Základní zabezpečení

Ing. Radomír Orkáč
14.4.2011, Opava

orkac@cesnet.cz

Mě se to netýká ...

„Proč by se chtěl někdo dostat do mého počítače?!”

Neblázni! Jim je úplně jedno, že jsi hodná kachna.
Oni střílejí všechny kachny.

Hrozba

- Šíření malware.
- Útoky na určitý typ slabiny.
- Cílem útočníka je infikovat/napadnout počítač, umožnit vzdálený přístupnit jiným osobám, získat citlivá (osobní) data.
- ...
- Síť napadených počítačů (Botnet)
  - Tisíce počítačů infikovaných stejným botem.
  - Počítače jsou nejčastěji zneužívány k rozesílaní spamu, phishingu, hromadným útokům, nebo také pro ”klikání” na reklamu (pay-per-click).

Hrozba aktuálně

Masmédia:

- Microsoft opraví 64 zranitelností, nový rekord.
- Odstavení botnetu Rustock snížilo množství spamu o třetinu.
- Microsoft varuje uživatele Office před útoky pomocí Flash Playeru.
- Další dva přeprodejci certifikátů byli kompromitováni.
- Útok na stránky americké pošty.
- Zeus - zdrojový kód je nyní prodáván (online) za pět tisíc dolarů.
- ...

Osobní firewall

Jde o bezpečnostní software, který kontroluje komunikaci počítače s ostatními počítači v síti.

Brána firewall Windows Vista/7

- Obousměrná kontrola komunikace.
- Při prvním připojení do neznámé sítě se systém zeptá na síťové umístění počítače. K dispozici jsou celkem tři profily doména, privátní síť a veřejná síť.
- Ve Windows XP SP2 poskytuje brána firewall pouze základní ochranu!

Ostatní firewally:

- Sunbelt Personal Firewall, Comodo Firewall, ESET Smart Security, AVG Anti-Virus plus Firewall

Aktualizace softwaru

Proč software aktualizovat?

- Každý program je buď triviální, nebo obsahuje alespoň jednu chybu.
- Oprava bezpečnostních chyb.
- Oprava chyb, které mohou způsobit ztátu dat.
- Oprava chyb ovlivňující stabilitu či chování.
- Nové funkce, databáze definic (antiviry).

http://cve.mitre.org/
http://www.update-scout.com/
http://www.secunia.com/
http://www.filehippo.com/updatechecker/

Secunia PSI

Personal Software Inspector (PSI) 2.0

Detects and installs missing security patches for your PC

79% Secunia System Score

Secunia Stay Secure

Patch Your PC

- Dashboard
- Scan Results (18)
- Scan

Configuration

Learn More

Scan Results

This view shows an aggregated list of programs detected on your PC with the latest Secunia PSI scan. Click any program for additional information and details.

Scan Results

Search for programs and paths | Search | Are you missing a program?

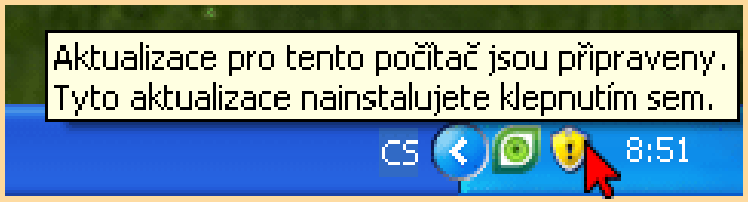
Program	#	Program State	Threat Rating	Detected Version	Install Solution
Adobe Photoshop CS3 10.x	1	End-of-Life		10.0.0.0	-
Apple Bonjour for Windows 1.x	1	End-of-Life		1.0.3.1	Install Solution
TeamSpeak Server 2.x	1	End-of-Life		2.0.21.3	Install Solution
Adobe Flash Player 10.x (ActiveX)	1	Insecure		10.1.53.64 (Activ...	Install Solution
Adobe Flash Player 10.x (NPAPI)	1	Insecure		10.2.152.32 (NP...	Install Solution
Adobe Reader 9.x	1	Insecure		9.3.0.148	Install Solution
Apache 2.2.x	1	Insecure		2.2.15	Install Solution
Apple Safari 5.x	1	Insecure		5.33.19.4	Install Solution
Microsoft Visual C++ 2005 Redistributable Packa...	1	Insecure		8.0.50727.762	Microsoft Update
Mozilla Thunderbird 3.1.x	1	Insecure		3.1.6	Install Solution
OpenOffice.org 3.x	1	Insecure		3.2.9483.500	Install Solution
Opera 11.x	1	Insecure		11.0.1156.0	Install Solution
PHP 5.2.x	1	Insecure		5.2.13	Install Solution
Sun Java JRE 1.6.x / 6.x	1	Insecure		6.0.170.4	Install Solution
TeamSpeak Client 2.x	1	Insecure		2.0.32.60	Install Solution
uTorrent 2.x	1	Insecure		2.0.0.18488	Install Solution
VLC media player 1.x	1	Insecure		1.0.5.0	Install Solution
7-zip 9.x	1	Patched	-	9.10.0.0	Up-to-date

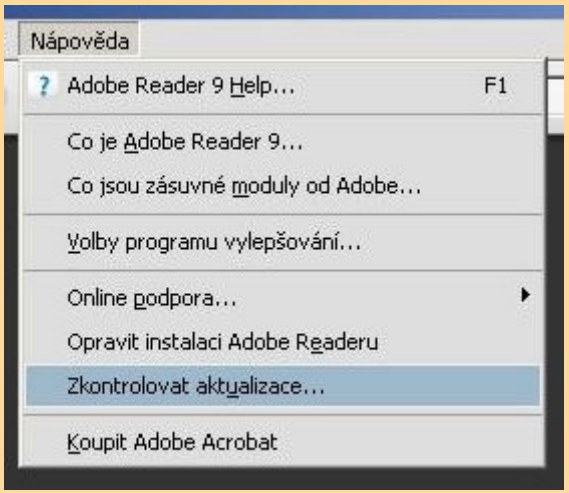
”Zadny z tech programu nepredstavuje jakoukoli hrozbu a nebudu je upgradovat na novejsi verzi.”

Aktualizace softwaru

Jak a kdy software aktualizovat

- služba Windows Update, služba automatické aktualizace (min. každé druhé úterý v měsíci)
- Firefox, Thunderbird, Adobe Reader
  - Nápověda -> Zkontrolovat aktualizace
- Adobe flash player, Adobe shockwave
  http://www.adobe.com/software/flash/about/
  http://www.adobe.com/shockwave/welcome/





Anti* nástroje

Antimalware nástroje založené na signaturách (definice škodlivého kódu) nenajdou 58% malware (zdroj ScanSafe: Global Threat Report).

32% počítačů, které jsou chráněny antivirem, jsou napadeny (zdroj: net-security.org).

Antiviry:

- Avast, AVG, NOD32, Microsoft Security Essentials

Nástroje pro odstranění spyware:

- Ad-Aware, Spybot Search & Destroy, Spyware Terminator, Hijackthis, Combofix

Nástroje pro odstranění rootkitů:

- Microsoft Rootkit Revealer

Antiviry online

Kompletní kontrola:

- http://www.eset.cz/online-skener
- http://www.kaspersky.com/kos/eng/partner/default/kavwebscan.html

Kontrola souboru:

- http://www.virustotal.com/
- http://onlinescan.avast.com/

Pozor na falešné antiviry!

- ukázka

Výsledky testů

File **Setup_71.exe** received on **2010.02.18 09:03:06 (UTC)**
Current status: **finished**
Result: **2/41 (4.88%)**

Compact | Print results

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.02.18	-
AhnLab-V3	5.0.0.2	2010.02.17	-
AntiVir	8.2.1.170	2010.02.17	-
Antiy-AVL	2.0.3.7	2010.02.18	-
Authentium	5.2.0.5	2010.02.18	-
Avast	4.8.1351.0	2010.02.17	-
AVG	9.0.0.730	2010.02.18	-
BitDefender	7.2	2010.02.18	-
CAT-QuickHeal	10.00	2010.02.18	-
ClamAV	0.96.0.0-git	2010.02.18	-
Comodo	3978	2010.02.18	-
DrWeb	5.0.1.12222	2010.02.18	-
eSafe	7.0.17.0	2010.02.17	-
eTrust-Vet	35.2.7310	2010.02.18	-
F-Prot	4.5.1.85	2010.02.17	-
F-Secure	9.0.15370.0	2010.02.18	Suspicious:W32/Malware!Gemini
Fortinet	4.0.14.0	2010.02.15	-
GData	19	2010.02.18	-
Ikarus	T3.1.1.80.0	2010.02.18	-
Jiangmin	13.0.900	2010.02.18	-
K7AntiVirus	7.10.976	2010.02.17	-
Kaspersky	7.0.0.125	2010.02.17	-
McAfee	5895	2010.02.17	-
McAfee+Artemis	5895	2010.02.17	-
McAfee-GW-Edition	6.8.5	2010.02.17	-
Microsoft	1.5406	2010.02.18	-
NOD32	4875	2010.02.17	-

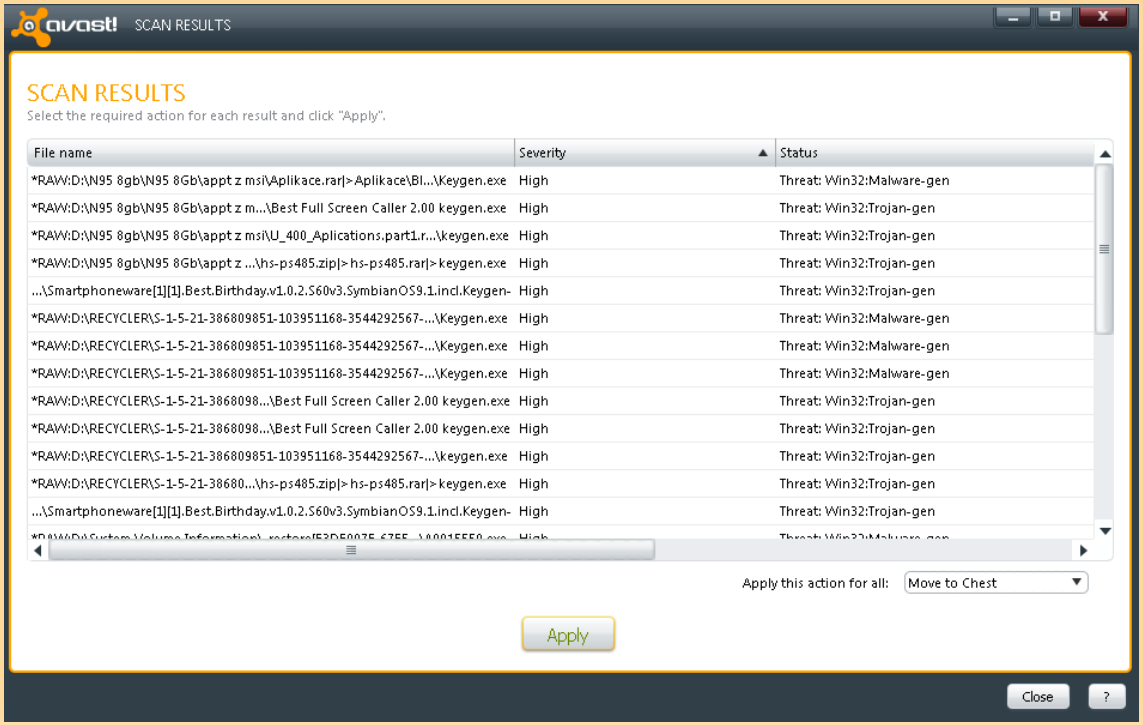
Nalezeny infiltrace!

Počet zkontrolovaných souborů:	9004
Nalezené infiltrace:	**388**
Odstraněné infiltrace:	**377**
Celkový čas kontroly:	00:17:01
Stav kontroly:	Ukončeno uživatelem

Seznam nalezených infiltrací
Spravovat karanténu

Zvolte Odinstalovat pokud chcete odstranit ESET Online Scanner z vašeho počítače. Při dalším spuštění aplikace ESET Online Scanner bude potřeba stáhnout všechny soubory znovu.

☐ Odinstalovat po skončení
☐ Smazat soubory z karantény



Hesla

Dobrý den,
Váš mail ohledně změnění hesla mně pěkně naštval....
a to hned ze 3 důvodů:
za 1) **Proč proboha měnit heslo,když jsme na něj zvyklí?**
-z vlastní zkušenosti vím,že mnoho lidí má takové heslo,které se dobře pamatuje a zároveň není příliš jeednoduché
za 2) **tak proč měnít hesla (navíc jak píšete,několikrát během šk. roku) ?!?!**
- **vždyť jsme na Vysoké škole,takže si myslím,že kdo z elity národa by chtěl školní poštu nějak zneužívat,hackovat či spamovat?!? - nikdo!!**
za 3) **když si budem furt měnit hesla,zatížíme systém, bude docházet ke ztrátám hesel u hodně lidí** a vám i nám to přidá hafo práce a starostí navíc...
- Vám snad připadá 10-ti místné heslo málo nebo lehko uhodnutelné????? (většina z nás to 10ti místné má...)
s pozdravem nespokojený student

Hesla

Nevhodná volba

- jména, rodná čísla, adresa, názvy, běžné znaky
- slovníková hesla

Mnemotechnické pomůcky

- Dvakrát do stejné řeky nevstoupíš! 2XdsrN!

Prolomitelnost (při rychlosti 100 hesel za sek.)

- znaky 0..9; délka 4→2min; délka 8→11dní
- znaky a..Z,0..9; délka 4→2dní; délka 8→70 000 let

Sociální inženýrství

Metoda využívána k získávání důležitých informací od uživatelů „bez jejich vědomí”

Médium

- telefon a Internet (e-mail, IM)

Zneužívání vlastností lidí

- důvěřivost, neznalost, ochota pomoci druhým, obava, nepodezíravost, naivita, hloupost

Obrana

- vzdělávání, jasně stanovená pravidla a postupy, (zpětné) ověřování totožnosti, zdravý rozum

Sociální inženýrství

Příklady zneužití

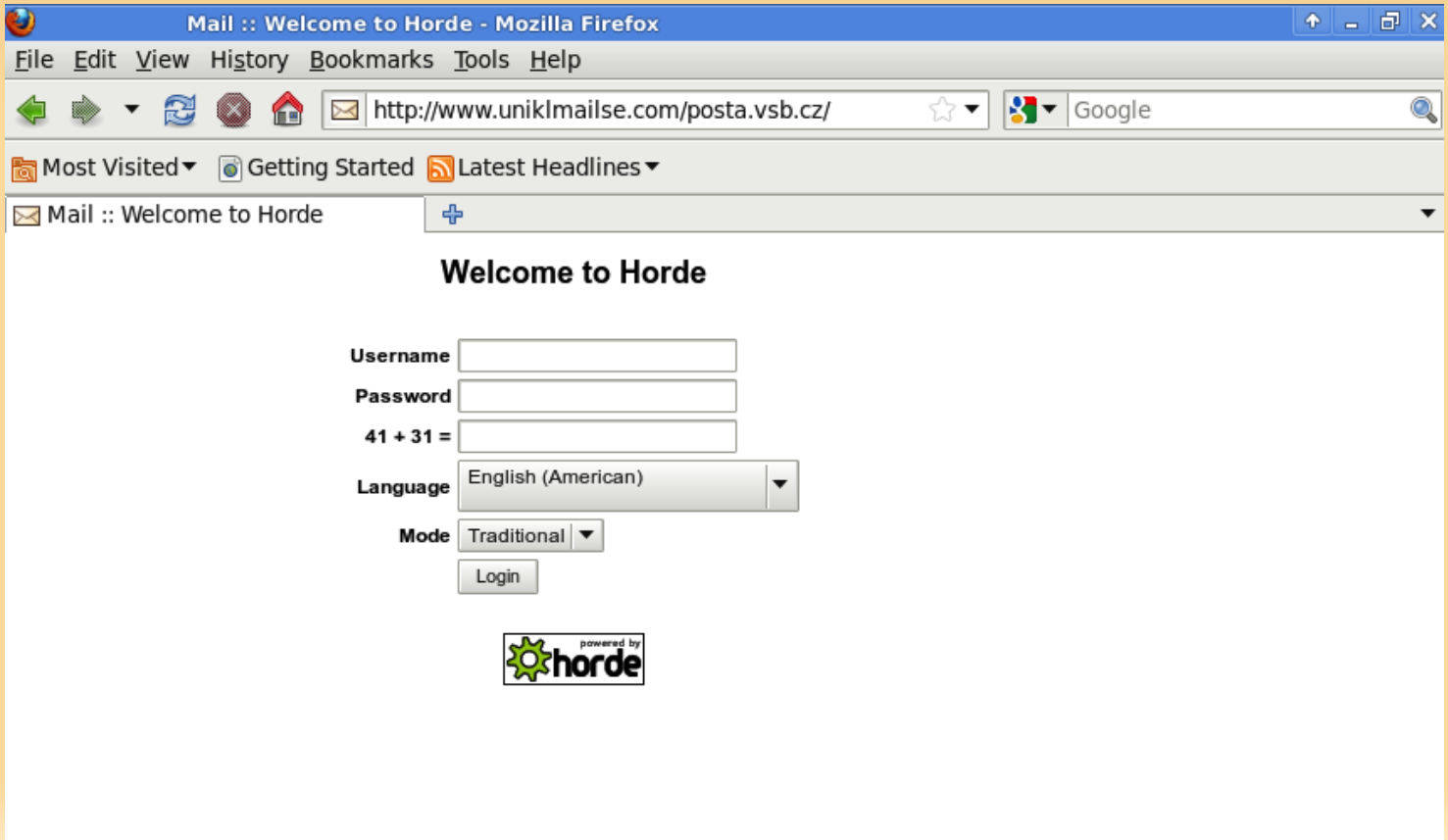
- Mám nový bankovní účet, pošlu Vám mail...
- Máte napadený počítač, navštivte tyto stránky a zjistěte mi prosím ...
- Potřebujeme ověřit Váš účet, zašlete nám heslo...

Phishing

Překročili jste limit úložiště na poštovní schránce.Nebudete moci odesílat nebo přijímat novou poštu dokud upgradevaší e-mailové kvóty. Zkopírujte níže odkaz a vyplňte formulář pro upgrade svého účtu.

http://www.uniklmailse.com/posta.vsb.cz

System Administrator 192.168.0.1



Několik doporučení

- Používejte osobní **firewall a antivir**.
- Pravidelně veškerý software **aktualizujte**.
- Nepoužívejte všude stejná **hesla** a hesla si měňte.
- Buďte obezřetní a používejte **zdravý rozum**.
- Neinstalujte neznámé aplikace a doplňky.
- Neklikejte na neznámé odkazy a ”neodhlašujte” spam.
- Kontrolujte URL adresu.
- Nepoužívejte warez (gamez, appz, crackz, moviez).
- Vždy se odhlašujte.

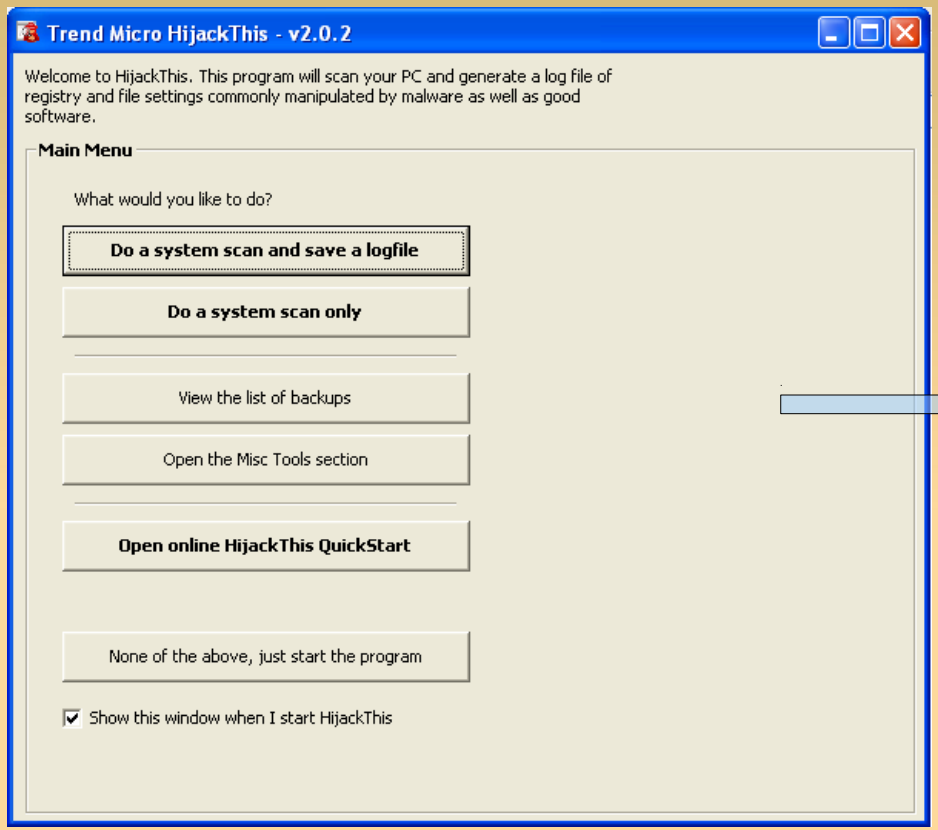
Dotazy?

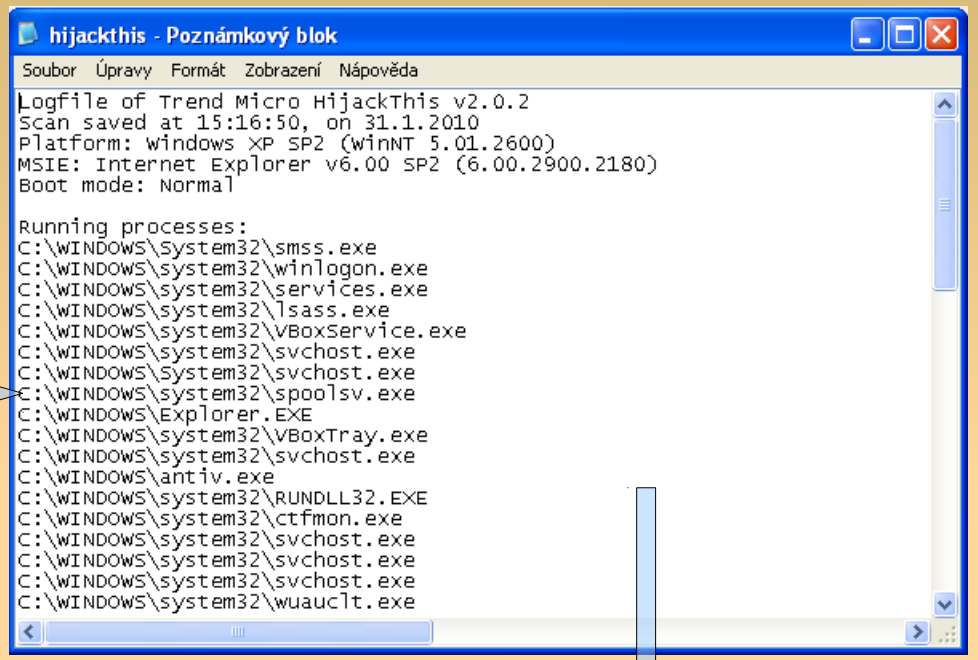
Děkuji za pozornost.

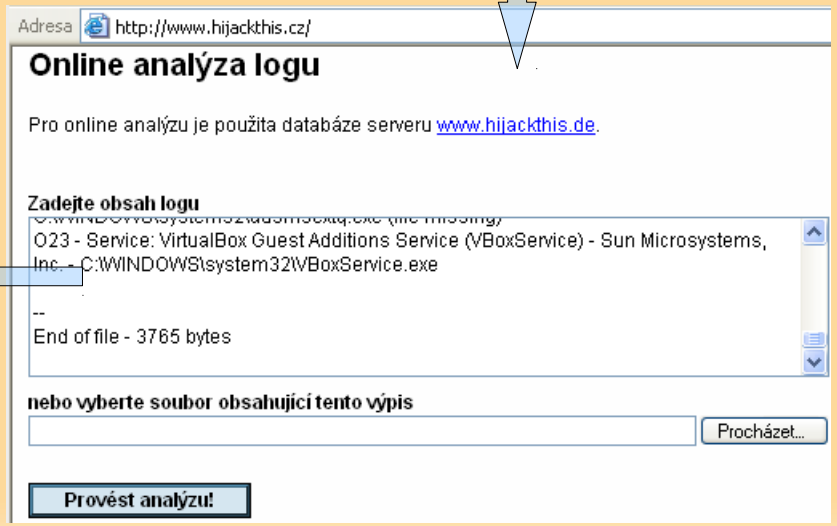
Autorská práva

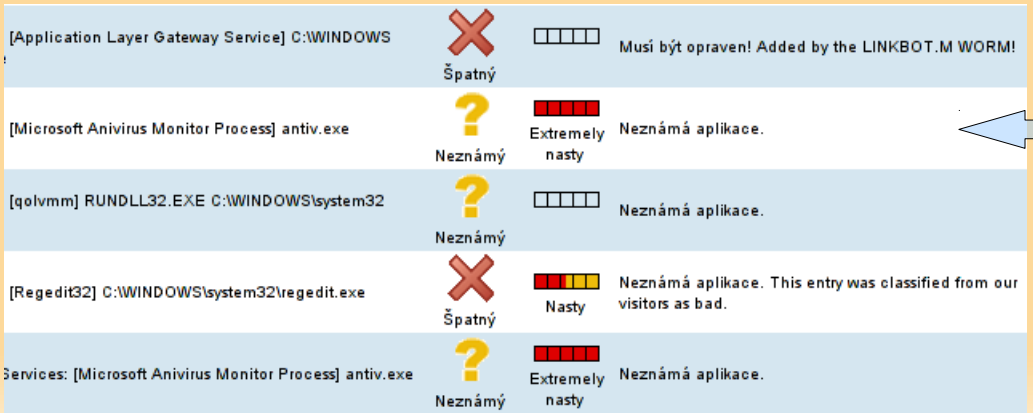
- © Radomír Orkáč, Pavel Kácha

Hijackthis


Trend Micro HijackThis - v2.0.2
Welcome to HijackThis. This program will scan your PC and generate a log file of registry and file settings commonly manipulated by malware as well as good software.
Main Menu
What would you like to do?
Do a system scan and save a logfile
Do a system scan only
View the list of backups
Open the Misc Tools section
Open online HijackThis QuickStart
None of the above, just start the program
Show this window when I start HijackThis


hijackthis - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
Logfile of Trend Micro HijackThis v2.0.2
Scan saved at 15:16:50, on 31.1.2010
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)
Boot mode: Normal
Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\VBoxService.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\VBoxTray.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\antiv.exe
C:\WINDOWS\system32\RUNDLL32.EXE
C:\WINDOWS\system32\ctfmon.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\wuauclt.exe


Adresa http://www.hijackthis.cz/
Online analýza logu
Pro online analýzu je použita databáze serveru www.hijackthis.de.
Zadejte obsah logu
O23 - Service: VirtualBox Guest Additions Service (VBoxService) - Sun Microsystems, Inc. - C:\WINDOWS\system32\VBoxService.exe
--
End of file - 3765 bytes
nebo vyberte soubor obsahující tento výpis
Procházet...
Provést analýzu!


[Application Layer Gateway Service] C:\WINDOWS
Špatný
Musí být opraven! Added by the LINKBOT.M WORM!
[Microsoft Anivirus Monitor Process] antiv.exe
Neznámý
Extremely nasty
Neznámá aplikace.
[qolvmm] RUNDLL32.EXE C:\WINDOWS\system32
Neznámý
Neznámá aplikace.
[Regedit32] C:\WINDOWS\system32\regedit.exe
Špatný
Nasty
Neznámá aplikace. This entry was classified from our visitors as bad.
Services: [Microsoft Anivirus Monitor Process] antiv.exe
Neznámý
Extremely nasty
Neznámá aplikace.