Havěť v praxi

Bc. Igor Hák, Eset software spol. s r. o.

Copyright © 2006 Eset software spol. s r. o.

Kam to všechno spěje...

- stále méně „klasické“ havěti
  - viry před vymřením
  - mediálně známí „pisálci“ před vymřením

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Kam to všechno spěje...

- hlavním problémem
  - je havět typu: spyware, adware, riskware, trojské koně...
  - **ale především zcela naivní uživatelé**

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Kam to všechno spěje...

- stále užší vazby mezi spamem, spyware, adware a trojany (popř. viry, červy), významným článkem je uživatel:
  - uživatel spustí trojan v poště (dropper, downloader)
  - nasazení backdoora (SMTP „zombie“)
  - vypuštění, stažení dalšího škodlivého softwaru
  - sběr a odesílání informací (např. dalších e-mailů)
  - útočník odesílá další spam či havěť na získané adresy

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

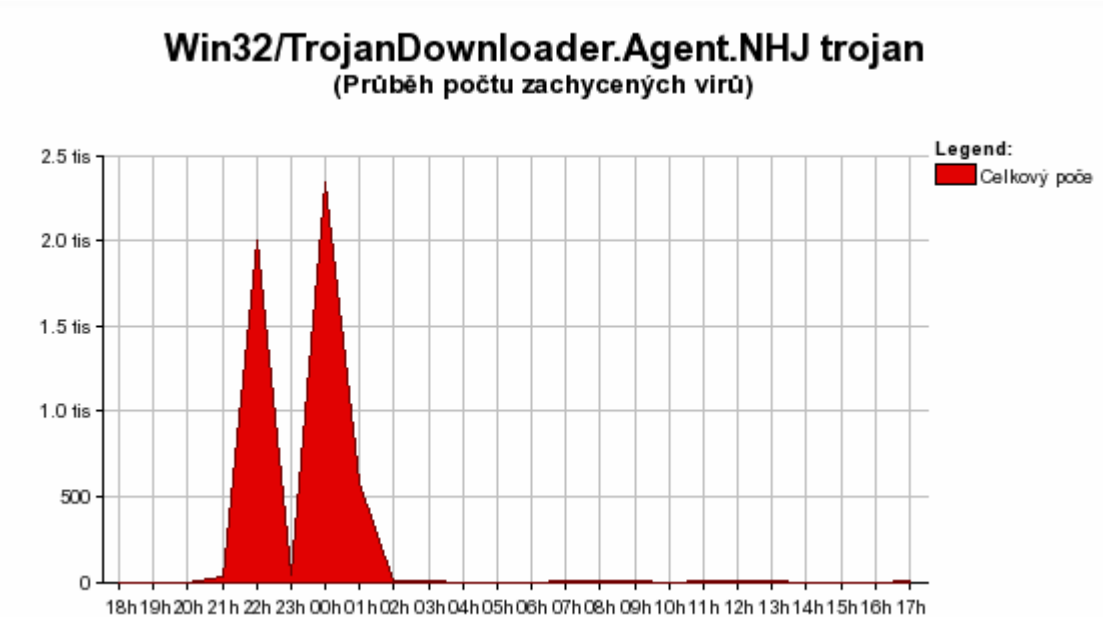
Kam to všechno spěje...

- „spamování“ havěti ve vlnách na povel útočníka
  - zneužití dříve infikovaných PC (backdoor) na Internetu („zombies“)
    - stěží lze vypátrat skutečného pachatele (SMTP oběti)
  - často bez funkce pro další automatické šíření (s přispěním uživatele)

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

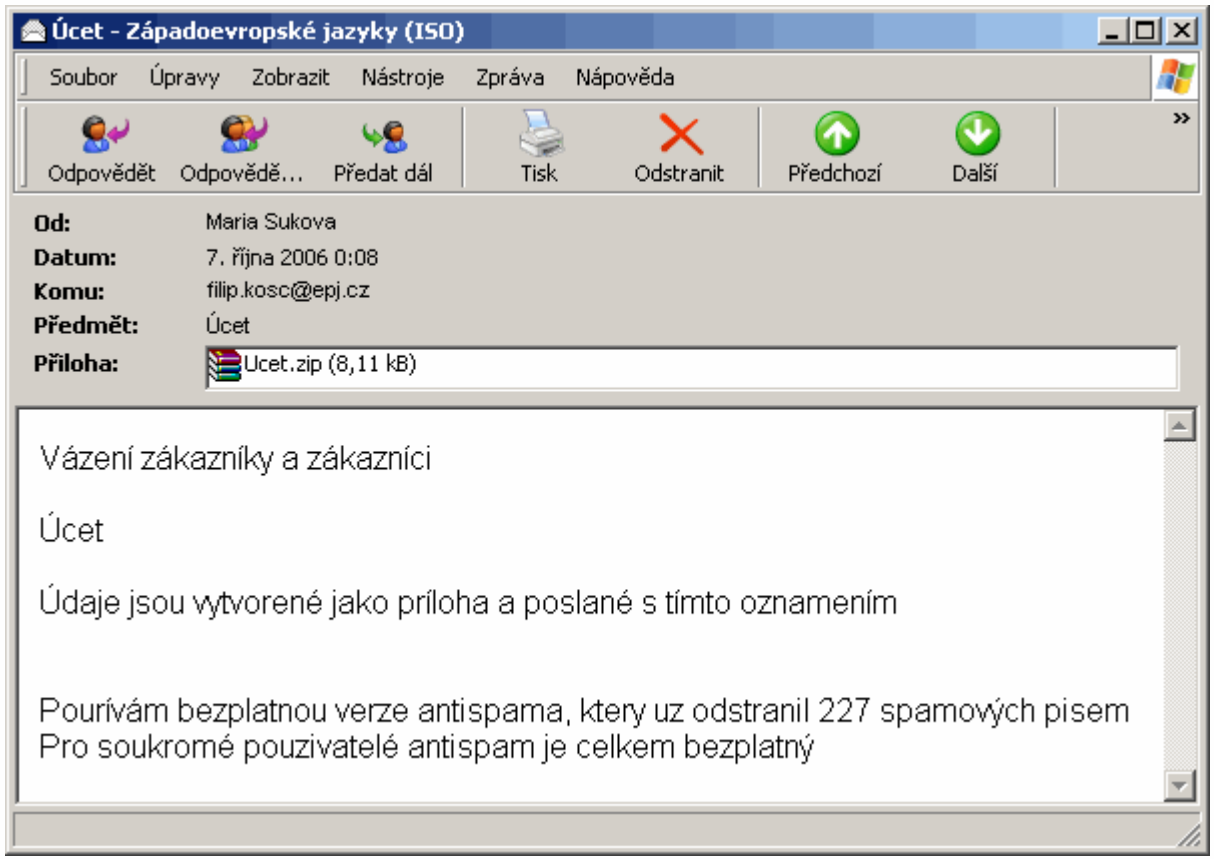
Kam to všechno spěje...



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Kam to všechno spěje...



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Havěť v praxi

```
Length Of Struc: 0424h
Length Of Value: 0034h
Type Of Struc:   0000h
Info:            VS_VERSION_INFO
Signature:       FEEF04BDh
Struc Version:   1.0
File Version:    5.1.2600.2180
Product Version: 5.1.2600.2180
File Flags Mask: 0.63
File Flags:      SPECIAL BUILD;
File OS:         WINDOWS32
File Type:       APP
File SubType:    UNKNOWN
File Date:       00:00:00  00/00/0000

     Struc has Child(ren). Size: 968 bytes.

Child Type:         StringFileInfo
Language/Code Page: 1033/1200
Comments:
CompanyName:        Microcoft Corporation
FileDescription:    upnp manager
FileVersion:        5.1.2600.2180
InternalName:       unker
LegalCopyright:     © Microcoft Corporation. All rights reserved
LegalTrademarks:    Microsoft (R)
OriginalFilename:   unker.EXE
PrivateBuild:
ProductName:        upnp  manager Microcoft® Windows®
ProductVersion:     5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
SpecialBuild:       5.1.2600.2180

Child Type:         VarFileInfo
Translation:        1033/1200
```

Bc. Igor Hák

hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

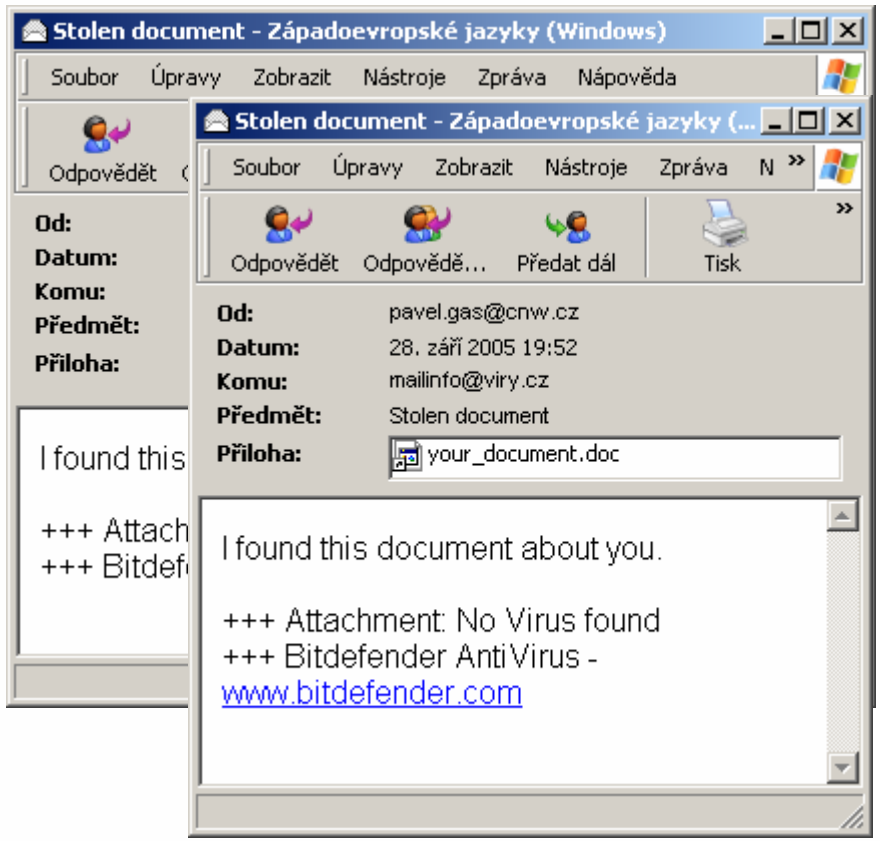
Havěť šířící se elektronickou poštou

- nejčastěji ve formě přílohy mailu

„Fígle“:

- falšování adresy odesílatele
- sociální inženýrství

  (nabádající texty, ujištění...)
- dvojité přípony, bílé mezery...



Bc. Igor Hák
hak@eset.cz

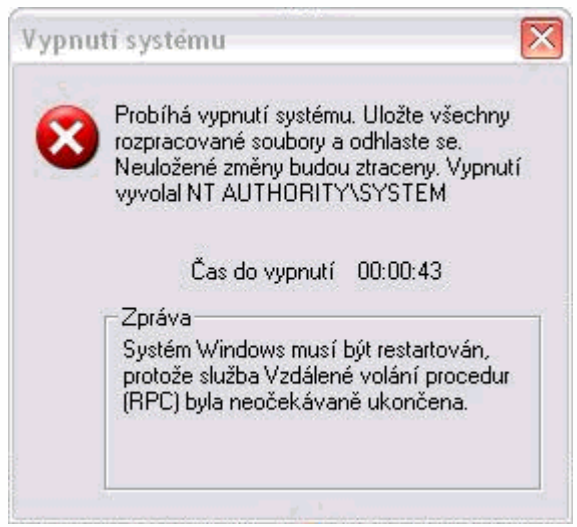
Copyright © 2006 Eset software spol. s r. o.

Internetové červi

- šíří se na úrovni síťových paketů
- **uživatel s nimi nepřijde přímo do styku (v souborech apod.)**
- obvykle zneužívají chyby v software (nejčastěji MS Windows)

- **„vadí“ především vedlejší účinky:**

⇒ „nejpopulárnější“ červ Blaster (2003):



⇒ **<u>OBRANOU NENÍ ANTIVIRUS, ALE FIREWALL</u>**

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Software typu: spyware, adware...

- „otravný“ software
- prohlížeč odkazuje na jiné stránky, než uživatel požaduje
- „vyskakující“ reklamní okna

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Žluté linky a dialers

- týká se „modemistů“
- vytáčení draze účtovaných tel. čísel

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Phishing, hoax, spam

- **phishing:**
- zpráva, vydávající se za prohlášení bank. instituce (nejčastěji)
- obvykle požaduje zadání čísla kreditní karty a PIN pro „ověření“

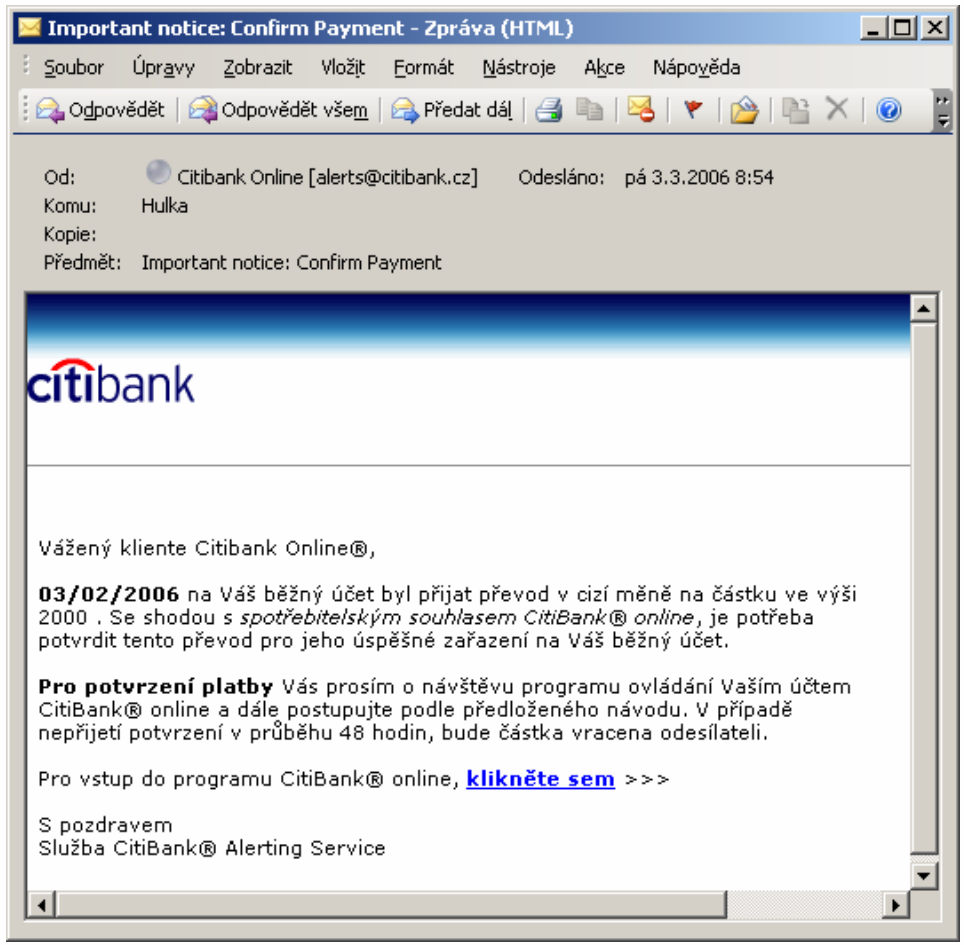
- **hoax:**
- falešné zprávy, typicky o ve skutečnosti neexistujícím viru, o nutnosti finanční podpory umírajících ..., www.hoax.cz

- **spam:**
- nevyžádaná pošta

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

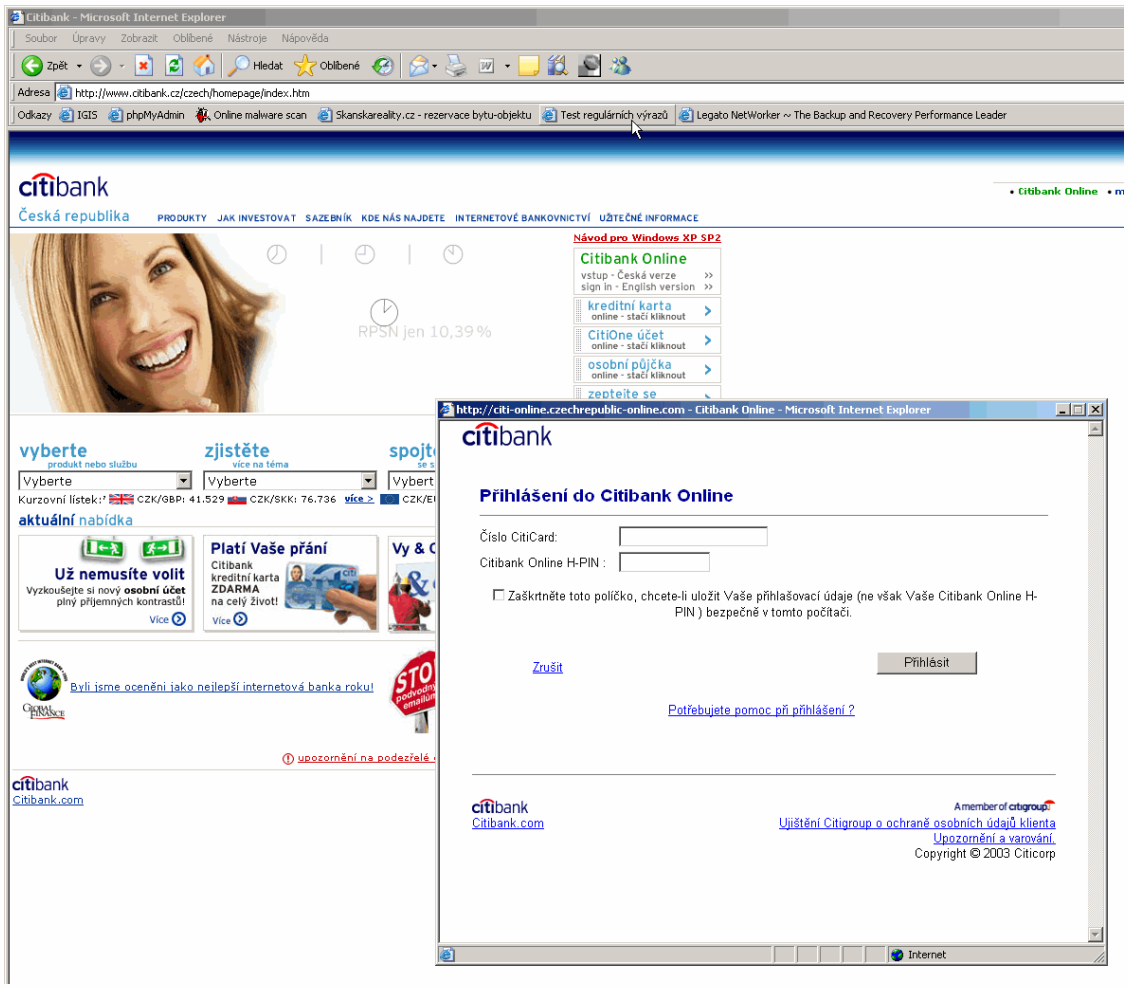
1. český phishing



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

1. český phishing



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Keyloggers, backdoors...

- **Keyloggers:**
- aplikace sledující stisky kláves (sledování zápisu hesel...)
- pro efekt je nutná přítomnost SW, který tyto informace odešle

- **Backdoors:**
- „zadní vrátka“. Útočník může převzít kontrolu nad PC připojeným do Internetu.

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Rootkity

- pojem z „UNIXového“ světa
  - programy pro zakrytí nekalé činnosti hackerů (nahrazení systémových souborů – login, ls...)
- pod Windows „novinka“ (pozor na stealth viry)

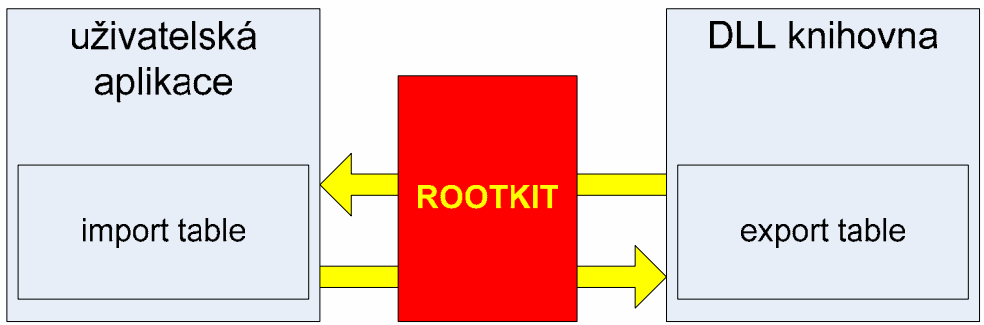
Rootkit je program, který se snaží zamaskovat vlastní přítomnost v PC (přítomnost souborů, změn v registru Windows...), popř. přítomnost jiných aplikací v PC.

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Rootkity

- obecný princip fungování:
  - „zavěšení“ na OS na co možná nejnižší vrstvě (kernelové / aplikační)
  - obr. přesměrování funkce (např. *FindFirstFile / FindNextFile*)



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Rootkity

- perle z praxe:
  - **„Sony BGM rootkit“**
    - některé hudební CD vybaveny „přehrávačem“ pro PC
    - v systému se po něm „zaprášilo“
    - => zneužito dalším škodlivým kódem (zakrývání adresářů *sys*)
  - **„rootkity“ v antivirech**
    - zásadní rozdíl: uživatel může instalaci odmítnout + ví, co instaluje

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Rootkity vs antiviry

- **Antiviry rootkity detekují a nedetekují**
  - spolehlivě je mohou detekovat na vstupu (podobně jako jinou havěť)
    - exaktní detekce (signatury)
    - generická detekce (heuristická analýza, obecný kód...)
    - otázka: aplikuje můj výrobce AV uvedené metody na rootkity?
  - často je nebudou detekovat aktivní v systému
    - existence speciálních utilit (vlastní ovladače pro čtení z disku...)
    - ideální: nastartovat OS z jiného zdroje (boot CD...)

Bc. Igor Hák
hak@eset.cz

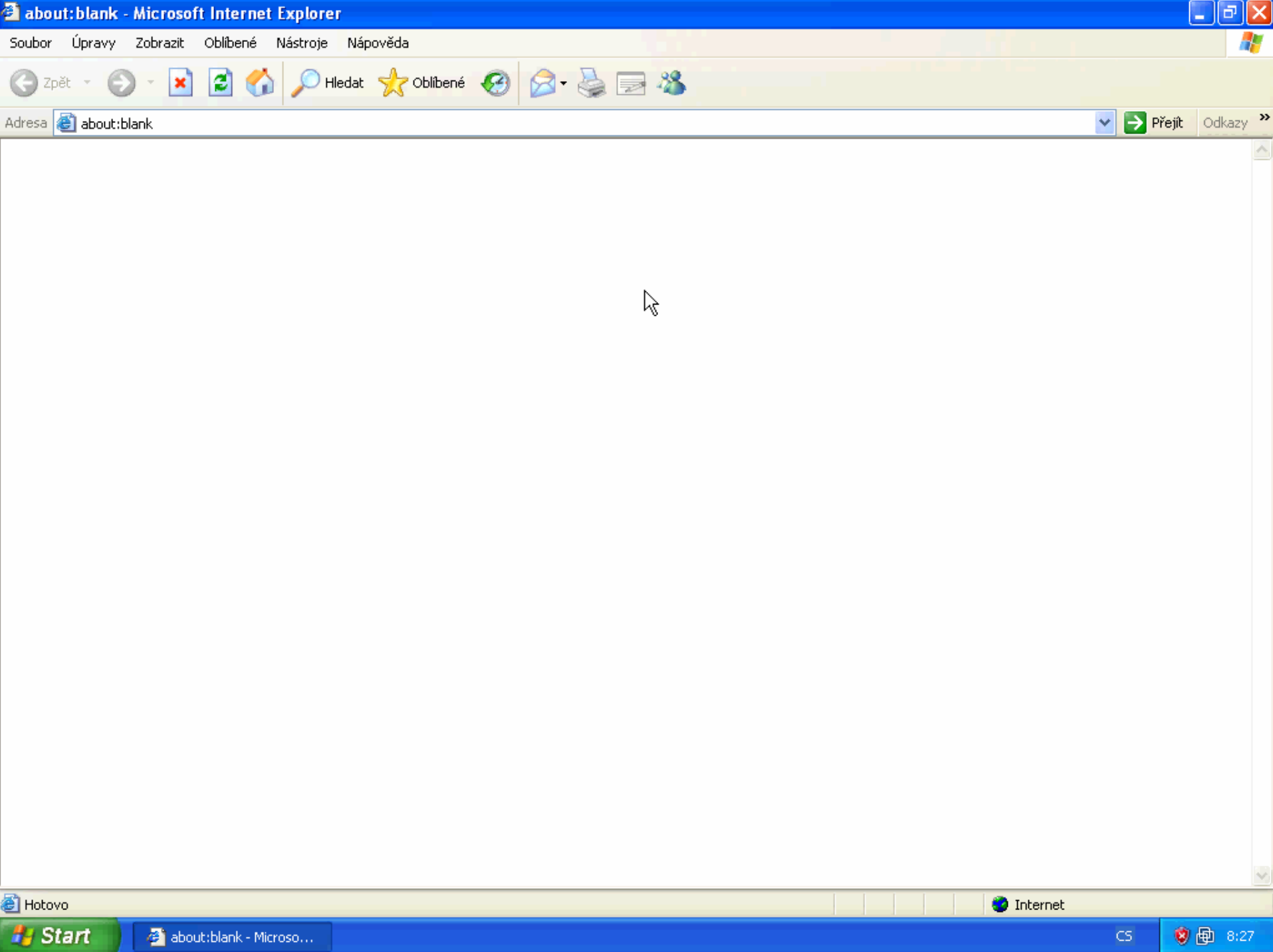
Copyright © 2006 Eset software spol. s r. o.

Rogue Antispyware

- http://www.spywarewarrior.com/rogue_anti-spyware.htm
  - seznam „nečistých“ antispyware aplikací

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.


about:blank - Microsoft Internet Explorer
Soubor
Úpravy
Zobrazit
Oblíbené
Nástroje
Nápověda
Zpět
Hledat
Oblíbené
Adresa
about:blank
Přejít
Odkazy
Hotovo
Internet
Start
about:blank - Microso...
CS
8:27

Globální problém

- dnes nevytváří jen několik „kousků“ havěti (Netsky, Bagle...tj. viry způsobující „out-breaky”)

- **vytváří tisíce různých programů typu adware, spyware...**
  - sami se dále nešíří (e-mailem, síť. pakety...)
  - „čekají“ na pochybných webech (zanedbatelné množství)
  - může trvat měsíce, než obdrží vzorek AV společnost

  => **jen stěží lze zaručit spolehlivou detekci na úrovni vzorků ve virové databázi**

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Globální problém

- denní zkušenosti:
  - ani kombinaci AV a AS řešení nemusí stačit (resp. nestačí)
  - **záleží především na chování uživatele**

- “dokonalá “ detekce: **HIJACKTHIS** aplikace – www.spyware.cz
  - vytváří protokol o PC a „místech“, které havěť zneužívá
  - nutné oko znalce pro odchyt známé i neznámé havěti

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Logfile of HijackThis v1.99.1
Scan saved at 19:15:29, on 7.10.2006
Platform: Windows 2000 SP4 (WinNT 5.00.2195)
MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:
C:\WINNT\System32\smss.exe
C:\WINNT\system32\winlogon.exe
C:\WINNT\system32\services.exe
C:\WINNT\system32\lsass.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\system32\spoolsv.exe
C:\WINNT\System32\svchost.exe
C:\WINNT\system32\regsvc.exe
C:\WINNT\system32\MSTask.exe
C:\Program Files\VMware\VMwareService.exe
C:\WINNT\System32\WBEM\WinMgmt.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\Explorer.EXE
C:\Program Files\VMware\VMwareTray.exe
C:\Program Files\VMware\VMwareUser.exe
C:\Program Files\Eset\nod32kui.exe
C:\WINNT\system32\internat.exe
C:\Program Files\PSPad\PSPad.exe
C:\totalcmd\TOTALCMD.EXE
C:\WINNT\regedit.exe
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\WINNT\System32\sysshtic.exe
C:\Documents and Settings\igi\Local Settings\Temporary Internet Files\Content.IE5\TXYTOSZ0\hijackthis[1].exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Odkazy
O3 - Toolbar: &Rdio - {8E718888-423F-11D2-876E-00A0C9082467} - C:\WINNT\system32\msdxm.ocx
O4 - HKLM\..\Run: [Synchronization Manager] mobsync.exe /logon
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMwareUser.exe
O4 - HKLM\..\Run: [nod32kui] "C:\Program Files\Eset\nod32kui.exe" /WAITSERVICE
O4 - HKCU\..\Run: [internat.exe] internat.exe
O9 - Extra button: Related - {c95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\WINNT\web\related.htm
O9 - Extra 'Tools' menuitem: Show &Related Links - {c95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\WINNT\web\related.htm
O16 - DPF: {6414512B-B978-451D-A0D8-FCFDF33E833C} (WUWebControl Class) -
http://update.microsoft.com/windowsupdate/v6/V5Controls/en/x86/client/wuweb_site.cab?1146143139953
O20 - AppInit_DLLs: evenncob.dll e1.dll
O20 - Winlogon Notify: sysshtic - C:\WINNT\system32\sysshtic.dll
O23 - Service: Logical Disk Manager Administrative Service (dmadmin) - VERITAS Software Corp. - C:\WINNT\System32\dmadmin.exe
O23 - Service: VMware Tools Service - VMware, Inc. - C:\Program Files\VMware\VMwareService.exe

Častý problém

- **O20 - AppInit_DLLs: evenncob.dll e1.dll**
- **O20 - Winlogon Notify: sysshtic - C:\WINNT\system32\sysshtic.dll**

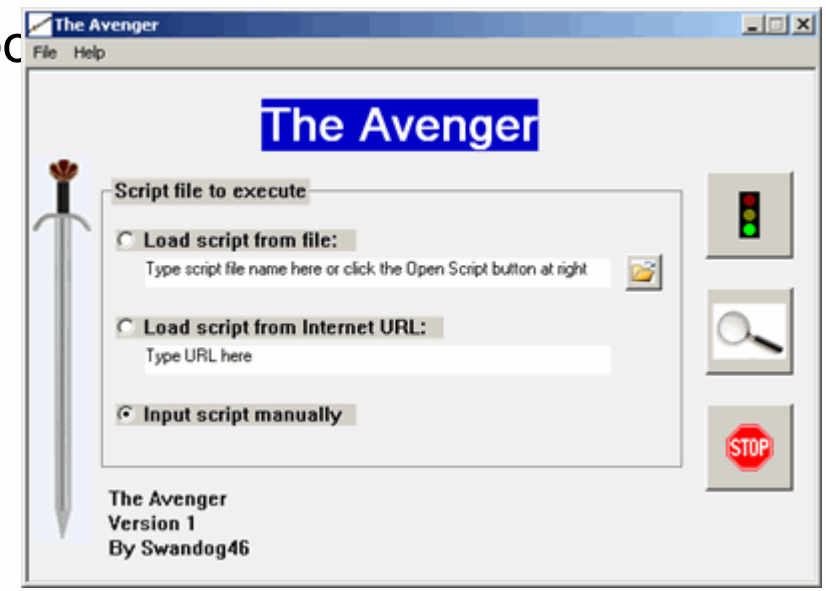
- brzké převzetí kontroly nad systémem (vazba na proces winlogon.exe a user32.dll)
- nemusí pomáhat ani nouzový režim Windows
- **řešením např. The Avenger**

Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Častý problém

- **řešení: The Avenger**
- na základě „rozkazů“ ve skriptovém souboru
  - odmaže infikované soubo
  - opraví registry...
- ihned při startu Windows



Bc. Igor Hák
hak@eset.cz

Copyright © 2006 Eset software spol. s r. o.

Files to delete:
%windir%\system32\dmimmdt2.exe
%windir%\system32\e1.dll
%windir%\system32\evenncob.dll
%windir%\system32\snmpmmcn.dll
%windir%\system32\sysshtic.dll
%windir%\system32\sysshtic.exe
%windir%\system32\winbpowr.exe
Registry values to delete:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows | AppInit_DLLs
Registry keys to delete:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\sysshtic



Děkuji za pozornost

Bc. Igor Hák, Eset software spol. s r. o.

Copyright © 2006 Eset software spol. s r. o.