

# Botnet eksperiment

**Kovačič Matej**

**Gašper Koren**

**(CC) 2005-2008**

*Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Streliška 1, 1000 Ljubljana.*

# **Primer napada v decembru 2004**

# Računalnik je povezan v prikrito omrežje preko vrat 443 (da zaobide požarni zid)

ettercap 0.6.4

SOURCE: ANY Filter: OFF  
DEST : illithid (IP based) - ettercap  
Active Dissector: OFF

hosts in this LAN (

1)	193.2	138	<-->	193.2.	:138	UDP	netbios-dgm
2)	193.2	137	<-->	193.2.	:137	UDP	netbios-ns
3)	193.	1588	<-->	193.2	:135	OPENING	
4)	193.2	1025	<-->	192.102.23.	4:443	silent	https
5)	192.102	2797	<-->	193.2.	:113	OPENING	auth
6)	192.102	2798	<-->	193.2.	:1080	OPENING	socks
7)	193.2	1030	<-->	193.2.	:53	UDP	domain
8)	193.2	1032	<-->	193.2.	:53	UDP	domain
9)	193.2	1031	<-->	193.2.	:53	UDP	domain
10)	193.2	1033	<-->	193.2.	:53	UDP	domain
11)	193.2	1034	<-->	63.111.	:80	KILLED	www
12)	193.2	1036	<-->	63.111.	:80	KILLED	www
13)	193.2	1037	<-->	63.111.	:80	KILLED	www
14)	193.2	1035	<-->	63.111.	:80	KILLED	www
15)	193.2	1038	<-->	193.2.	:161	UDP	snmp
16)	193.2	1040	<-->	193.2.14	:445	OPENING	
17)	193.2	1039	<-->	193.2.	:445	OPENING	
18)	193.2	1041	<-->	193.2.14	:445	OPENING	
19)	193.2	1042	<-->	193.2.16	:445	OPENING	
20)	193.2	1043	<-->	193.2.	:445	OPENING	
21)	193.2	1044	<-->	193.2.12	:445	OPENING	

Your IP: MAC: Iface: eth0 Link: not tested

# Po vključitvi v prikrito omrežje prične 'skenirati'

ettercap 0.6.4

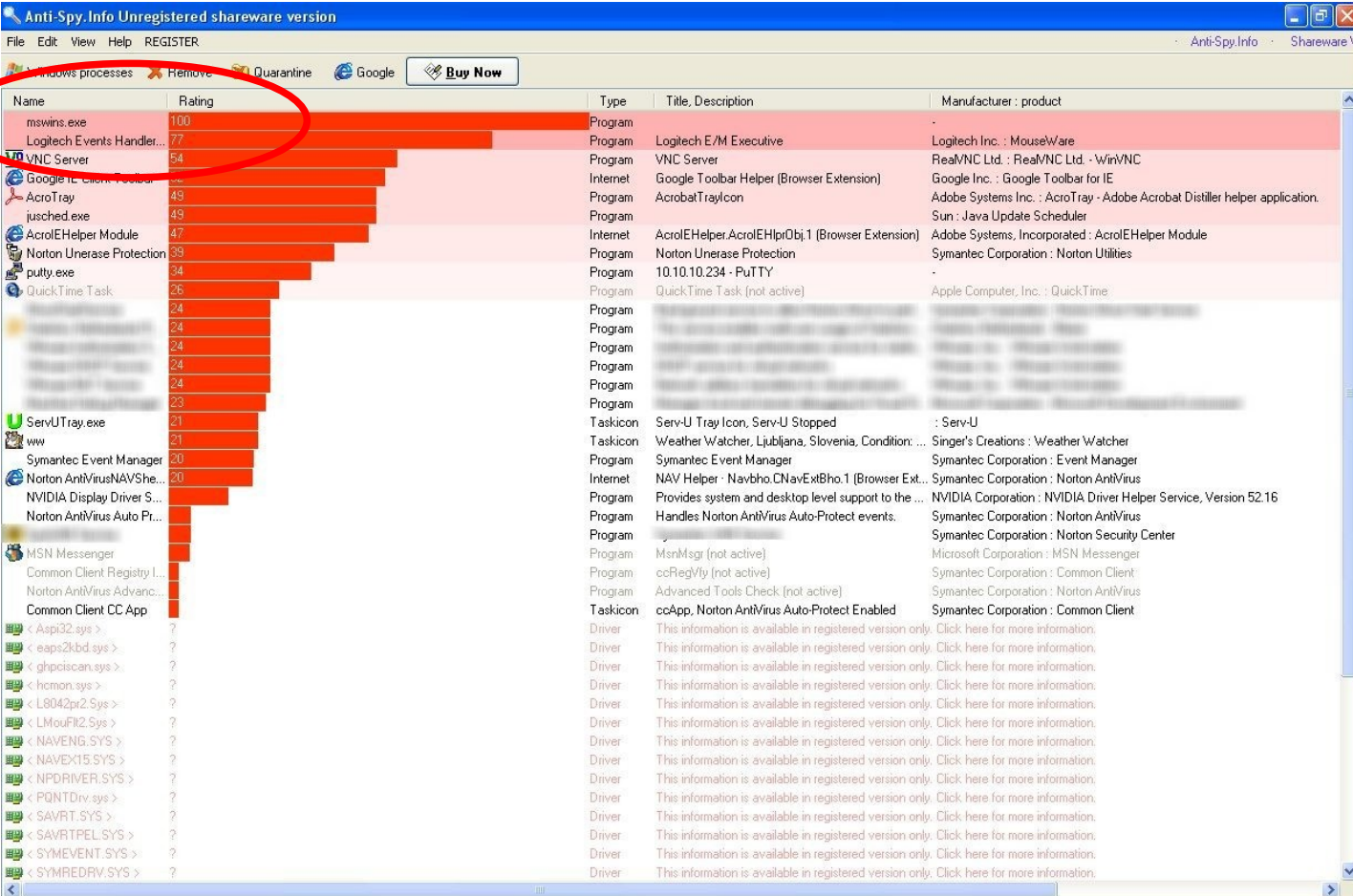
SOURCE: ANY Filter: OFF  
DEST: illithid (IP based) - ettercap  
Active Dissector: OFF

??? hosts in this LAN (

13)	193.2.	:1355	<-->	193.2.252.14:445	OPENING
14)	193.2.	:1357	<-->	193.2.75.114:445	OPENING
15)	193.2.	:1358	<-->	193.2.36.214:445	OPENING
16)	193.2.	:1359	<-->	193.2.169.182:445	OPENING
17)	193.2.	:1360	<-->	193.2.229.218:445	OPENING
18)	193.2.	:1361	<-->	193.2.100.208:445	OPENING
19)	193.2.	:1362	<-->	193.2.238.68:445	OPENING
20)	193.2.	:1363	<-->	193.2.0.133:445	OPENING
21)	193.2.	:1364	<-->	193.2.11.101:445	OPENING
22)	193.2.	:1365	<-->	193.2.206.23:445	OPENING
23)	193.2.	:1366	<-->	193.2.56.125:445	OPENING
24)	193.2.	:1367	<-->	193.2.192.3:445	OPENING
25)	193.2.	:1368	<-->	193.2.17.194:445	OPENING
26)	193.2.	:1369	<-->	193.2.123.83:445	OPENING
27)	193.2.	:1370	<-->	193.2.138.43:445	OPENING
28)	193.2.	:1371	<-->	193.2.174.223:445	OPENING
29)	193.2.	:1372	<-->	193.2.224.84:445	OPENING
30)	193.2.	:1373	<-->	193.2.162.234:445	OPENING
31)	193.77.10	:15848	<-->	193.2.:19950	UDP
32)	193.2.	:1374	<-->	193.2.208.137:445	OPENING
33)	193.2.	:1375	<-->	193.2.19.201:445	OPENING

Your IP: MAC: Iface: eth0 Link: not tested

# Proces smo zaznali le z orodjem Anti-Spy.info



The screenshot shows the Anti-Spy.info application window. The main area is a table of running processes, sorted by rating. A red circle highlights the first row, which is 'mswins.exe' with a rating of 100. The table has columns for Name, Rating, Type, Title, Description, and Manufacturer: product.

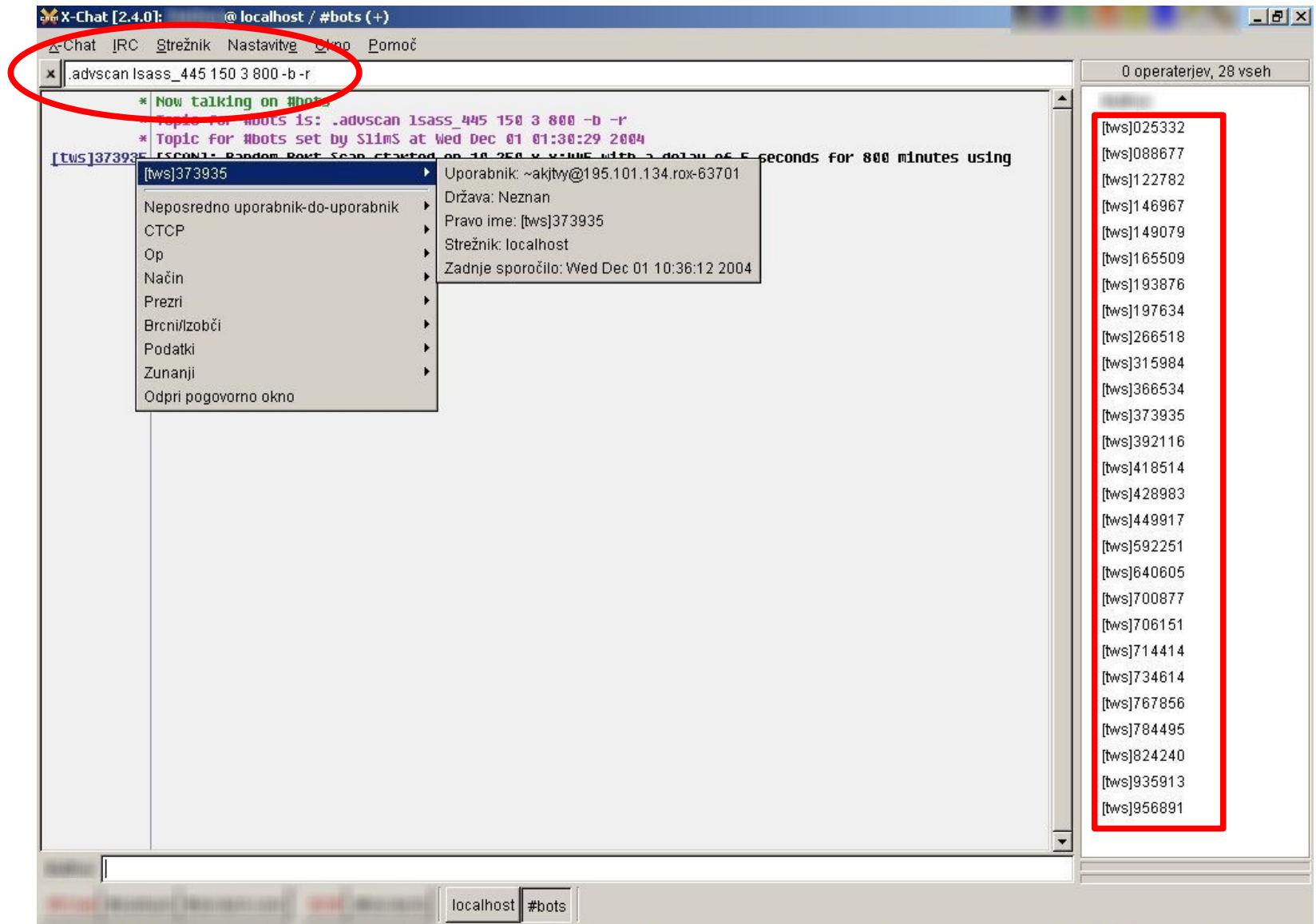
Name	Rating	Type	Title, Description	Manufacturer: product
mswins.exe	100	Program		
Logitech Events Handler...	77	Program	Logitech E/M Executive	Logitech Inc. : MouseWare
VNC Server	64	Program	VNC Server	RealVNC Ltd. : RealVNC Ltd. - WinVNC
Google Toolbar Helper (Browser Extension)	52	Internet	Google Toolbar Helper (Browser Extension)	Google Inc. : Google Toolbar for IE
AcroTray	49	Program	AcrobatTrayIcon	Adobe Systems Inc. : AcroTray - Adobe Acrobat Distiller helper application.
jusched.exe	49	Program		Sun : Java Update Scheduler
AcroEHelper Module	47	Internet	AcroEHelper.AcroEHLPrObj.1 (Browser Extension)	Adobe Systems, Incorporated : AcroEHelper Module
Norton Unerase Protection	39	Program	Norton Unerase Protection	Symantec Corporation : Norton Utilities
putty.exe	34	Program	10.10.10.234 - PuTTY	
QuickTime Task	26	Program	QuickTime Task (not active)	Apple Computer, Inc. : QuickTime
	24	Program		
	24	Program		
	24	Program		
	24	Program		
	24	Program		
	24	Program		
ServUTray.exe	21	Taskicon	Serv-U Tray Icon, Serv-U Stopped	: Serv-U
Weather Watcher	21	Taskicon	Weather Watcher, Ljubljana, Slovenia, Condition: ...	Singer's Creations : Weather Watcher
Symantec Event Manager	20	Program	Symantec Event Manager	Symantec Corporation : Event Manager
Norton AntiVirusNAVShel...	20	Internet	NAV Helper - Navbho.CNavExBho.1 (Browser Ext...	Symantec Corporation : Norton AntiVirus
NVIDIA Display Driver S...		Program	Provides system and desktop level support to the ...	NVIDIA Corporation : NVIDIA Driver Helper Service, Version 52.16
Norton AntiVirus Auto Pr...		Program	Handles Norton AntiVirus Auto-Protect events.	Symantec Corporation : Norton AntiVirus
		Program		Symantec Corporation : Norton Security Center
MSN Messenger		Program	MsnMsr (not active)	Microsoft Corporation : MSN Messenger
Common Client Registry I...		Program	ccRegVly (not active)	Symantec Corporation : Common Client
Norton AntiVirus Advanc...		Program	Advanced Tools Check (not active)	Symantec Corporation : Norton AntiVirus
Common Client CC App		Taskicon	ccApp, Norton AntiVirus Auto-Protect Enabled	Symantec Corporation : Common Client
< Aspi32.sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< eaps2kbd.sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< ghpciscan.sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< hcmon.sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< L8042prt.Sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< LmouFlr2.Sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< NAVENG.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< NAVEX15.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< NPDRIVER.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< PQNTDrv.sys >	?	Driver	This information is available in registered version only. Click here for more information.	
< SAVRT.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< SAVRTPEL.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< SYMEVENT.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	
< SYMREDRV.SYS >	?	Driver	This information is available in registered version only. Click here for more information.	

At the bottom of the window, there is a blue banner with the text 'Anti-Spy.Info' and a bomb icon. Below the banner, there are three instructions:

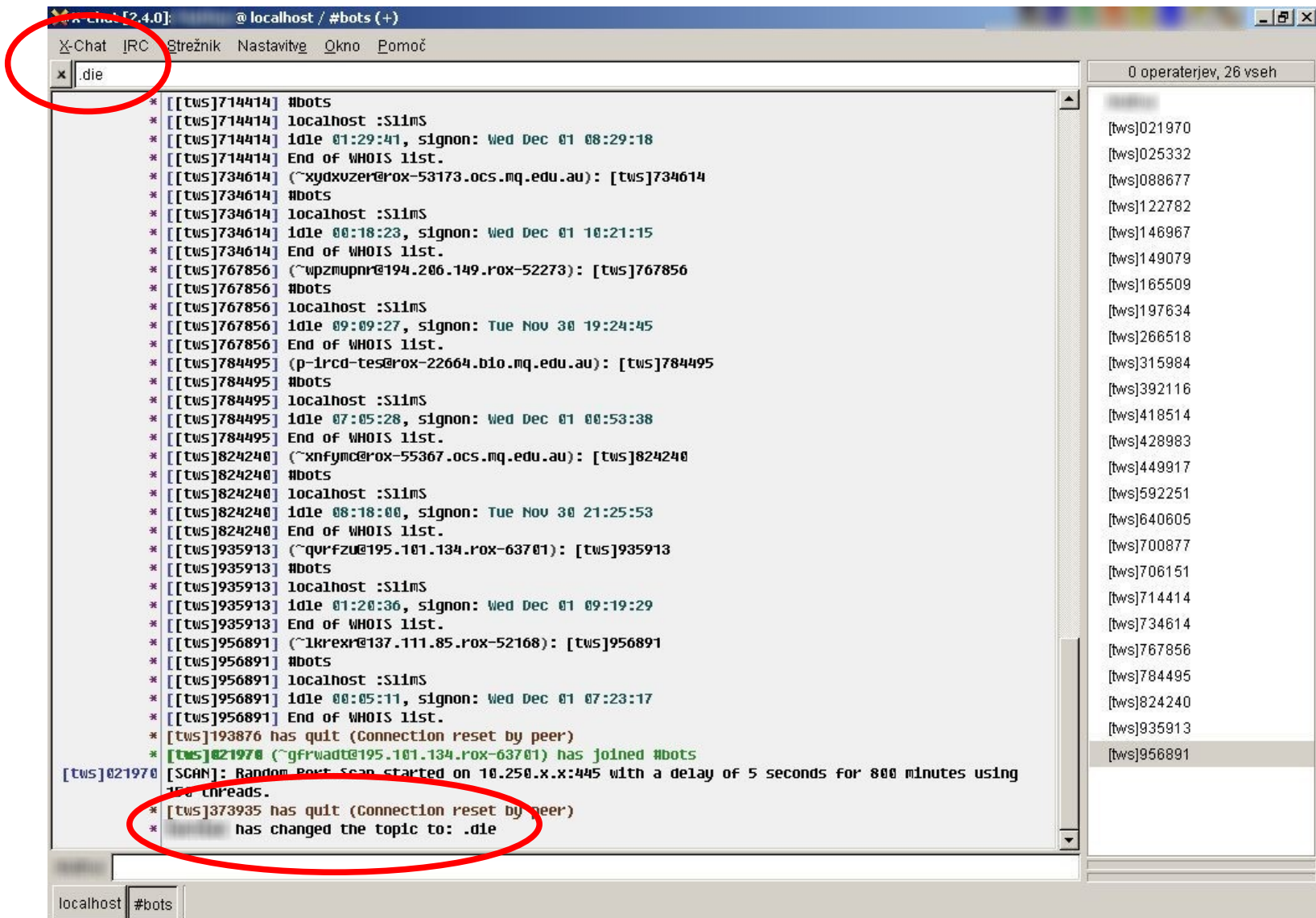
- Highly rated programs do not always have to be dangerous, because they just have some typical spyware properties.
- Click on a process to get more details.
- If you do not trust a process, you can quarantine it.

Sort by Rating

# Vstop v prikrito omrežje



# Neuspešen poiskus uničenja omrežja



## Hitro samodejno širjenje omrežja

- [01-12-2004 **10:48:47**] [tws]706151 [lsass\_445]: Exploiting IP: 203.232.133.153.
- [01-12-2004 **10:48:49**] [tws]706151 [FTP]: File transfer complete to IP: 203.232.133.153 (C:\WINDOWS\System32\mswins.exe).
- [01-12-2004 **10:50:22**] \* [tws]866541 (~itxuyafw@203.232.133.rox-62925) has joined #bots.

# **Eksperiment**

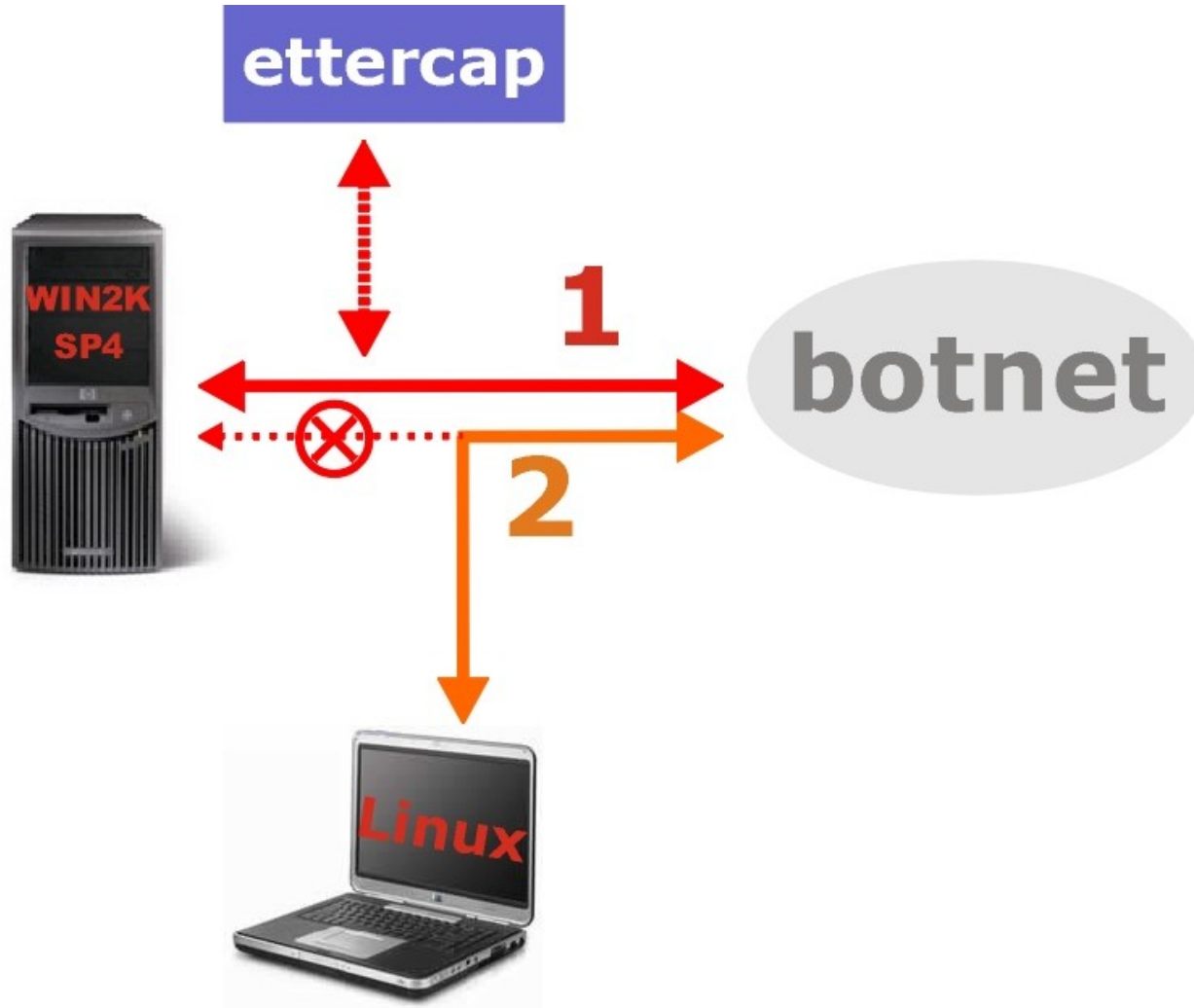
# Past

- Računalnik z nameščenimi Windows 2000 SP4, običajna namestitvev brez nalaganja dodatnih popravkov ali kakršnekoli programske opreme. Računalnik je bil vključen v internet in ni bil uporabljan.
- Vklop računalnika v internet: 8. december 2004 ob 17:35.
- **Uspešen vdor v 17-20 urah.**
- Vdor smo zaznali z analizo omrežnega prometa (z orodjem *ettercap*), z analizo povezave pa smo ugotovili kam se ugrabljeni računalnik povezuje.

# Maskiranje

- Maskirani 'bot': prenosni računalnik z nameščenim Debian Linux, jedro 2.6.8.1, vključen požarni zid, ki je blokiral vse vhodne povezave (razen 'veljavnega' ICMP prometa in SSH iz točno določenih IP naslovov). 'Bot' je bil maskiran pomočjo programa X-Chat (ime in vzdevek sta bila ustrezno izbrana), X-Chat je vse pogovore beležil v datoteko aktivnosti.
- Oblika maskiranja je razvidna iz prijave: "[stickibot]16133 (umw@Recycled-irc-3E9F4F46.fdv.uni-lj.si) has joined #STICKYWORLD".
- Začetek beleženja prometa na botnetu: 9. december 2004 ob 14:40:28.
- Konec beleženja prometa na botnetu: 3. januar 2005 ob 10:00:17.
- IRC strežnik preko katerega je bilo upravljano z botnetom je javno dostopen, celo preko web-a: **[http://info.recycled-irc.org/view\\_chan.php?chan=stickyworld](http://info.recycled-irc.org/view_chan.php?chan=stickyworld)**
- Tema kanala: ".advscan lsass\_445 100 3 9999 -r -b", nastavljen "StickyFingerz".

# Shema



# Maskiranje v X-Chatu

The screenshot shows the X-Chat IRC client interface. The title bar reads "X-Chat [2.4.0]: [stickibot]30324 @ wipe.recycled-irc.org / #STICKYWORLD (+ntr)". The main window displays a message from user [stickibot]30324: ".advscan lsass\_445 100 3 9999 -r -b". A context menu is open over the message, showing user information for [stickibot]50060. The menu items are: "Neposredno uporabnik-do-uporabnik", "CTCP", "Op", "Način", "Prezri", "Brični/zobči", "Podatki", "Zunanji", and "Odpri pogovorno okno".

Annotations in the image include:

- Red circles around the message text ".advscan lsass\_445 100 3 9999 -r -b" and the user name "[stickibot]50060" in the context menu.
- Red arrows pointing from the circles to red boxes labeled "prenosnik" and "Matej".
- A red circle around the user name "[stickibot]30324" in the top right corner of the chat window.

At the bottom of the window, the status bar shows the current user "[stickibot]30324" and the channel "#STICKYWORLD".

# Analiza datotek aktivnosti

- Datoteka aktivnosti je obsegala 961 vrstic sporočil.
- V času opazovanja se je na kanal prijavilo 96 botov + 3 lažni boti (187 *join*, 179 *quit*, vmes smo nekajkrat izgubili povezavo).
- 48 botov je javno sporočalo stanje na kanal (iz teh sporočil se lahko naučimo ukazov za upravljanje z boti), nekaj komunikacije je zagotovo potekalo tudi neposredno med upravljalcem omrežja in boti.
- Na kanal so se prijavljale tudi osebe, 10 *pseudonimov* se je pogovarjalo, ena oseba je zagotovo uporabljala več psevdonimov.

# Naključni obiskovalci - primeri

- **eXpLoSiV** - prišel iz *Owns.The.World.edu* za cca. 10 minut.
- **TaKoS** - prišel iz *wanadoo.fr* za cca. 2 minuti.
- **TheGame1492** - prišel dvakrat iz *t-dialin.net* za eno minuto.
- **M|SA** - prišel iz *.se* domene za cca. pol minute.

# Osebe, ki so na kanalu govorile

- Domnevni upravitelj omrežja:
  - StickyFingerz (Sticky@Recycled-irc-5B998540.dip.t-dialin.net): 86 sporočil
  - Stickyfingerz: 4 sporočil
  - DaStorm (~Sticky@Recycled-irc-CA58B3FF.dip.t-dialin.net): 14 sporočil
  - KinGaway (~Sticky@Recycled-irc-353F3876.dip.t-dialin.net): 10 sporočil
- Ostali, ki so komunicirali večinoma z njim:
  - klr54000: 75 sporočil
  - *Matej: 22 sporočil*
  - US-ShArK-s: 5 sporočil
  - Dr4gOoN: 2 sporočili
  - cedr1k: 1 sporočilo
  - NazBroque: 1 sporočilo

# Pridobitev gesla

- Počakamo, da se upravitelj omrežja prijavi na lažnega bot-a:
  - [09-12-2004 19:01:46]<StickyFingerz> **.login xxxxxxx**
  - [09-12-2004 19:20:38]<StickyFingerz> **.login xxxxxxx**
  - [09-12-2004 20:00:27]<-- StickyFingerz has quit (?? I was using Millenium.IRC 6.0 (Build: 6015.20030531 - Alpha Version) (milleniumirc.cjb.net) ??)
- V enem primeru je upravitelj omrežja zaklenil dostop do kanala (misleč, da so na kanalu samo boti) in potem uporabil geslo:
  - [21-12-2004 13:43:10]--- StickyFingerz sets channel keyword to **secret**
  - [21-12-2004 13:43:18]<StickyFingerz> **.login xxxxxxx**
  - [21-12-2004 13:43:18]<[stickibot]21632> [MAIN]: **Password accepted.**

# Upravljanje z boti\*

- **Prijava na bota:**

- [12-16-2004 13:03:29] Matej >.login **xxxxxxx**
- [12-16-2004 13:03:29] [stickibot]45479 >[MAIN]:  
**Password accepted.**

- **Ukazi:**

- [12-16-2004 13:03:35] Matej >.uptime
- [12-16-2004 13:03:36] [stickibot]45479 >[MAIN]:  
Uptime: 0d 3h 39m.
- [12-16-2004 13:03:42] Matej >.netinfo
- [12-16-2004 13:03:43] [stickibot]45479 >[NETINFO]:  
[Type]: LAN (LAN Connection). [IP Address]:  
**193.2.85.XXX.** [Hostname]: **XXX.FDV.UNI-LJ.SI.**

\* Ukazi in odzivi nanje so bili pridobljeni s pomočjo spremljanja prometa v prikitem omrežju ter s preskušanjem. Preskušanje ukazov je potekalo na okuženem računalniku; lastnik okuženega računalnika je bil s tem seznanjen oz. se je strinjal, na koncu je bil bot odstranjen iz okuženega računalnika.

# Upravljanje z boti

- **Ukazi:**
- [12-16-2004 13:03:50] Matej > **.driveinfo**
- [12-16-2004 13:03:51] [stickibot]45479 > [MAIN]: Disk Drive (C:\): 20,482,840KB total, 13,848,040KB free, 13,848,040KB available.
- [12-16-2004 13:03:53] [stickibot]45479 > [MAIN]: Disk Drive (D:\): 120,615,988KB total, 58,287,412KB free, 58,287,412KB available.
- [12-16-2004 13:03:55] [stickibot]45479 > [MAIN]: Disk Drive (E:\): 100,141,144KB total, 6,644,628KB free, 6,644,628KB available.

# Upravljanje z boti

- **Ukazi:**
- [12-16-2004 13:03:56] Matej > **.sysinfo**
- [12-16-2004 13:03:57] [stickibot]45479 > [MAIN]:  
Cdrom Drive (F:\): Failed to stat, device not ready.
- [12-16-2004 13:04:00] [stickibot]45479 > [SYSINFO]:  
[CPU]: 2400MHz. [RAM]: 1,048,048KB total,  
1,048,048KB free. [Disk]: 20,482,840KB total,  
13,848,040KB free. [OS]: Windows 2K (Service Pack 4)  
(5.0, Build 2195). [Sysdir]: C:\WINNT\system32.  
[Hostname]: XXX.FDV.UNI-LJ.SI (193.2.85.XXX).  
[Current User]: xxx\_xxx. [Date]: 16:Dec:2004. [Time]:  
13:01:44. [Uptime]: 0d 3h 39m.

# Upravljanje z boti

- **Ukazi:**

- [21-12-2004 13:48:51] StickyFingerz >.procs
- [21-12-2004 13:48:52] [stickibot]21632 >[PROC]: Listing processes:
- [21-12-2004 13:48:52] [stickibot]21632 > System (4)
- [21-12-2004 13:48:54] [stickibot]21632 > smss.exe (424)
- [21-12-2004 13:48:56] [stickibot]21632 > csrss.exe (528)
- ...
- [21-12-2004 13:49:46] [stickibot]21632 > sqlmangr.exe (3252)
- [21-12-2004 13:49:48] [stickibot]21632 > updateservereasy.exe (464)
- [21-12-2004 13:49:50] [stickibot]21632 > SincroServer.exe (2192)
- ...
- [21-12-2004 13:50:14] [stickibot]21632 > POP3Svc.exe (5996)
- ...
- [21-12-2004 13:50:22] [stickibot]21632 > explorer.exe (2148)
- [21-12-2004 13:50:24] [stickibot]21632 > NET Traffic Meter.exe (5408)
- ...
- [21-12-2004 13:50:50] [stickibot]21632 >[PROC]: Process list completed.

# Upravljanje z boti

- **Ukazi - iskanje varnostnih lukenj:**
- [21-12-2004 13:56:46] StickyFingerz >**.reboot**
- [21-12-2004 13:56:46] [stickibot]21632 >[MAIN]:  
Failed to reboot system.
  
- [21-12-2004 14:48:09] StickyFingerz >**.advscan  
lsass\_445 100 3 9999 -r -b**
- [21-12-2004 14:48:09] [stickibot]21632 >[SCAN]:  
Random Port Scan started on 192.168.x.x:445 with a  
delay of 5 seconds for 800 minutes using 100 threads.

# Upravljanje z boti

- **Ukazi – seznam varnostnih lukenj, ki jih bot izkorišča:**
- [12-16-2004 13:04:03] Matej > **.stats**
- [12-16-2004 13:04:04] [stickibot]45479 >[SCAN]:  
Exploit Statistics: WebDav: 0, NetBios: 0, NTPass: 0,  
Dcom135: 0, Dcom445: 0, Dcom1025: 0, Dcom2: 0,  
IIS5SSL: 0, MSSQL: 0, Beagle1: 0, Beagle2: 0,  
MyDoom: 0, Isass\_445: 0, Isass\_139: 0, Optix: 0,  
UPNP: 0, NetDevil: 0, DameWare: 0, Kuang2: 0, Sub7:  
0, Total: 0 in 0d 3h 29m.

# Upravljanje z boti

- **Ukazi**
- [12-16-2004 13:04:16] Matej > **.id**
- [12-16-2004 13:04:17] [stickibot]45479 >[MAIN]: Bot ID: sticki.
- [12-16-2004 13:04:21] Matej > **.version**
- [12-16-2004 13:04:22] [stickibot]45479 [MAIN]: [PeSt]
- [12-16-2004 13:04:27] Matej > **.scanstop**
- [12-16-2004 13:04:28] [stickibot]45479 >[SCAN]: No Scan thread found.

# Upravljanje z boti

- **Ukazi – odklop bota**
- [12-16-2004 13:04:32] Matej >**.remove**
- [12-16-2004 13:04:32] [stickibot]45479 >[MAIN]:  
**Removing Bot.**
- [12-16-2004 13:04:33] \* **[stickibot]45479 has quit (Client exited)**

# Ostali ukazi

muzzleflash.org - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://66.102.9.104/search?q=cache:z11ATKJUXuWJ:muzzleflash.org/articlecomments.php%3Farticle\_id%3D5+remove+... Go

tel\_imenik1.htm Leet to Plain Text c... GEEK TOOLS WINAMP.COM | Music SHOUTcast - HOME Instruments of Stat... FDV - Fakulteta za d...

This is **G o o g l e**'s cache of [http://muzzleflash.org/articlecomments.php?article\\_id=5](http://muzzleflash.org/articlecomments.php?article_id=5) as retrieved on 31 Dec 1969 23:59:59 GMT. **G o o g l e**'s cache is the snapshot that we took of the page as we crawled the web. The page may have changed since that time. Click here for the [current page](#) without highlighting. This cached page may reference images which are no longer available. Click here for the [cached text](#) only. To link to or bookmark this page, use the following url: [http://www.google.com/search?q=cache:z11ATKJUXuWJ:muzzleflash.org/articlecomments.php%3Farticle\\_id%3D5+remove+bot+netinfo+rxbot&hl=en&client=firefox-a](http://www.google.com/search?q=cache:z11ATKJUXuWJ:muzzleflash.org/articlecomments.php%3Farticle_id%3D5+remove+bot+netinfo+rxbot&hl=en&client=firefox-a)

*Google is not affiliated with the authors of this page nor responsible for its content.*

These search terms have been highlighted: **remove** **bot** **netinfo** **rxbot**

muzzleflash.org

[Home](#) | [FAQ](#) | [Articles](#) | [Forum](#) | [Add News](#) | [Admin](#) | Tuesday, November 02, 2004

Stuff

- [Home](#)
- [Articles](#)
- [Downloads](#)
- [Contact](#)
- [Guestbook](#)
- [Hot Links](#)

Latest Articles

- [About me](#)
- [RXbot Commandlist](#)

Guest

Username

Password

**RXbot** Commandlist  
Posted by [muzzleflash](#) on June 28 2004 - 19:36:02

## Command Reference

For **rxBot**

By some guy, cleaned up by me.

People who use this commandlist (and especially those who registered on the site): I'm almost done with moving to my new house. Once I'm settled in, you can expect a lot of new updates, a design overhaul, site engine upgrades, and cool new content. I'll also put together more command lists and maybe some guides, including one on how you can make beer money or even more \*legitly\* profiting off of zombies and spyware. If you'd like to be kept informed of updates, I suggest you register. Then you can be emailed when things begin. Anyway, thanks for liking the commandlist. Live long in whatever you do, and I hope you damn well prosper! ;)

Oh, and check out the link section. There's some awesome stuff in there.

[General Commands](#) - [Scanning Functions](#) - [Clones](#) - [DDoS Functions](#) - [Downloading & Updating](#) - [Redirecting](#) - [FTP Functions](#)

Command Name	Alias	Syntax	Command Information	Example
--------------	-------	--------	---------------------	---------

Done M 0 Adblock