
- Účelem přesvědčit: spusťte, řekněte…

- Cílem jsou především **autentizační údaje** (a všechny informace, které lze zpeněžit)
- Neoprávněné požadavky (na soubor kolegy, údaje k VPN, email mimo společnost…)
- Fyzický průnik: velké firmy, kurýr, opravář…

- Nejznámějším a nejčastějším příkladem je nyní phishing a trojské koně





Phishing, pharming

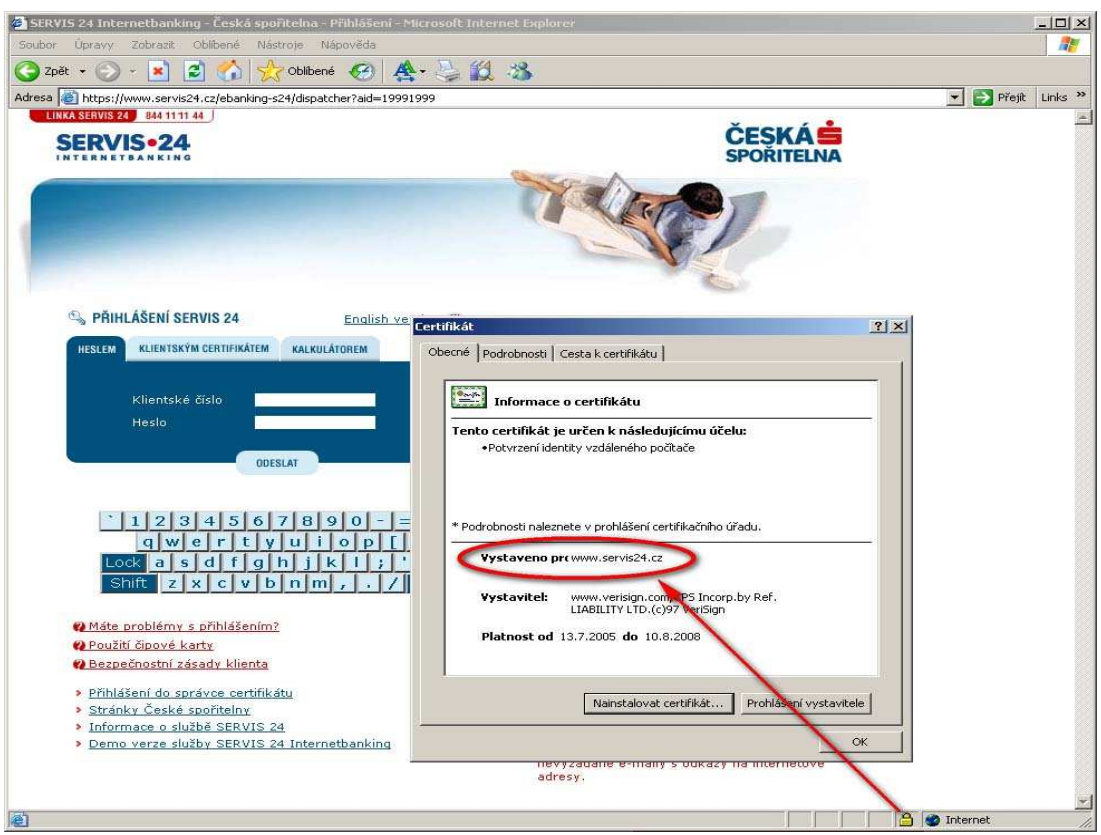
- ***Phishing*** *(rhybaření) = nevyžádaný email vyzývající k poskytnutí důvěrných osobních informací, nejčastěji prostřednictvím falešné webové stránky, za účelem podvodu.*
- ***Pharming*** *= napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné webové stránky (za účelem podvodu).*

- **Cíl:** autentizační a bankovní údaje (jména, hesla, čísla účtů a čísla karet, osobní údaje) – vše za účelem podvodu a finančního obohacení.
- **Důvod**: dle fy Gartner: V roce 2007 škody za $ 3.2 mld (2,3 miliardy v roce 2006), měsíčně 2.2 mld emailů, 1 % phishingu je úspěšné !
  V roce 2009 oproti situaci před rokem vzrostl počet obětí asi o 40 %.
- **Proč je úspěšný**: jazykové mutace, neznalost uživatelů, *whaling* a *spear phishing*.

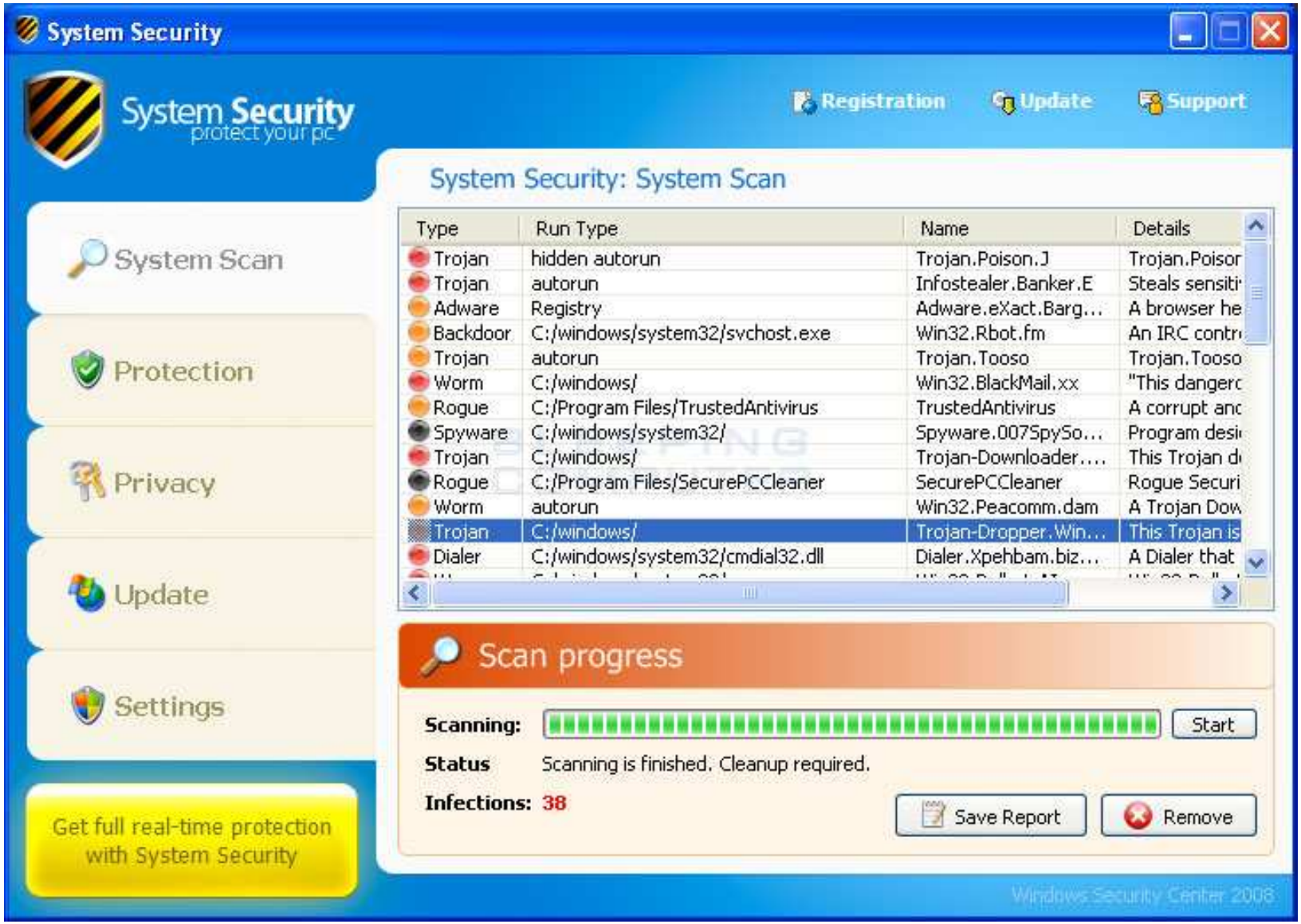
© Scott Adams, Inc./Dist. by UFS, Inc.

Phishing, pharming – obrana

- Zdravý rozum, školení
- Kontrola URL (omezená účinnost)
- Preferovat šifrovaná spojení, kontrolovat certifikát
- Anti-phishing technologie v prohlížečích
- Doplňky prohlížečů (NetCraft, AVG)



Poznáváte?


System Security
System Security
protect your pc
Registration
Update
Support
System Security: System Scan
System Scan
Protection
Privacy
Update
Settings
Get full real-time protection with System Security
Type
Run Type
Name
Details
Trojan hidden autorun Trojan.Poison.J Trojan.Poisor
Trojan autorun Infostealer.Banker.E Steals sensiti
Adware Registry Adware.eXact.Barg... A browser he
Backdoor C:/windows/system32/svchost.exe Win32.Rbot.fm An IRC contr
Trojan autorun Trojan.Tooso Trojan.Tooso
Worm C:/windows/ Win32.BlackMail.xx "This dangerc
Rogue C:/Program Files/TrustedAntivirus TrustedAntivirus A corrupt anc
Spyware C:/windows/system32/ Spyware.007SpySo... Program desi
Trojan C:/windows/ Trojan-Downloader.... This Trojan d
Rogue C:/Program Files/SecurePCCleaner SecurePCCleaner Rogue Securi
Worm autorun Win32.Peacomm.dam A Trojan Dow
Trojan C:/windows/ Trojan-Dropper.Win... This Trojan is
Dialer C:/windows/system32/cmdial32.dll Dialer.Xpehbam.biz... A Dialer that
Scan progress
Scanning:
Start
Status
Scanning is finished. Cleanup required.
Infections: 38
Save Report
Remove
Windows Security Center 2008

Falešný software

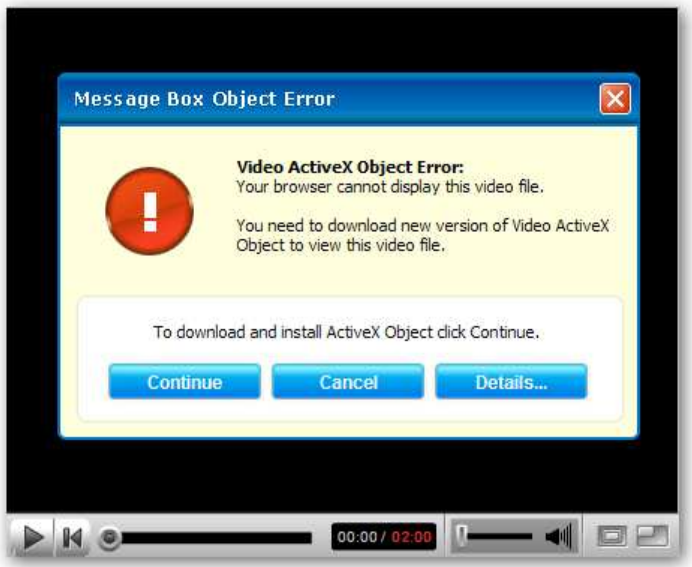
- Stále populárnější forma sociálního inženýrství

- Falešný software
  - „Videokodeky“
  - „Bezpečnostní aplikace“, tzv. *rogue anti-malware*
    http://en.wikipedia.org/wiki/Rogue_security_software

- V čem je problém? Vždyť jste si ho sami pozvali…

- Co dělá?
  - Deaktivuje instalovaný antivir, firewall,…
  - Naleznou imaginární „škodnou“
  - Chce zaplatit za odstranění („registrace produktu“)
  - Problémy s odstraňováním, ale je to možné

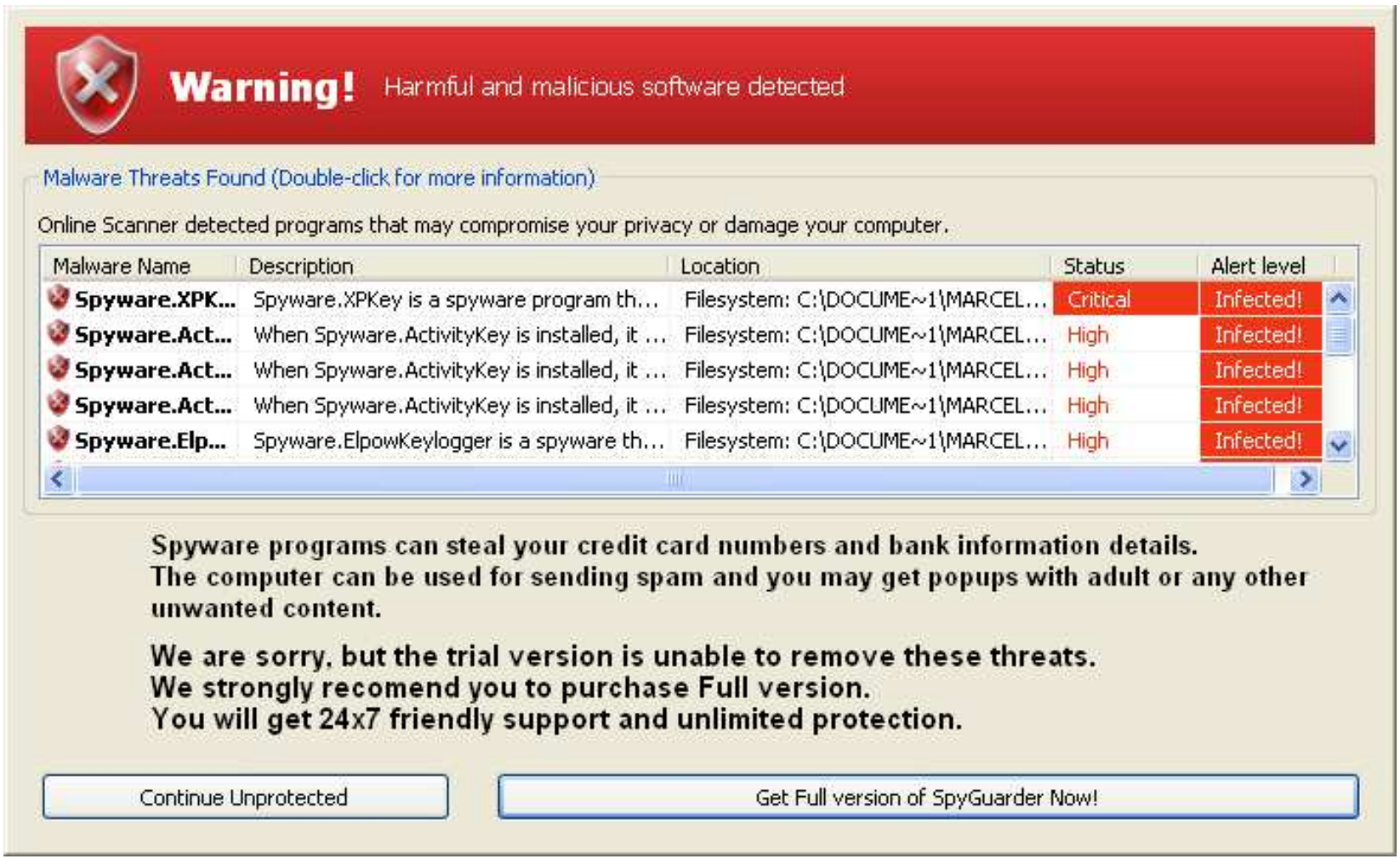
- Jak se bránit?
  - Neinstalovat žádný bezpečnostní SW zdarma, pokud jej dobře neznáte
  - V případě příznaků nakládat s počítačem jako se zavirovaným (ve firmě nahlásit)
  - Aktualizovaný prověřený bezpečnostní produkt



Rank	Region
1	Spyware Guard 2008
2	AntiVirus 2008
3	AntiVirus 2009
4	Spyware Secure
5	XPAntivirus
6	WinFixer
7	SafeStrip
8	Error Repair
9	Internet Antivirus
10	DriveCleaner

Table 2. Top reported rogue security software
Source: Symantec

Rogue antimalware – další ukázky



Trojské koně

- Co je trojský kůň?
  a) Bojový prostředek Řeků při dobývání Tróje.
  b) Program (či jeho část) skrytá uživateli vykonávající na pozadí běžných funkcí nežádoucí (škodlivou) činnost.

- Možnosti trojských koní
  – Sběr a odesílání dat o počítači a uživateli
  – Sběr a odesílání vybraných souborů
  – Sledování uživatele či sítě v reálném čase (autentizační údaje)
  – Eskalace práv a ovládnutí počítače

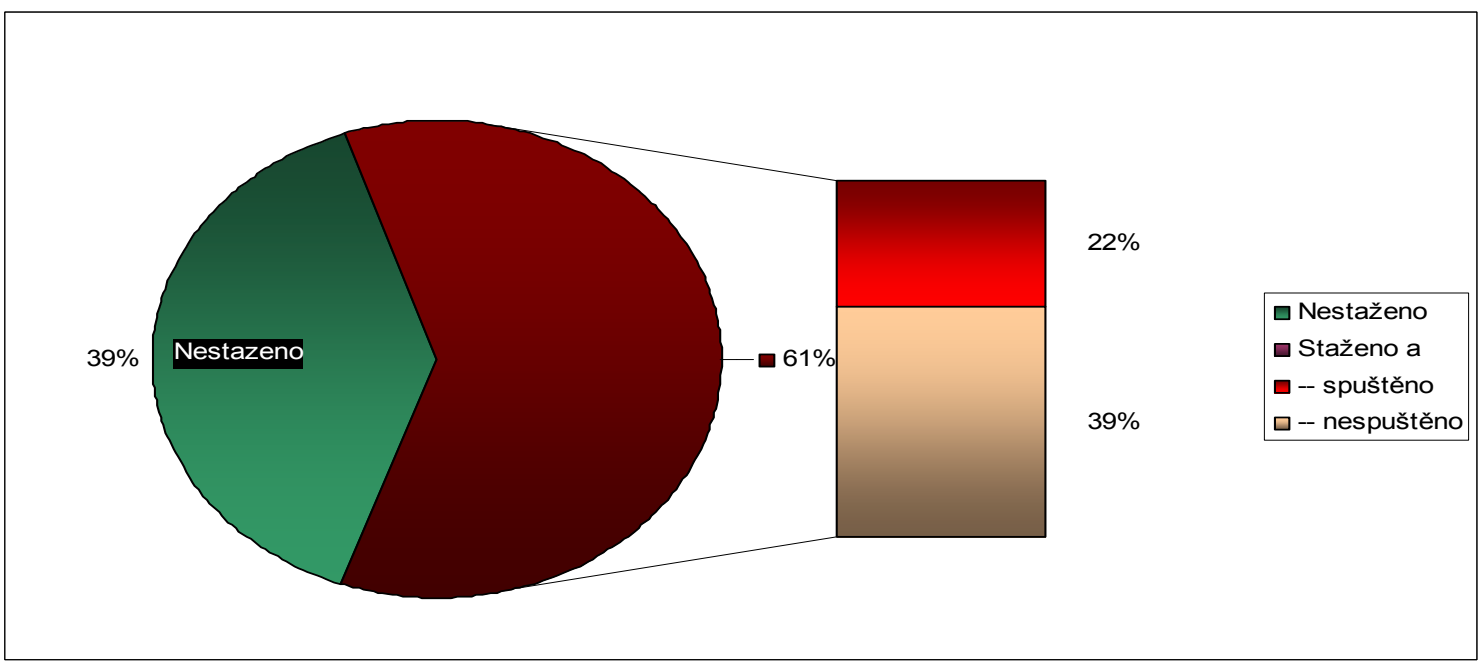
Trojské koně z pozice útočníka

- Jak ho dostat k uživateli
  - Web (P2P sítě, warez, erotika)
  - Email (jen odkaz)
  - Fyzicky (flash disk, CD), zejména soutěže a jiné marketingové akce
- Je třeba vyřešit odesílání dat útočníkovi
  - Běžné http (GET, POST)
  - BITS
  - Opakované DNS dotazy
- Speciality
  - Omezená životnost
  - Sebedestrukce

Trojský kůň - statistiky

- Společnost A
  - Trojský kůň emailem (odkaz na EXE a ZIP)
  - Trojský kůň na CD (veřejně dostupná místa)
  - Možnost výhry

Údaj	Hodnota
Odesláno emailem	780
Email - Prokazatelně staženo	61 %
Email - Prokazatelně spuštěno	**22 %**
CD - úspěšnost	5 %
CD - Počet manuálního spuštění trojského koně	75 %
Počet uživatelů zařazených ve skupině *Administrators*	17 (10 %)



Zdroj: DCIT

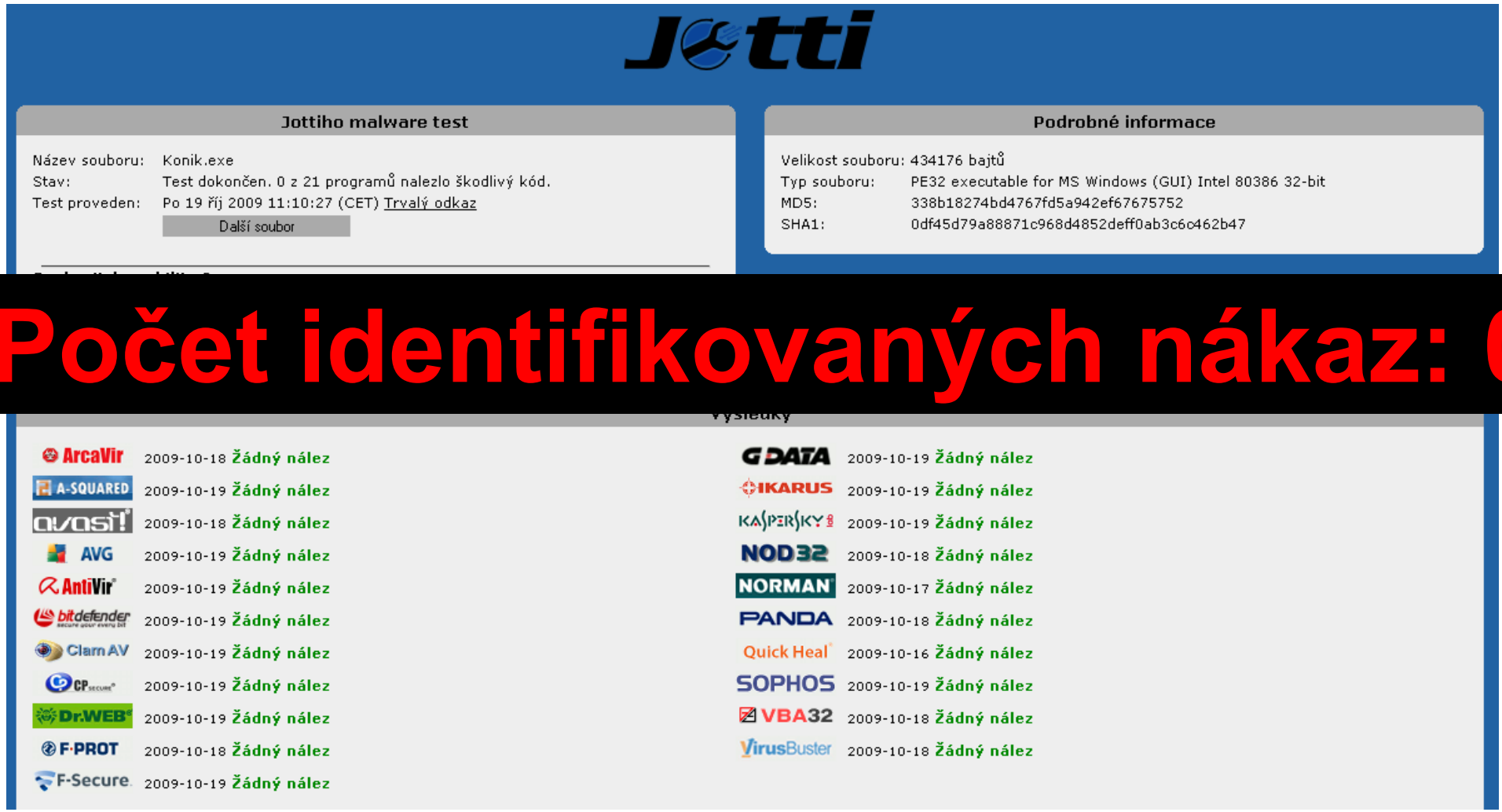
Trojský kůň - statistiky

- Společnost B
  - Trojský kůň na flash disku
  - Zasláno fyzicky poštou
  - Možnost výhry

Údaj	Hodnota
Odesláno flash disků s trojským koněm	100
Počet použitých USB disků	66 (66 %)
Počet jednotlivých spuštění trojského koně	271
Maximální počet uživatelů, kteří spustili trojského koně z jednoho USB flash disku	8
Maximální počet spuštění jednoho trojského koně	22
Počet automatického spuštění trojského koně	58 %
Počet manuálního spuštění trojského koně	42 %
Počet uživatelů zařazených ve skupině *Administrators*	20 (7,3 %)

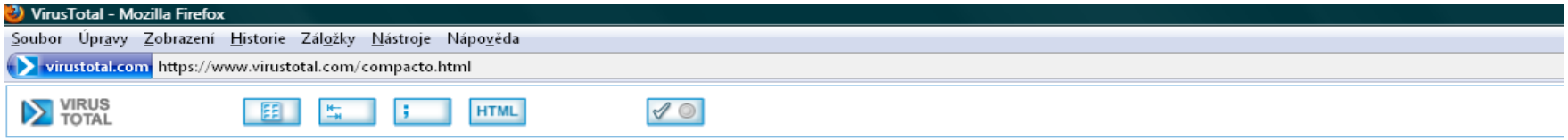
Zdroj: DCIT

Trojský kůň a antiviry (1)



Zdroj: http://virusscan.jotti.org

Trojský kůň a antiviry (2)



Soubor Konik.exe přijatý 2009.10.19 09:18:37 (UTC)

Antivirus	Verze	Poslední aktualizace	Výsledek
a-squared	4.5.0.41	2009.10.19	-
AhnLab-V3	5.0.0.2	2009.10.17	-
AntiVir	7.9.1.35	2009.10.19	-
Antiy-AVL	2.0.3.7	2009.10.19	-
Authentium	5.1.2.4	2009.10.18	-
Avast	4.8.1351.0	2009.10.18	-
AVG	8.5.0.420	2009.10.19	-
BitDefender	7.2	2009.10.19	-
CAT-QuickHeal	10.00	2009.10.18	-
ClamAV	0.94.1	2009.10.19	-
Comodo	2654	2009.10.19	-
DrWeb	5.0.0.12182	2009.10.19	-
eSafe	7.0.17.0	2009.10.18	-
eTrust-Vet	35.1.7074	2009.10.19	-
F-Prot	4.5.1.85	2009.10.18	-
F-Secure	9.0.15300.0	2009.10.16	-
Fortinet	3.120.0.0	2009.10.19	-
GData	19	2009.10.19	-
Ikarus	T3.1.1.72.0	2009.10.19	-
Jiangmin	11.0.800	2009.10.19	-
K7AntiVirus	7.10.872	2009.10.16	-
Kaspersky	7.0.0.125	2009.10.19	-
McAfee	5775	2009.10.18	-
McAfee+Artemis	5775	2009.10.18	-
McAfee-GW-Edition	6.8.5	2009.10.19	Heuristic.BehavesLike.Win32.Trojan.I
Microsoft	1.5101	2009.10.19	-
NOD32	4520	2009.10.18	-
Norman	6.03.02	2009.10.17	-
nProtect	2009.1.8.0	2009.10.19	-
Panda	10.0.2.2	2009.10.18	-
PCTools	4.4.2.0	2009.10.18	-
Prevx	3.0	2009.10.19	-
Rising	21.52.02.00	2009.10.19	-
Sophos	4.46.0	2009.10.19	-
Sunbelt	3.2.1858.2	2009.10.18	-
Symantec	1.4.4.12	2009.10.19	-
TheHacker	6.5.0.2.046	2009.10.19	-
TrendMicro	8.950.0.1094	2009.10.19	-
VBA32	3.12.10.11	2009.10.18	-
ViRobot	2009.10.19.1993	2009.10.19	-
VirusBuster	4.6.5.0	2009.10.18	-

Zdroj: https://www.virustotal.com

Neklesejme na mysli

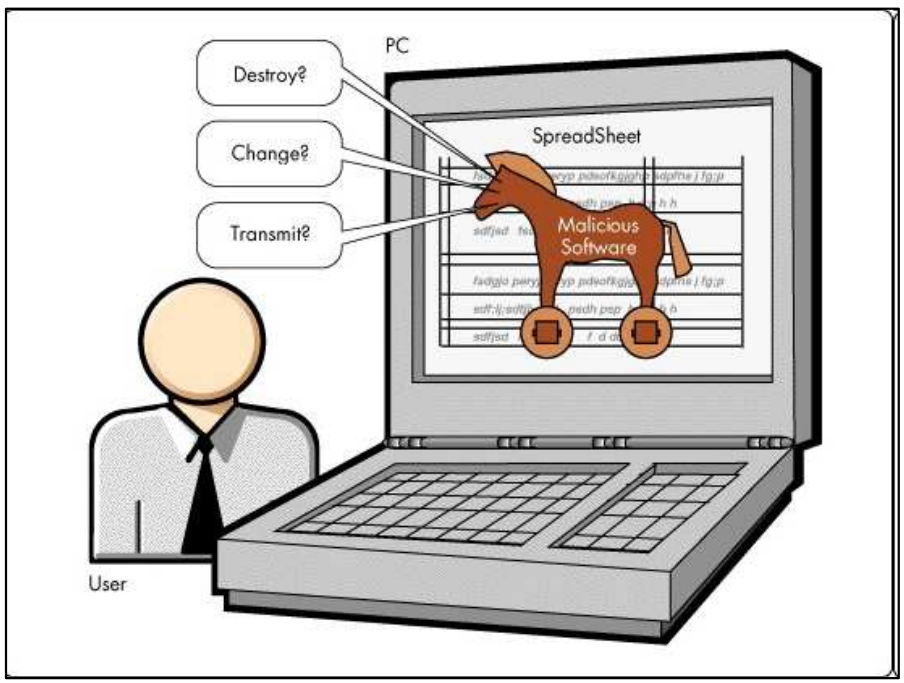
- Technické prostředky jsou základ
  - *Autorun* vypnout doménovou politikou
  - Monitoring/řízení USB portů
  - Omezení stahování spustitelných souborů (content filtering)

  - Aktuální antimalware
  - Aktuální operační systém
  - **Aktuální software třetích stran** (Adobe produkty+Flash, browsery, multimédia)

- Bez „nadstavby“ to ale nepůjde
  - Školení uživatelů v oblasti informační bezpečnosti
  - Omezit používání privilegovaných účtů (zejména skupina *Administrators*)
  - Bezpečnostní dokumentace (směrnice)
  - Kontrola

Testujeme a prověřujeme

- Způsob kontroly trojským koněm
  - Citlivé politické rozhodnutí. Souhlas managementu nezbytný.
  - Pečlivá příprava (cíl, způsob doručení, „respondenti“)
  - Odpovídající vyhodnocení



Citlivá oblast testování a kontroly !

Děkuji za pozornost

- Prostor pro dotazy

- Kontakt
  hlavac@dcit.cz