ISS – X-Force Professional Security Services

Malware Forensics: Detecting The Unknown

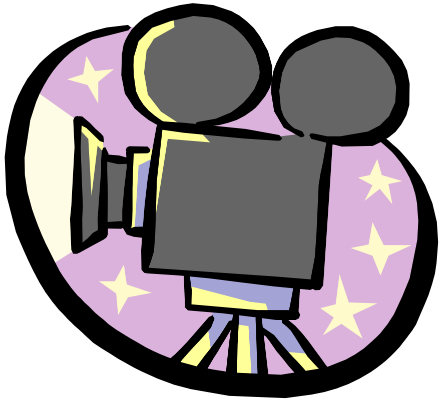
- Martin Overton
- Malware/Anti-Malware SME

Abstract

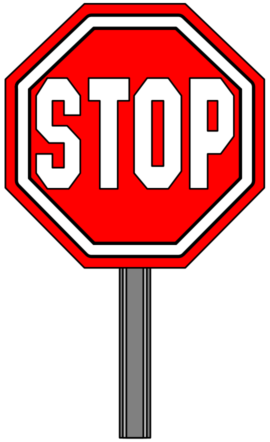
- *The increasing speed of new malware strains being written and released means that security professionals are more likely than ever before to see new malware.*
- *This means new malware which is not detected by the anti-malware solutions they have deployed in their infrastructure, be it workstation, server, PDA or at the gateway.*
- *Imagine this scenario: An end-user calls the helpdesk and reports that their system is running very sluggishly when it wasn't a week ago and that they can't access the Windows 'Task Manager' or open a command prompt any more.*
- *Is this caused by malware or is it a 'user' problem? The virus scanner is right up to date and active, and it says the system is clean; the personal firewall is active too. Where do you go from here? Investigate or rebuild the box?*
- *How can you tell if the machine is clean or infected by a new malware, with a reasonable level of confidence for your conclusion?*
- *The paper looks at what tricks, tools and techniques you can use to help establish the true state of the 'suspect' system. It will focus on a step by step approach of what tools to use, what to look for and what to do with any suspicious files. It will also discuss the use of forensic tools in such a scenario, as a last port of call.*
- *The paper draws on real scenarios where new [undetected] malware has been responsible for 'odd' system or network behaviour.*

Agenda

- Disclaimer
- What is Malware?
- Solutions
  - Steps 1-6
  - Conclusions
- Questions



Disclaimer



- Products named in this presentation are used as examples only, and should not be taken as any form of endorsement by IBM or ISS.

- All trademarks and copyrights are acknowledged.

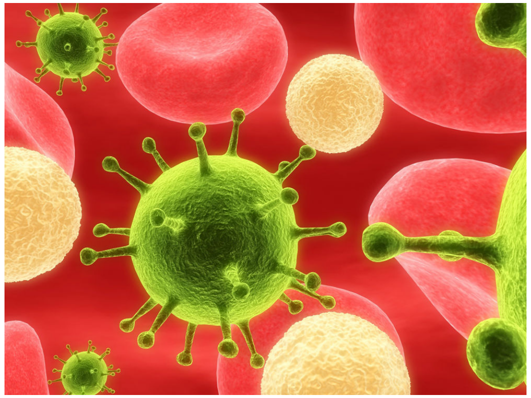
What is Malware?

- “Malware is the generic name [or short name] used to describe **Mal**icious Soft**ware**. This includes viruses, worms, Trojans, bots and related threats…”

Source: Bots and Botnets: Risks, Issues and Prevention, VB2005

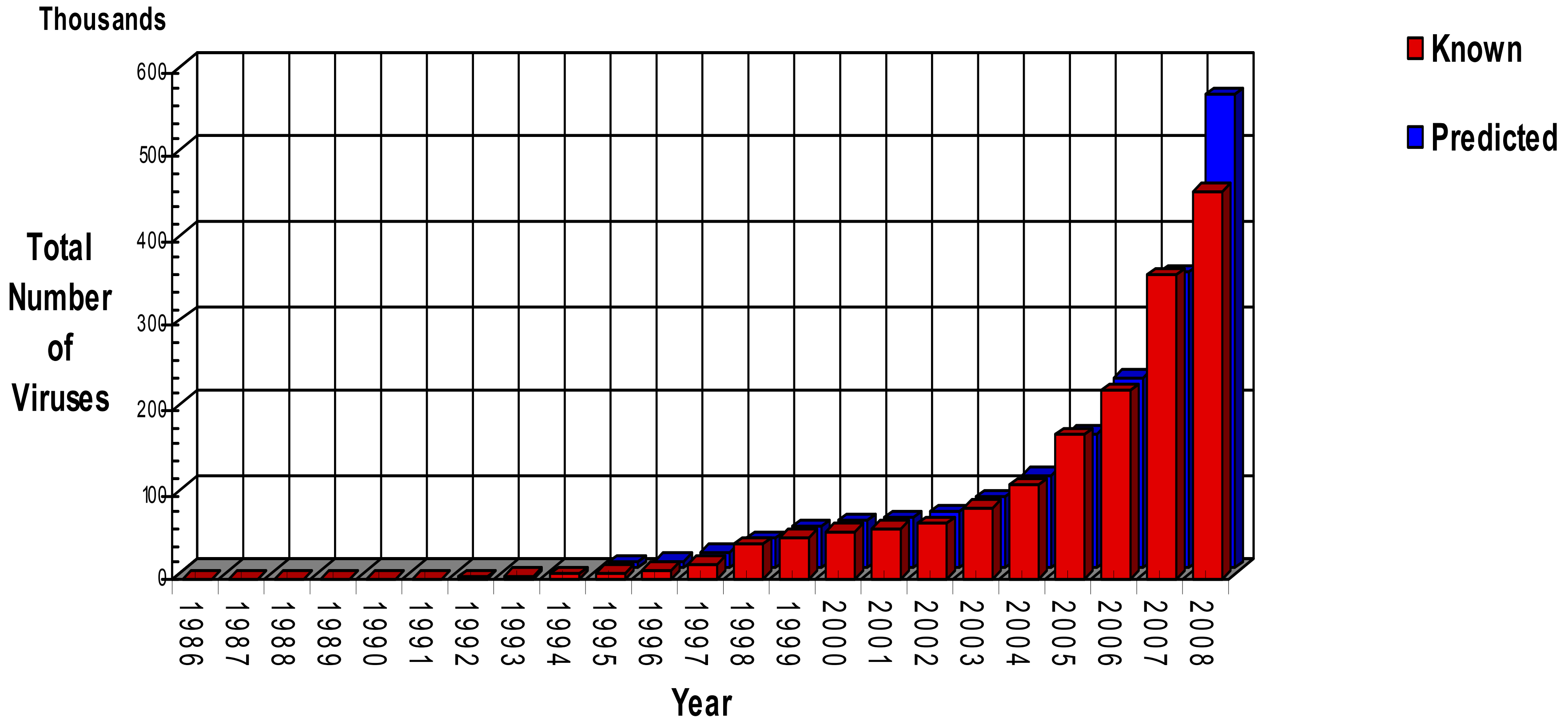
Speed of infection/infestation?

- **How long can an unprotected PC last on the Internet before it gets infected/infested?**
  - According to SOPHOS, just 720 seconds!

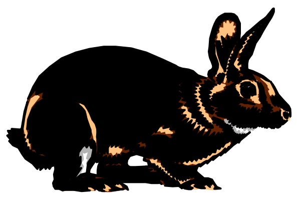


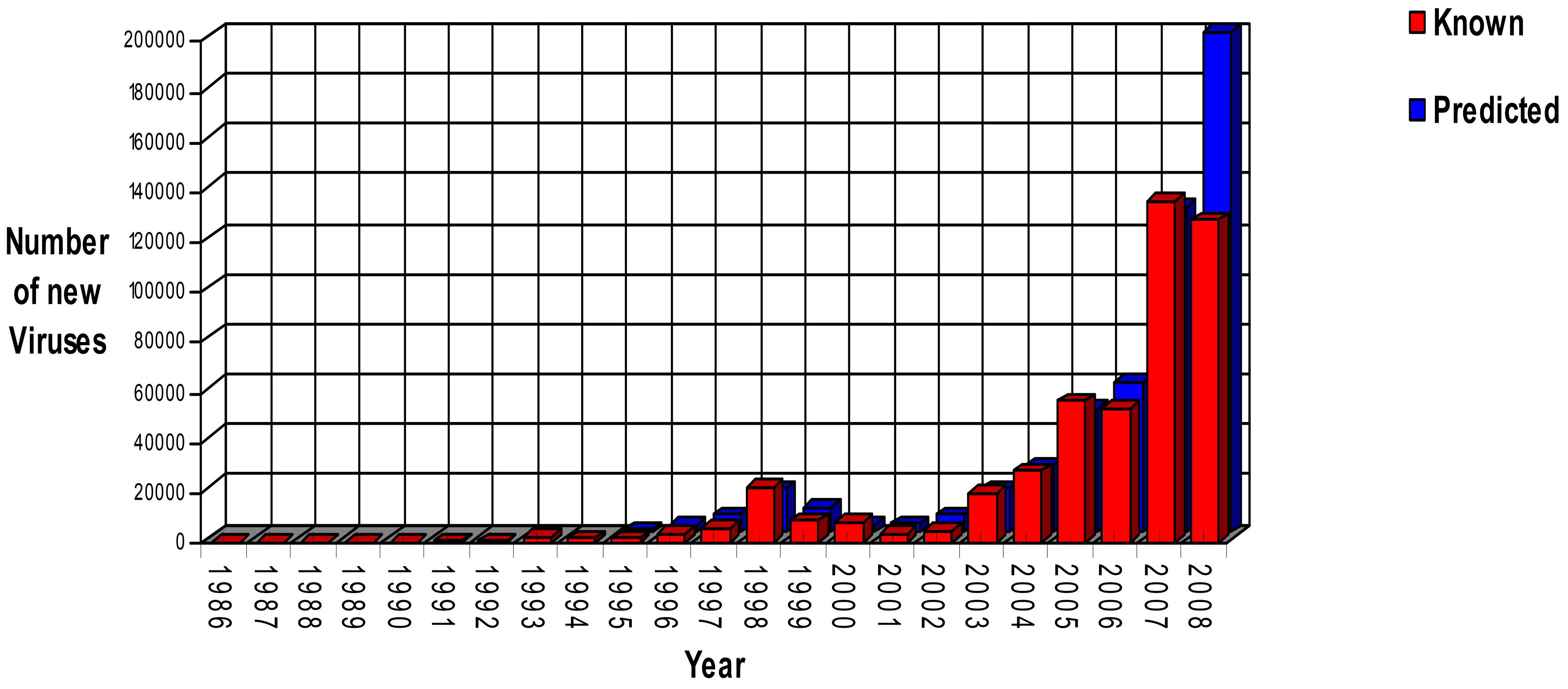
- **Here's a quote from them which was used in an article on The Register in 2005:**
  - "*More computer viruses and worms mean an unprotected Windows PC (without either firewall or antivirus protection) stands a 50 per cent chance of infection by a worm after just 12 minutes online. Graham Cluley, senior technology consultant at Sophos, conceded*"

Virus Growth - Running Total
(by year: actual and predicted)



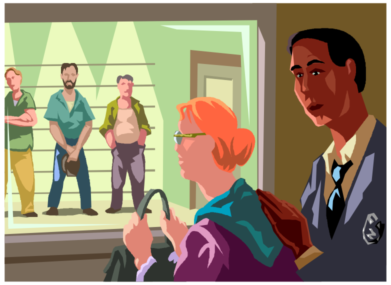
Virus Growth (Actual)
(by year: actual and predicted)





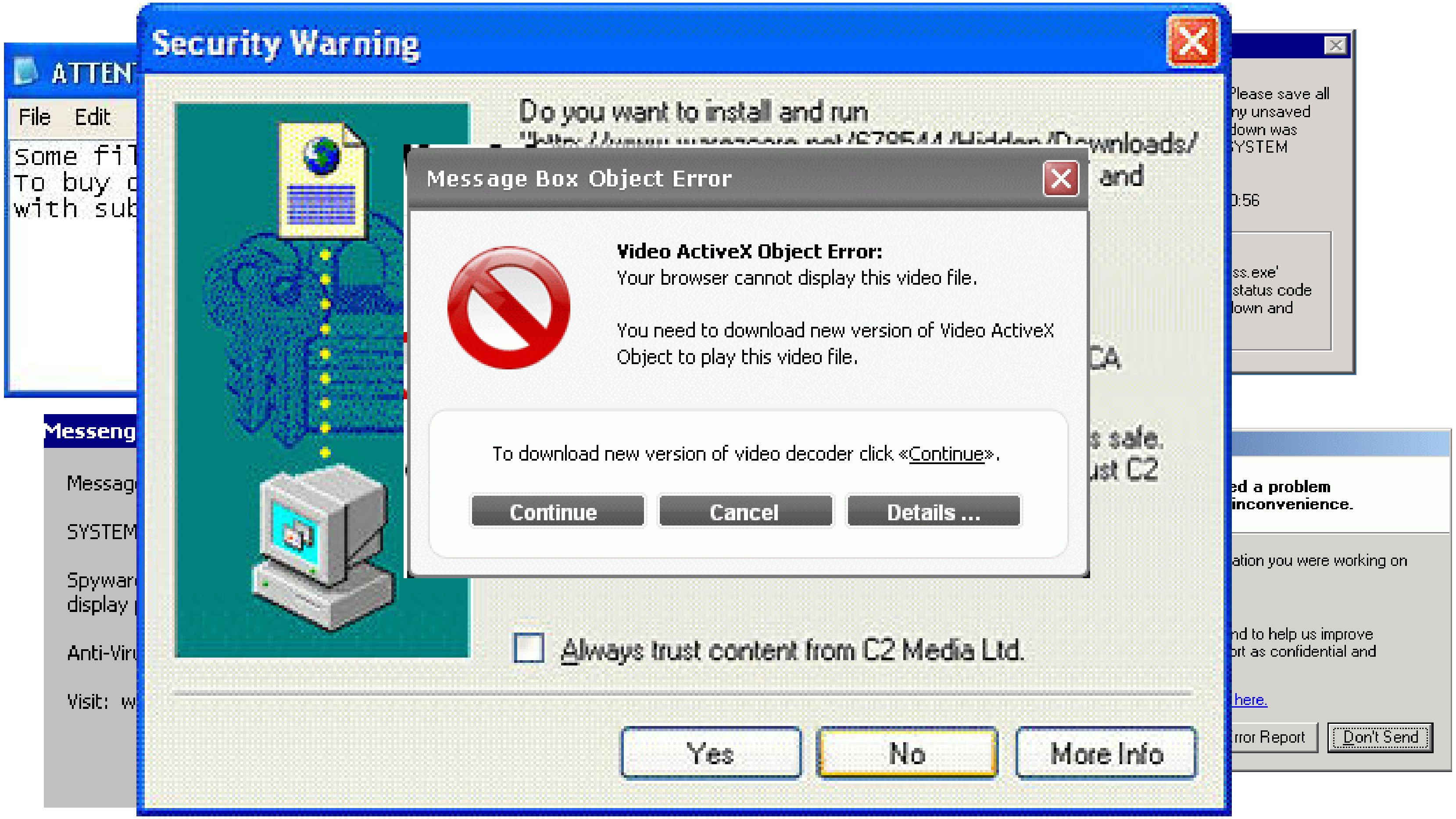
Solutions……

Step 1: Identifying Suspect Systems



- **The first thing to do is to understand that you have a problem**
  - the next thing to do is to try and identify possible systems that may be infected.
- **This information can come from:**
  - help-desk tickets [personal firewall or anti-malware alerts, strange system behaviour, etc], Log files from your routers, proxies, firewalls, IDS/IPS systems, DNS and so on, or maybe even just a passing comment from a colleague or even a customer or other third party [maybe to your *abuse@yourdomain.com* e-mail address].
- **Once you have a potential suspect, gather all the data you can from it and network traffic to and from it.**
- **Once the machine has been removed from the main network, you can either investigate it in isolation or move it to a test [secure] network used for analysing suspected infected systems.**
- **To analyse suspected traffic on your test network you could use tools such as SNORT, WireShark or WinDump.**
- **You may also decide to carry out some vulnerability assessment of the suspected system; this can be done via tools such as Nmap, Superscan, Nessus or the Microsoft Baseline Security Analyzer.**

Error Messages Are Your Friends



Security Warning

Do you want to install and run

and

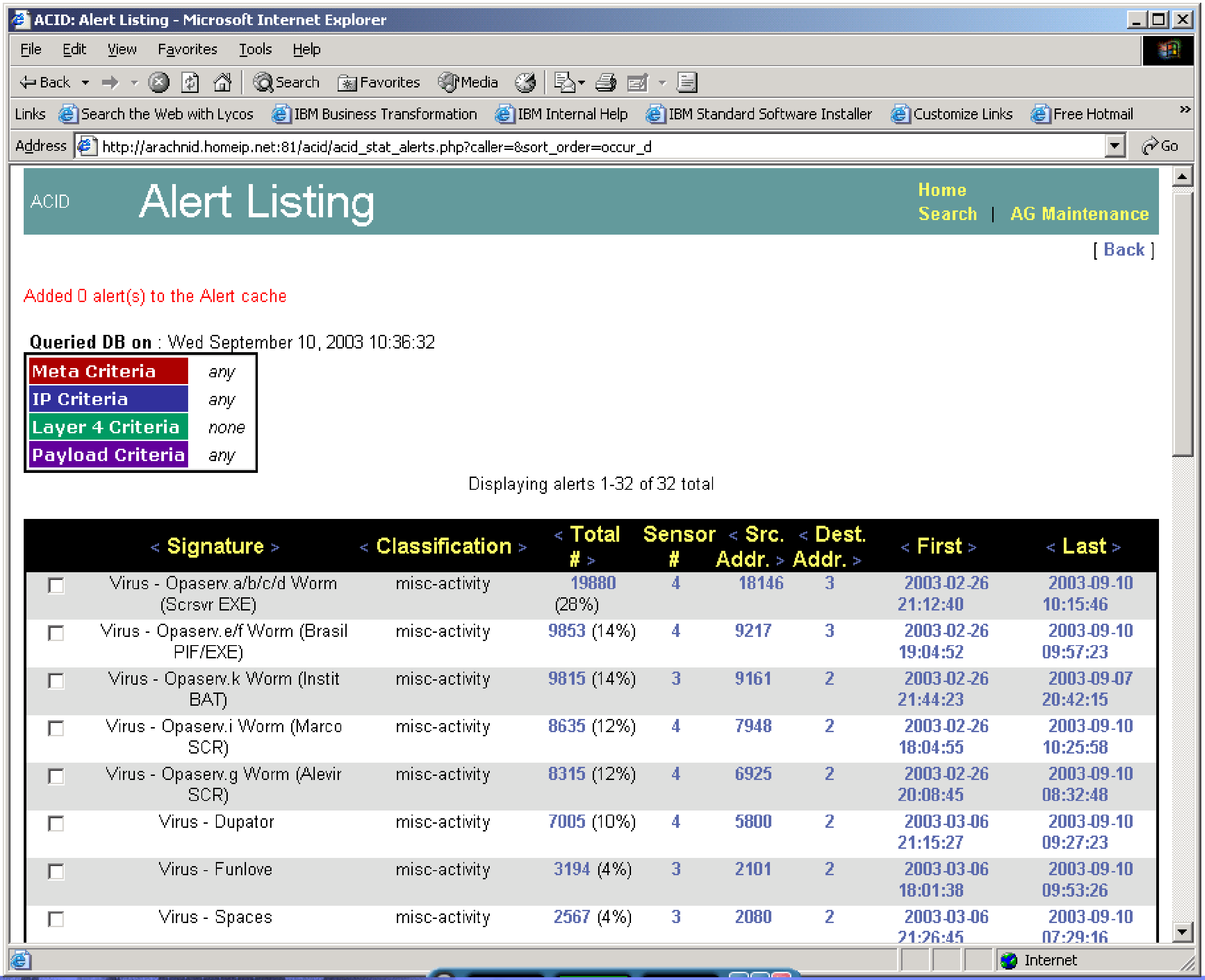
Message Box Object Error

Video ActiveX Object Error:
Your browser cannot display this video file.

You need to download new version of Video ActiveX Object to play this video file.

To download new version of video decoder click «Continue».

SNORT


ACID: Alert Listing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links Search the Web with Lycos IBM Business Transformation IBM Internal Help IBM Standard Software Installer Customize Links Free Hotmail
Address
Go
Internet

http://arachnid.homeip.net:81/acid/acid_stat_alerts.php?caller=&sort_order=occur_d

ACID **Alert Listing**

Home
Search | AG Maintenance

[Back]

Added 0 alert(s) to the Alert cache

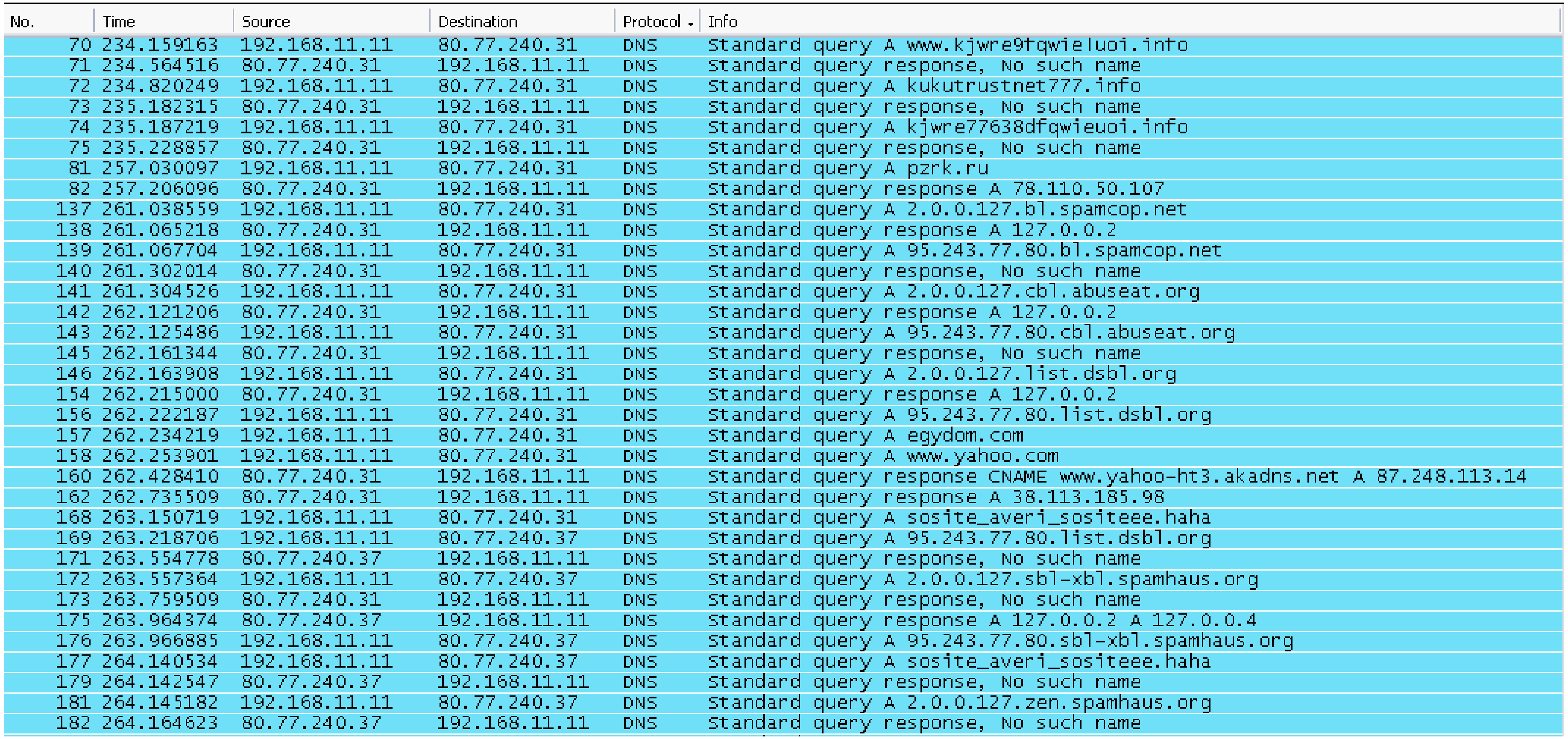
Queried DB on : Wed September 10, 2003 10:36:32

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying alerts 1-32 of 32 total

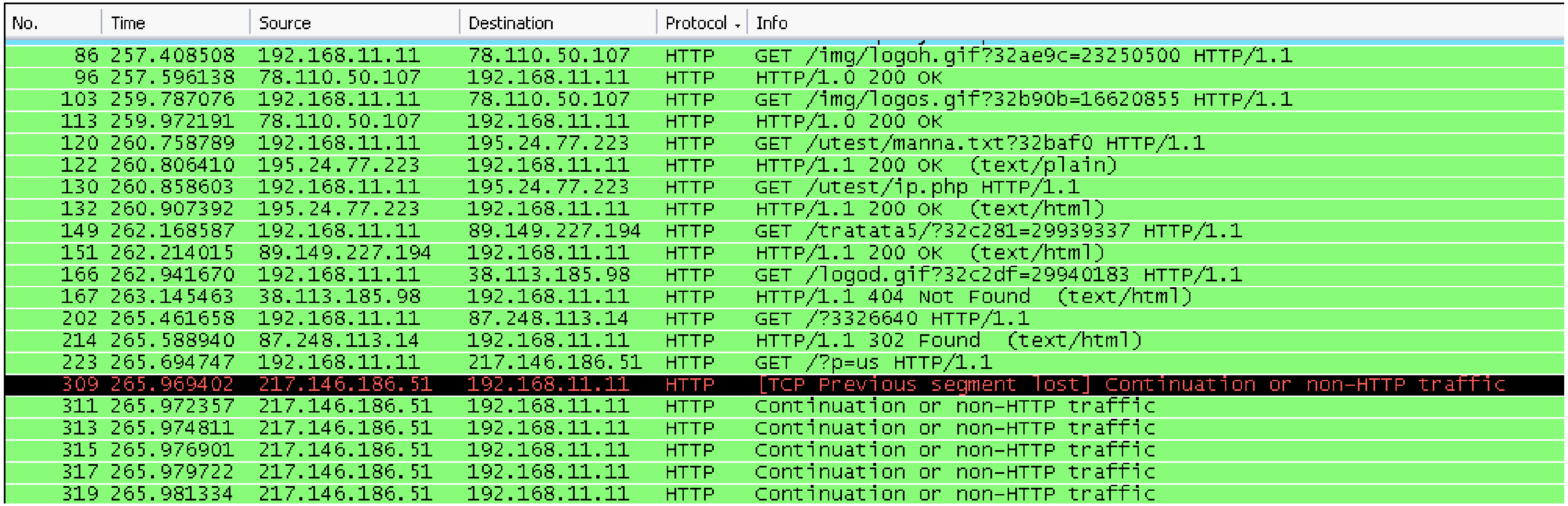
	< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
□	Virus - Opaserv.a/b/c/d Worm (Scrsvr EXE)	misc-activity	19880 (28%)	4	18146	3	2003-02-26 21:12:40	2003-09-10 10:15:46
□	Virus - Opaserv.e/f Worm (Brasil PIF/EXE)	misc-activity	9853 (14%)	4	9217	3	2003-02-26 19:04:52	2003-09-10 09:57:23
□	Virus - Opaserv.k Worm (Instit BAT)	misc-activity	9815 (14%)	3	9161	2	2003-02-26 21:44:23	2003-09-07 20:42:15
□	Virus - Opaserv.i Worm (Marco SCR)	misc-activity	8635 (12%)	4	7948	2	2003-02-26 18:04:55	2003-09-10 10:25:58
□	Virus - Opaserv.g Worm (Alevir SCR)	misc-activity	8315 (12%)	4	6925	2	2003-02-26 20:08:45	2003-09-10 08:32:48
□	Virus - Dupator	misc-activity	7005 (10%)	4	5800	2	2003-03-06 21:15:27	2003-09-10 09:27:23
□	Virus - Funlove	misc-activity	3194 (4%)	3	2101	2	2003-03-06 18:01:38	2003-09-10 09:53:26
□	Virus - Spaces	misc-activity	2567 (4%)	3	2080	2	2003-03-06 21:26:45	2003-09-10 07:29:16

Wireshark - Win32/Sality.nar - DNS



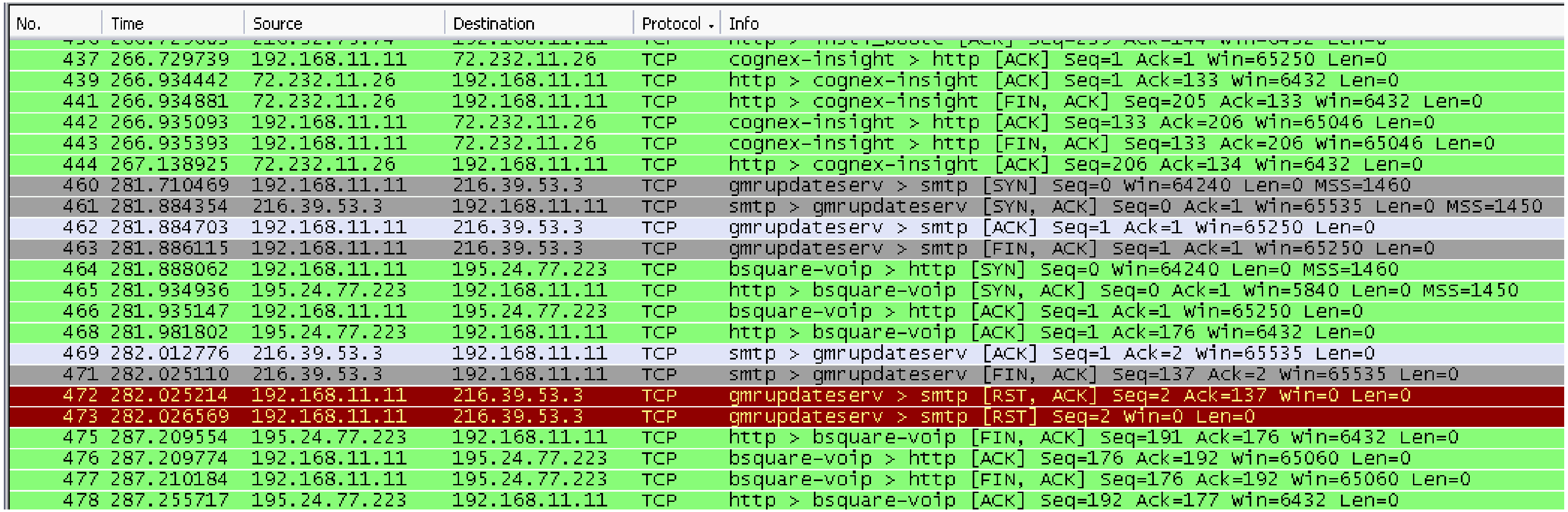
No.	Time	Source	Destination	Protocol	Info
70	234.159163	192.168.11.11	80.77.240.31	DNS	Standard query A www.kjwre9fqwieluoi.info
71	234.564516	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
72	234.820249	192.168.11.11	80.77.240.31	DNS	Standard query A kukutrustnet777.info
73	235.182315	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
74	235.187219	192.168.11.11	80.77.240.31	DNS	Standard query A kjwre77638dfqwieuoi.info
75	235.228857	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
81	257.030097	192.168.11.11	80.77.240.31	DNS	Standard query A pzrk.ru
82	257.206096	80.77.240.31	192.168.11.11	DNS	Standard query response A 78.110.50.107
137	261.038559	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.bl.spamcop.net
138	261.065218	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
139	261.067704	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.bl.spamcop.net
140	261.302014	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
141	261.304526	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.cbl.abuseat.org
142	262.121206	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
143	262.125486	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.cbl.abuseat.org
145	262.161344	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
146	262.163908	192.168.11.11	80.77.240.31	DNS	Standard query A 2.0.0.127.list.dsbl.org
154	262.215000	80.77.240.31	192.168.11.11	DNS	Standard query response A 127.0.0.2
156	262.222187	192.168.11.11	80.77.240.31	DNS	Standard query A 95.243.77.80.list.dsbl.org
157	262.234219	192.168.11.11	80.77.240.31	DNS	Standard query A egydom.com
158	262.253901	192.168.11.11	80.77.240.31	DNS	Standard query A www.yahoo.com
160	262.428410	80.77.240.31	192.168.11.11	DNS	Standard query response CNAME www.yahoo-ht3.akadns.net A 87.248.113.14
162	262.735509	80.77.240.31	192.168.11.11	DNS	Standard query response A 38.113.185.98
168	263.150719	192.168.11.11	80.77.240.31	DNS	Standard query A sosite_averi_sositeee.haha
169	263.218706	192.168.11.11	80.77.240.37	DNS	Standard query A 95.243.77.80.list.dsbl.org
171	263.554778	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name
172	263.557364	192.168.11.11	80.77.240.37	DNS	Standard query A 2.0.0.127.sbl-xbl.spamhaus.org
173	263.759509	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
175	263.964374	80.77.240.37	192.168.11.11	DNS	Standard query response A 127.0.0.2 A 127.0.0.4
176	263.966885	192.168.11.11	80.77.240.37	DNS	Standard query A 95.243.77.80.sbl-xbl.spamhaus.org
177	264.140534	192.168.11.11	80.77.240.37	DNS	Standard query A sosite_averi_sositeee.haha
179	264.142547	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name
181	264.145182	192.168.11.11	80.77.240.37	DNS	Standard query A 2.0.0.127.zen.spamhaus.org
182	264.164623	80.77.240.37	192.168.11.11	DNS	Standard query response, No such name

Wireshark - Win32/Sality.nar - HTTP



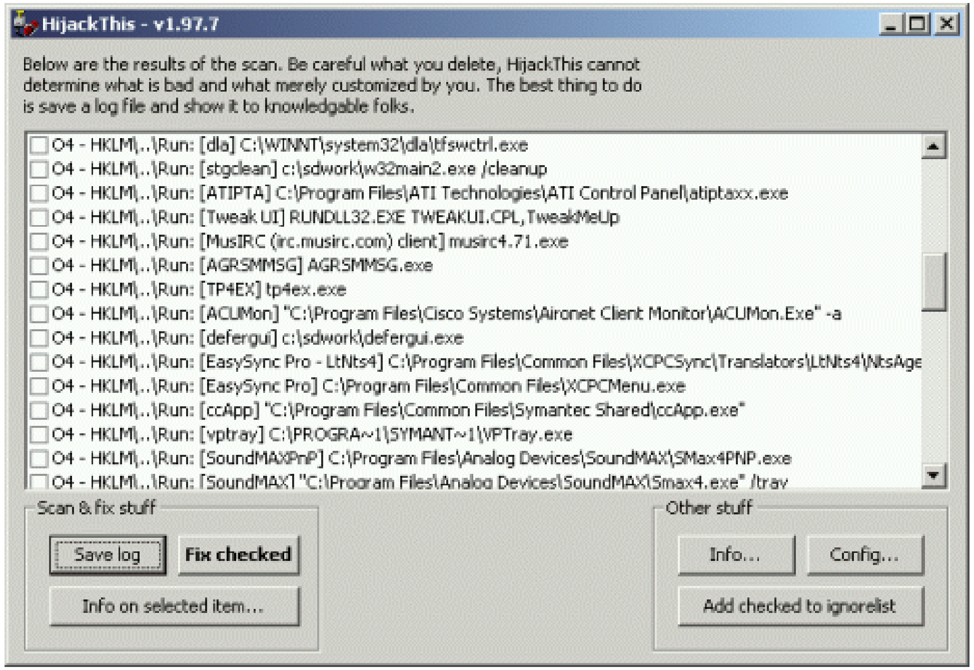
No.	Time	Source	Destination	Protocol	Info
86	257.408508	192.168.11.11	78.110.50.107	HTTP	GET /img/logoh.gif?32ae9c=23250500 HTTP/1.1
96	257.596138	78.110.50.107	192.168.11.11	HTTP	HTTP/1.0 200 OK
103	259.787076	192.168.11.11	78.110.50.107	HTTP	GET /img/logos.gif?32b90b=16620855 HTTP/1.1
113	259.972191	78.110.50.107	192.168.11.11	HTTP	HTTP/1.0 200 OK
120	260.758789	192.168.11.11	195.24.77.223	HTTP	GET /utest/manna.txt?32baf0 HTTP/1.1
122	260.806410	195.24.77.223	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/plain)
130	260.858603	192.168.11.11	195.24.77.223	HTTP	GET /utest/ip.php HTTP/1.1
132	260.907392	195.24.77.223	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/html)
149	262.168587	192.168.11.11	89.149.227.194	HTTP	GET /tratata5/?32c281=29939337 HTTP/1.1
151	262.214015	89.149.227.194	192.168.11.11	HTTP	HTTP/1.1 200 OK (text/html)
166	262.941670	192.168.11.11	38.113.185.98	HTTP	GET /logod.gif?32c2df=29940183 HTTP/1.1
167	263.145463	38.113.185.98	192.168.11.11	HTTP	HTTP/1.1 404 Not Found (text/html)
202	265.461658	192.168.11.11	87.248.113.14	HTTP	GET /?3326640 HTTP/1.1
214	265.588940	87.248.113.14	192.168.11.11	HTTP	HTTP/1.1 302 Found (text/html)
223	265.694747	192.168.11.11	217.146.186.51	HTTP	GET /?p=us HTTP/1.1
309	265.969402	217.146.186.51	192.168.11.11	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
311	265.972357	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
313	265.974811	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
315	265.976901	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
317	265.979722	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic
319	265.981334	217.146.186.51	192.168.11.11	HTTP	Continuation or non-HTTP traffic

Wireshark - Win32/Sality.nar - SMTP



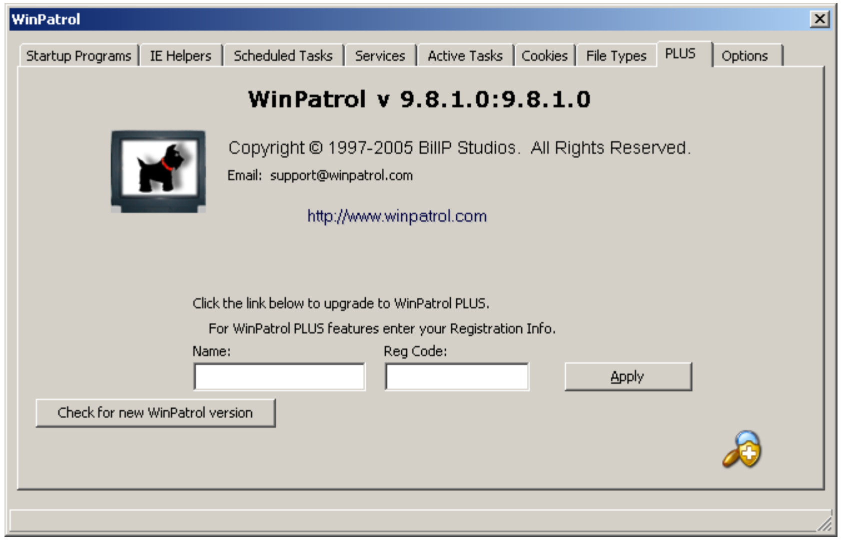
```
No.  Time        Source          Destination     Protocol  Info
437  266.729739  192.168.11.11   72.232.11.26    TCP       cognex-insight > http [ACK] Seq=1 Ack=1 Win=65250 Len=0
439  266.934442  72.232.11.26    192.168.11.11   TCP       http > cognex-insight [ACK] Seq=1 Ack=133 Win=6432 Len=0
441  266.934881  72.232.11.26    192.168.11.11   TCP       http > cognex-insight [FIN, ACK] Seq=205 Ack=133 Win=6432 Len=0
442  266.935093  192.168.11.11   72.232.11.26    TCP       cognex-insight > http [ACK] Seq=133 Ack=206 Win=65046 Len=0
443  266.935393  192.168.11.11   72.232.11.26    TCP       cognex-insight > http [FIN, ACK] Seq=133 Ack=206 Win=65046 Len=0
444  267.138925  72.232.11.26    192.168.11.11   TCP       http > cognex-insight [ACK] Seq=206 Ack=134 Win=6432 Len=0
460  281.710469  192.168.11.11   216.39.53.3     TCP       gmrupdateserv > smtp [SYN] Seq=0 Win=64240 Len=0 MSS=1460
461  281.884354  216.39.53.3     192.168.11.11   TCP       smtp > gmrupdateserv [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1450
462  281.884703  192.168.11.11   216.39.53.3     TCP       gmrupdateserv > smtp [ACK] Seq=1 Ack=1 Win=65250 Len=0
463  281.886115  192.168.11.11   216.39.53.3     TCP       gmrupdateserv > smtp [FIN, ACK] Seq=1 Ack=1 Win=65250 Len=0
464  281.888062  192.168.11.11   195.24.77.223   TCP       bsquare-voip > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
465  281.934936  195.24.77.223   192.168.11.11   TCP       http > bsquare-voip [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1450
466  281.935147  192.168.11.11   195.24.77.223   TCP       bsquare-voip > http [ACK] Seq=1 Ack=1 Win=65250 Len=0
468  281.981802  195.24.77.223   192.168.11.11   TCP       http > bsquare-voip [ACK] Seq=1 Ack=176 Win=6432 Len=0
469  282.012776  216.39.53.3     192.168.11.11   TCP       smtp > gmrupdateserv [ACK] Seq=1 Ack=2 Win=65535 Len=0
471  282.025110  216.39.53.3     192.168.11.11   TCP       smtp > gmrupdateserv [FIN, ACK] Seq=137 Ack=2 Win=65535 Len=0
472  282.025214  192.168.11.11   216.39.53.3     TCP       gmrupdateserv > smtp [RST, ACK] Seq=2 Ack=137 Win=0 Len=0
473  282.026569  192.168.11.11   216.39.53.3     TCP       gmrupdateserv > smtp [RST] Seq=2 Win=0 Len=0
475  287.209554  195.24.77.223   192.168.11.11   TCP       http > bsquare-voip [FIN, ACK] Seq=191 Ack=176 Win=6432 Len=0
476  287.209774  192.168.11.11   195.24.77.223   TCP       bsquare-voip > http [ACK] Seq=176 Ack=192 Win=65060 Len=0
477  287.210184  192.168.11.11   195.24.77.223   TCP       bsquare-voip > http [FIN, ACK] Seq=176 Ack=192 Win=65060 Len=0
478  287.255717  195.24.77.223   192.168.11.11   TCP       http > bsquare-voip [ACK] Seq=192 Ack=177 Win=6432 Len=0
```

HijackThis, WinPatrol



Below are the results of the scan. Be careful what you delete, HijackThis cannot determine what is bad and what merely customized by you. The best thing to do is save a log file and show it to knowledgable folks.

```
□ O4 - HKLM\..\Run: [dla] C:\WINNT\system32\dla\tfswctrl.exe
□ O4 - HKLM\..\Run: [stgclean] c:\sdwork\w32main2.exe /cleanup
□ O4 - HKLM\..\Run: [ATIPTA] C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe
□ O4 - HKLM\..\Run: [Tweak UI] RUNDLL32.EXE TWEAKUI.CPL,TweakMeUp
□ O4 - HKLM\..\Run: [MusIRC (irc.musirc.com) client] musirc4.71.exe
□ O4 - HKLM\..\Run: [AGRSMMSG] AGRSMMSG.exe
□ O4 - HKLM\..\Run: [TP4EX] tp4ex.exe
□ O4 - HKLM\..\Run: [ACUMon] "C:\Program Files\Cisco Systems\Aironet Client Monitor\ACUMon.Exe" -a
□ O4 - HKLM\..\Run: [defergui] c:\sdwork\defergui.exe
□ O4 - HKLM\..\Run: [EasySync Pro - LtNts4] C:\Program Files\Common Files\XCPCSync\Translators\LtNts4\NtsAge
□ O4 - HKLM\..\Run: [EasySync Pro] C:\Program Files\Common Files\XCPCMenu.exe
□ O4 - HKLM\..\Run: [ccApp] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
□ O4 - HKLM\..\Run: [vptray] C:\PROGRA~1\SYMANT~1\VPTray.exe
□ O4 - HKLM\..\Run: [SoundMAXPnP] C:\Program Files\Analog Devices\SoundMAX\SMax4PNP.exe
□ O4 - HKLM\..\Run: [SoundMAX] "C:\Program Files\Analog Devices\SoundMAX\Smax4.exe" /tray
```



WinPatrol v 9.8.1.0:9.8.1.0

Copyright © 1997-2005 BillP Studios. All Rights Reserved.

Email: support@winpatrol.com

http://www.winpatrol.com

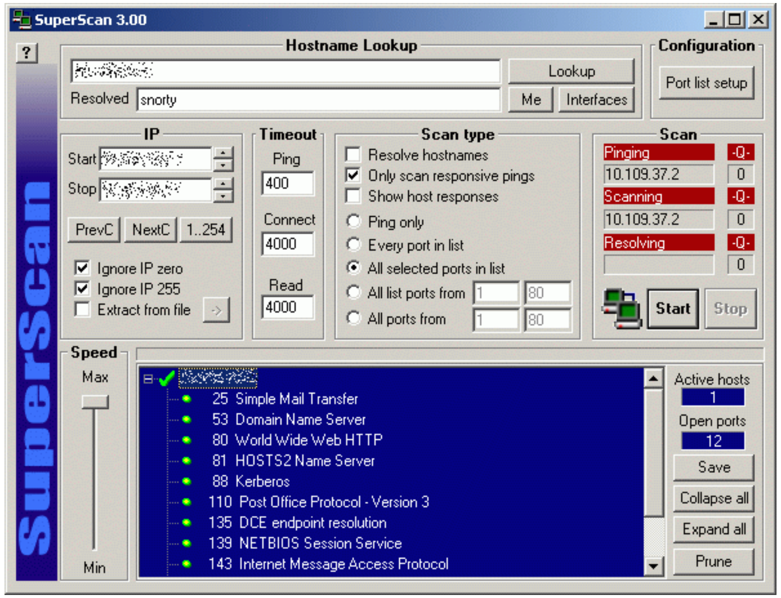
Click the link below to upgrade to WinPatrol PLUS.

For WinPatrol PLUS features enter your Registration Info.

Name:

Reg Code:

Superscan, Nmap, Netstat



Hostname: [redacted]
Resolved: snorty

IP Start: [redacted]
IP Stop: [redacted]

☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

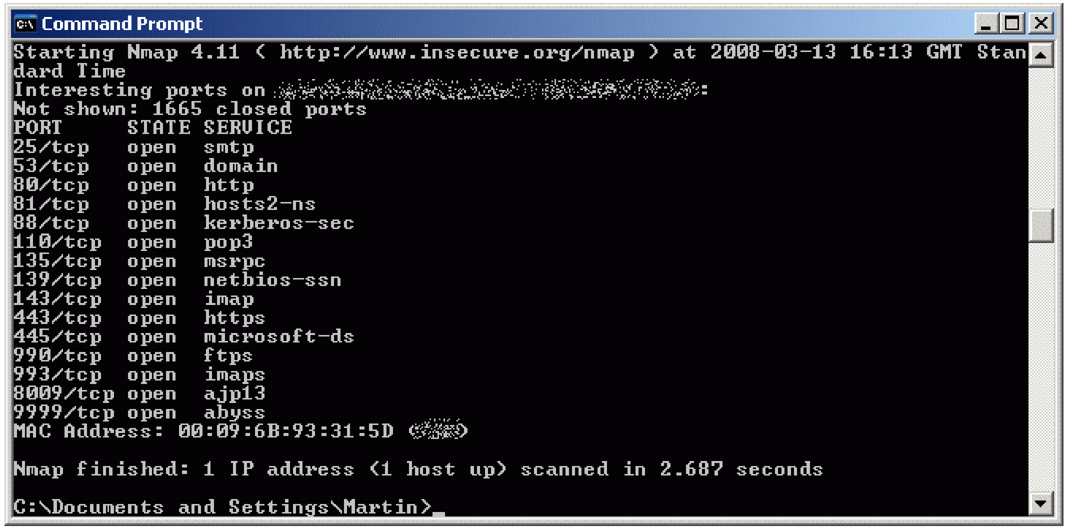
Timeout — Ping: 400 — Connect: 4000 — Read: 4000

Scan type:
☐ Resolve hostnames
☑ Only scan responsive pings
☐ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 80
○ All ports from 1 80

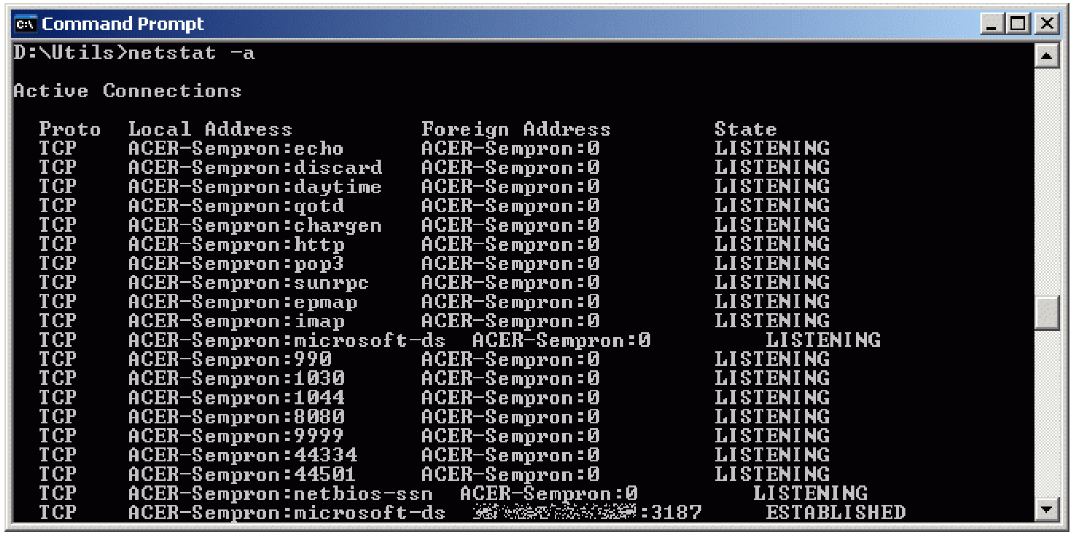
Pinging	-Q-
10.109.37.2	0
Scanning	-Q-
10.109.37.2	0
Resolving	-Q-
	0

[redacted]
- 25 Simple Mail Transfer
- 53 Domain Name Server
- 80 World Wide Web HTTP
- 81 HOSTS2 Name Server
- 88 Kerberos
- 110 Post Office Protocol - Version 3
- 135 DCE endpoint resolution
- 139 NETBIOS Session Service
- 143 Internet Message Access Protocol

Active hosts: 1
Open ports: 12



```
Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2008-03-13 16:13 GMT Stan
dard Time
Interesting ports on [redacted]:
Not shown: 1665 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
88/tcp    open  kerberos-sec
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
990/tcp   open  ftps
993/tcp   open  imaps
8009/tcp  open  ajp13
9999/tcp  open  abyss
MAC Address: 00:09:6B:93:31:5D [redacted]

Nmap finished: 1 IP address (1 host up) scanned in 2.687 seconds

C:\Documents and Settings\Martin>
```



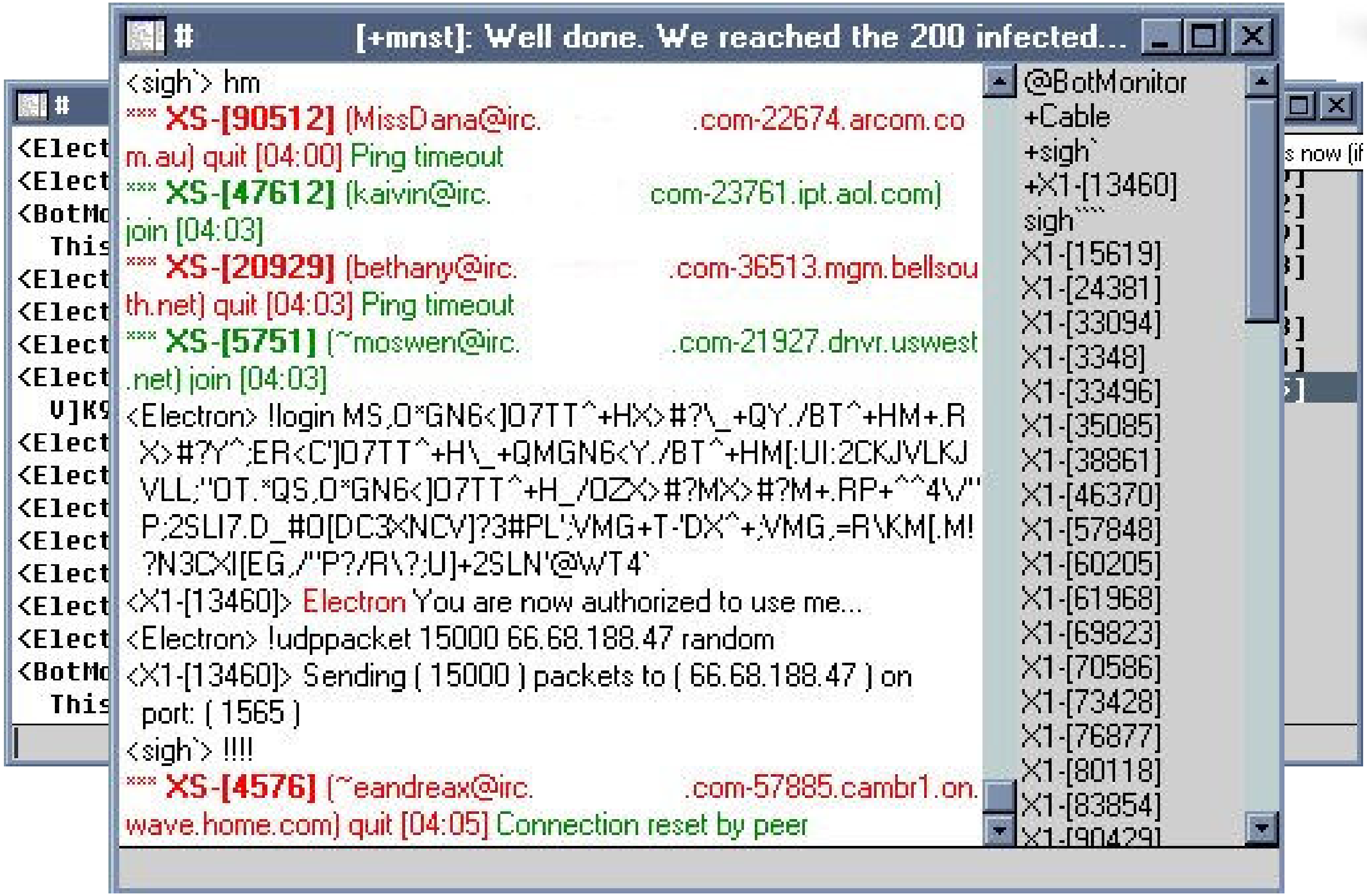
```
D:\Utils>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    ACER-Sempron:echo      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:discard   ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:daytime   ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:qotd      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:chargen   ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:http      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:pop3      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:sunrpc    ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:epmap     ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:imap      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:microsoft-ds  ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:990       ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:1030      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:1044      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:8080      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:9999      ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:44334     ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:44501     ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:netbios-ssn  ACER-Sempron:0         LISTENING
  TCP    ACER-Sempron:microsoft-ds  [redacted]:3187      ESTABLISHED
```

Step 2: Analyse The Data (Part 1)

- **At this point you may already be able to state with some level of confidence that the system is infected by a malcode which *phones-home.***
  - Examples of these include bot clients, or a Trojan or multi-component malcode [such as a dropper] that has contacted one or more websites to download other malcode or adware to install. This act, in many cases effectively starts a chain reaction leading to a heavily infected system with tens or hundreds of malcode files [or components] installed.

- **In either case, you could, visit the websites, FTP sites or IRC channels used to gather more information or even a *fresh* sample [or samples, scripts, etc.] of what you are fighting.**
  - This will help in your remediation, as well as allowing you to supply your anti-malware vendor with something to analyse, which in turn could end up making remediation [or at least detection] easier.

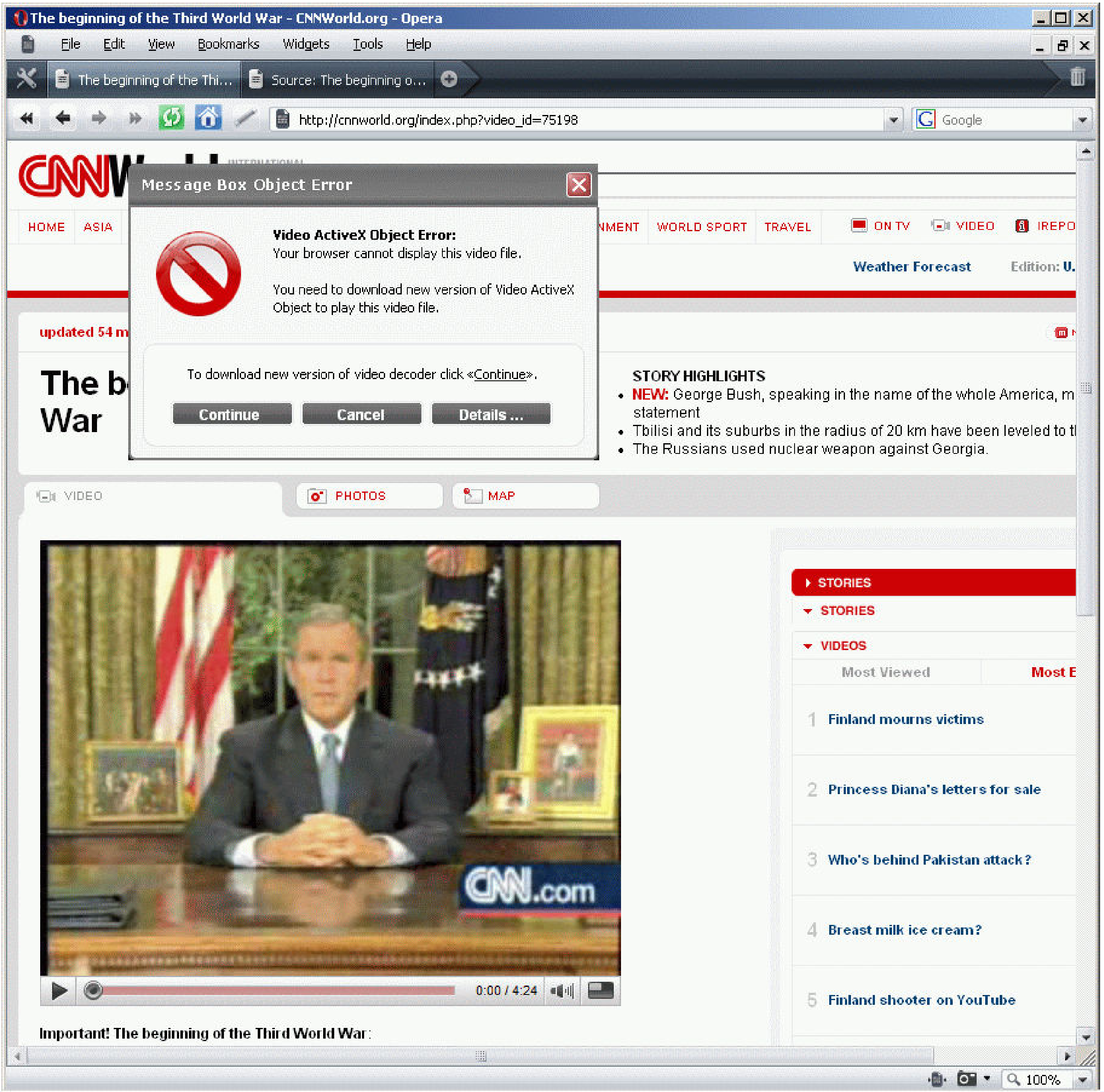
IRC Channels – as used by Bots



```
<sigh`> hm
*** XS-[90512] (MissDana@irc.           .com-22674.arcom.co
m.au) quit [04:00] Ping timeout
*** XS-[47612] (kaivin@irc.           com-23761.ipt.aol.com)
join [04:03]
*** XS-[20929] (bethany@irc.           .com-36513.mgm.bellsou
th.net) quit [04:03] Ping timeout
*** XS-[5751] (~moswen@irc.           .com-21927.dnvr.uswest
.net) join [04:03]
<Electron> !login MS,0*GN6<]07TT^+HX>#?\_+QY./BT^+HM+.R
  X>#?Y^;ER<C']07TT^+H\_+QMGN6<Y./BT^+HM[:UI:2CKJVLKJ
  VLL;"0T.*QS,0*GN6<]07TT^+H_/0ZX>#?MX>#?M+.RP+^^4V"
  P;2SLI7.D_#0[DC3XNCV]?3#PL';VMG+T-'DX^+;VMG,=R\KM[.M!
  ?N3CXI[EG,/"P?/R\?;U]+2SLN'@WT4`
<X1-[13460]> Electron You are now authorized to use me...
<Electron> !udppacket 15000 66.68.188.47 random
<X1-[13460]> Sending ( 15000 ) packets to ( 66.68.188.47 ) on
  port: ( 1565 )
<sigh`> !!!!
*** XS-[4576] (~eandreax@irc.           .com-57885.cambr1.on.
wave.home.com) quit [04:05] Connection reset by peer
```

```
@BotMonitor
+Cable
+sigh`
+X1-[13460]
sigh````
X1-[15619]
X1-[24381]
X1-[33094]
X1-[3348]
X1-[33496]
X1-[35085]
X1-[38861]
X1-[46370]
X1-[57848]
X1-[60205]
X1-[61968]
X1-[69823]
X1-[70586]
X1-[73428]
X1-[76877]
X1-[80118]
X1-[83854]
X1-[90429]
```

```
#
<Elect
<Elect
<BotMo
  This
<Elect
<Elect
<Elect
<Elect
  V]K9
<Elect
<Elect
<Elect
<Elect
<Elect
<Elect
<Elect
<BotMo
  This
```



The beginning of the Third World War - CNNWorld.org - Opera

http://cnnworld.org/index.php?video_id=75198

Message Box Object Error

Video ActiveX Object Error:
Your browser cannot display this video file.

You need to download new version of Video ActiveX Object to play this video file.

To download new version of video decoder click «Continue».

Continue | Cancel | Details ...

updated 54 m

The b
War

STORY HIGHLIGHTS

- NEW: George Bush, speaking in the name of the whole America, m statement
- Tbilisi and its suburbs in the radius of 20 km have been leveled to t
- The Russians used nuclear weapon against Georgia.

1 Finland mourns victims

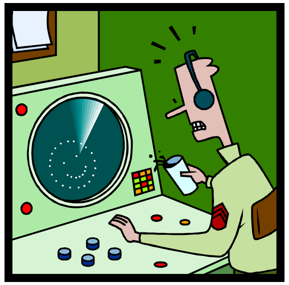
2 Princess Diana's letters for sale

3 Who's behind Pakistan attack?

4 Breast milk ice cream?

5 Finland shooter on YouTube

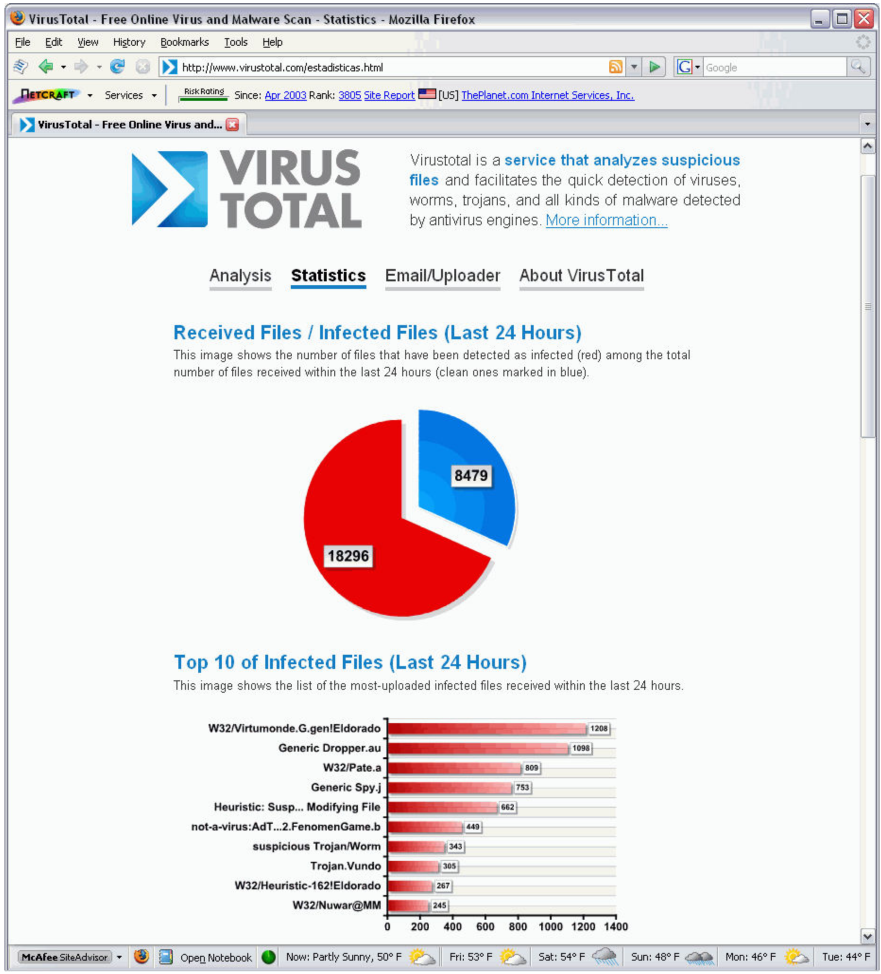
Important! The beginning of the Third World War:



Step 3a: Scan The System

- Scan with up-to-date anti-malware tools and see if anything is identified, ensure that heuristics and generic detection features are enabled. Preferably you should use at least two different products from each category, after all the anti-malware solution you have deployed didn't detect it, did it?
- Try clean-booting if performing a *live* system scan fails [or if a Windows system try booting into *Safe Mode* first] to find anything. Clean booting will ensure that any active malware or related processes are not active.
- Any files identified as malcode or flagged as suspicious should be copied to a USB flash drive or other removable media and labelled as potential malcode.
- As with *Step 2*, if you now have some suspected files, send them to your anti-malware vendor for analysis, however, this does not stop you analysing the files yourself.
- Place suspect files into a password protected zip file [use the password of *infected*] and send them to your preferred anti-malware company.
- You could also send any samples to scanning services, such as VirusTotal and Jotti, and also to sandboxes such as the one run by Norman, or the CWSandbox [also available via Sunbelt].
- Some of these services will analyse the files in great depth and supply you with copious amounts of useful data. This can help you to understand what the files are doing, and therefore how to remediate any affected systems, even before your anti-malware vendor has detection.

Online Scanners


VirusTotal - Free Online Virus and Malware Scan - Statistics - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/estadisticas.html
Services
Since: Apr 2003 Rank: 3805 Site Report [US] ThePlanet.com Internet Services, Inc.
VirusTotal - Free Online Virus and...
VIRUS TOTAL
Analysis
Statistics
Email/Uploader
About VirusTotal
8479
18296
W32/Virtumonde.G.gen!Eldorado 1208
Generic Dropper.au 1098
W32/Pate.a 809
Generic Spy.j 753
Heuristic: Susp... Modifying File 662
not-a-virus:AdT...2.FenomenGame.b 449
suspicious Trojan/Worm 343
Trojan.Vundo 305
W32/Heuristic-162!Eldorado 267
W32/Nuwar@MM 245
0 200 400 600 800 1000 1200 1400
Open Notebook
Now: Partly Sunny, 50° F
Fri: 53° F
Sat: 54° F
Sun: 48° F
Mon: 46° F
Tue: 44° F

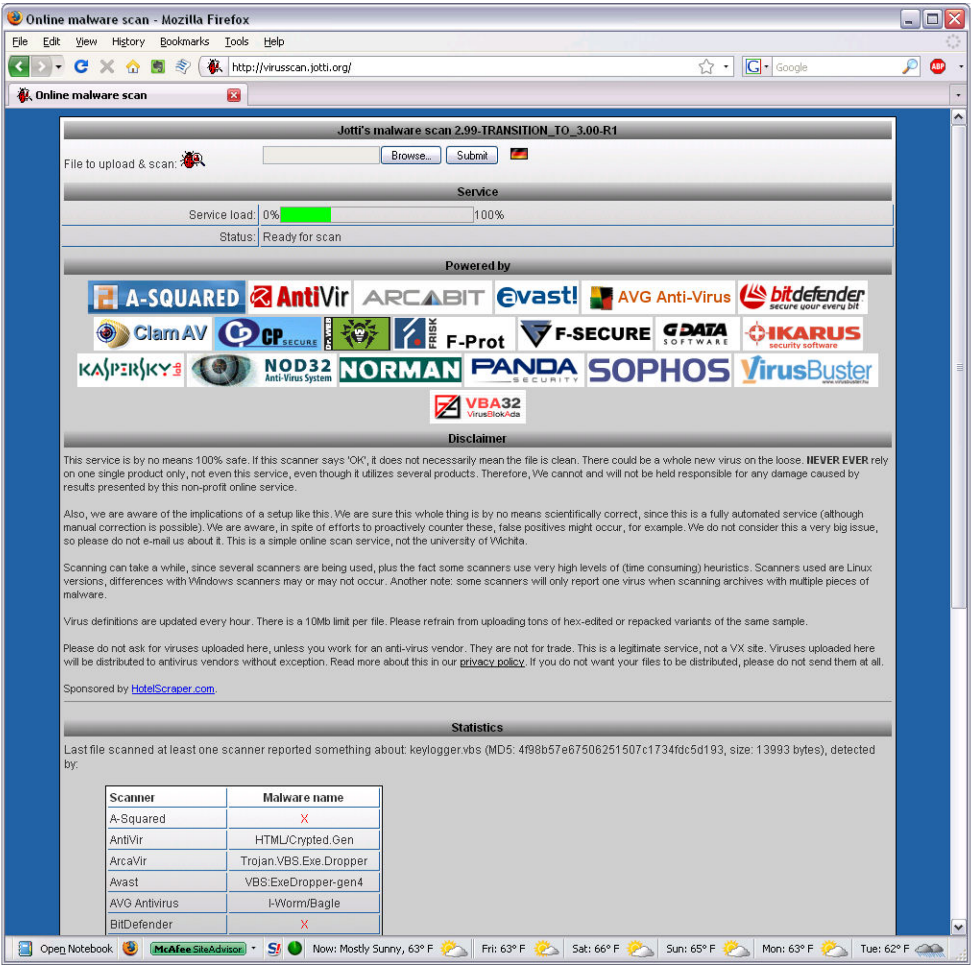
Virustotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

Received Files / Infected Files (Last 24 Hours)

This image shows the number of files that have been detected as infected (red) among the total number of files received within the last 24 hours (clean ones marked in blue).

Top 10 of Infected Files (Last 24 Hours)

This image shows the list of the most-uploaded infected files received within the last 24 hours.



Jotti's malware scan 2.99-TRANSITION_TO_3.00-R1

File to upload & scan:

Service

Service load: 0% 100%

Status: Ready for scan

Disclaimer

This service is by no means 100% safe. If this scanner says 'OK', it does not necessarily mean the file is clean. There could be a whole new virus on the loose. **NEVER EVER** rely on one single product only, not even this service, even though it utilizes several products. Therefore, We cannot and will not be held responsible for any damage caused by results presented by this non-profit online service.

Also, we are aware of the implications of a setup like this. We are sure this whole thing is by no means scientifically correct, since this is a fully automated service (although manual correction is possible). We are aware, in spite of efforts to proactively counter these, false positives might occur, for example. We do not consider this a very big issue, so please do not e-mail us about it. This is a simple online scan service, not the university of Wichita.

Scanning can take a while, since several scanners are being used, plus the fact some scanners use very high levels of (time consuming) heuristics. Scanners used are Linux versions, differences with Windows scanners may or may not occur. Another note: some scanners will only report one virus when scanning archives with multiple pieces of malware.

Virus definitions are updated every hour. There is a 10Mb limit per file. Please refrain from uploading tons of hex-edited or repacked variants of the same sample.

Please do not ask for viruses uploaded here, unless you work for an anti-virus vendor. They are not for trade. This is a legitimate service, not a VX site. Viruses uploaded here will be distributed to antivirus vendors without exception. Read more about this in our privacy policy. If you do not want your files to be distributed, please do not send them at all.

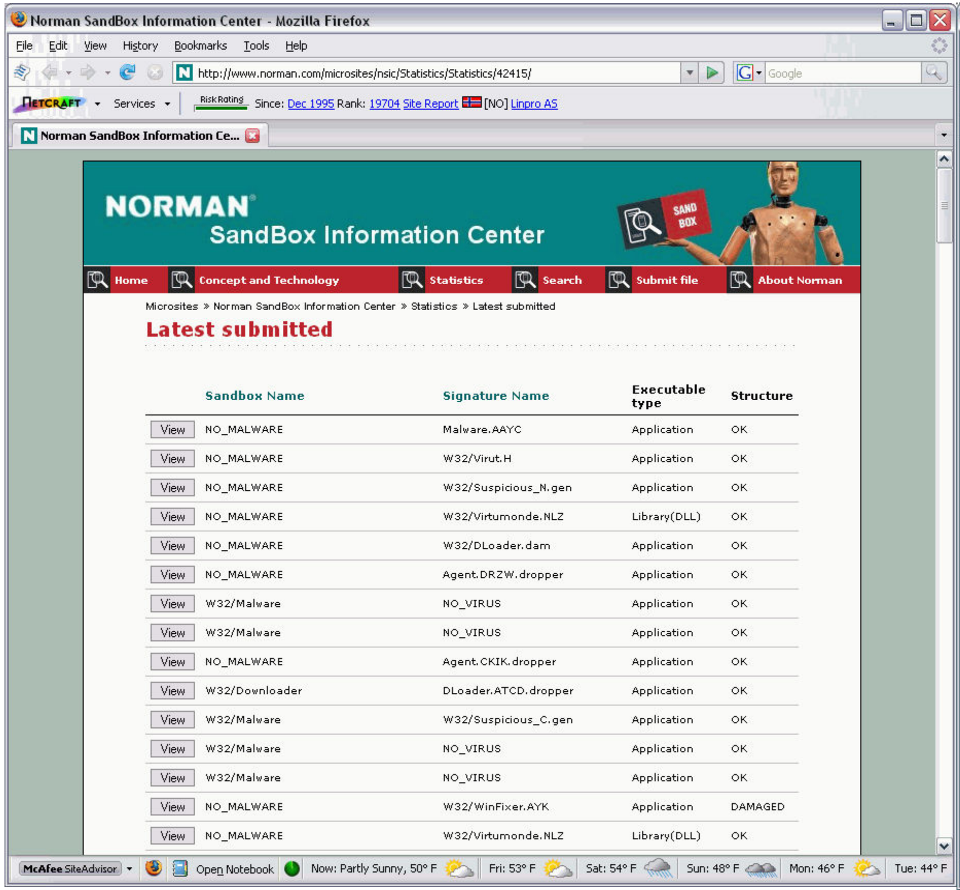
Sponsored by HotelScraper.com.

Statistics

Last file scanned at least one scanner reported something about: keylogger.vbs (MD5: 4f98b57e67506251507c1734fdc5d193, size: 13993 bytes), detected by:

Scanner	Malware name
A-Squared	X
AntiVir	HTML/Crypted.Gen
ArcaVir	Trojan.VBS.Exe.Dropper
Avast	VBS:ExeDropper-gen4
AVG Antivirus	I-Worm/Bagle
BitDefender	X

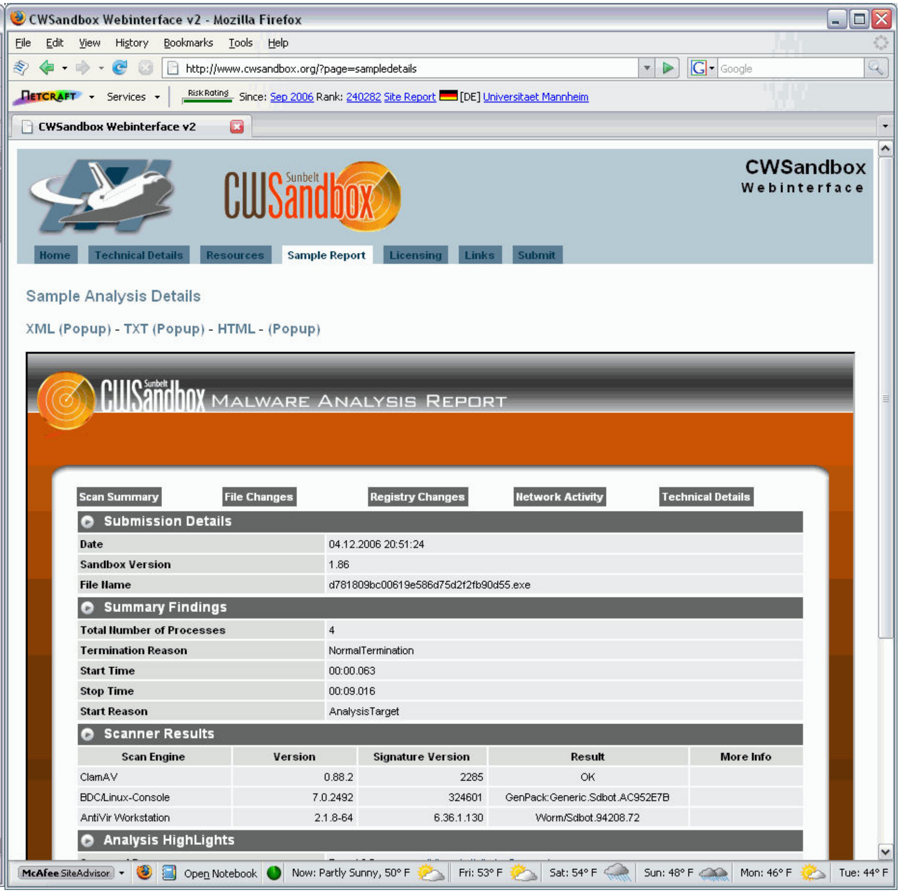
Sandboxes


Norman SandBox Information Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.norman.com/microsites/nsic/Statistics/Statistics/42415/
Services
Since: Dec 1995 Rank: 19704 Site Report [NO] Linpro AS
Norman SandBox Information Ce...
NORMAN
SandBox Information Center
Home
Concept and Technology
Statistics
Search
Submit file
About Norman
Open Notebook
Now: Partly Sunny, 50° F
Fri: 53° F
Sat: 54° F
Sun: 48° F
Mon: 46° F
Tue: 44° F

Microsites » Norman SandBox Information Center » Statistics » Latest submitted

Latest submitted

	Sandbox Name	Signature Name	Executable type	Structure
View	NO_MALWARE	Malware.AAYC	Application	OK
View	NO_MALWARE	W32/Virut.H	Application	OK
View	NO_MALWARE	W32/Suspicious_N.gen	Application	OK
View	NO_MALWARE	W32/Virtumonde.NLZ	Library(DLL)	OK
View	NO_MALWARE	W32/DLoader.dam	Application	OK
View	NO_MALWARE	Agent.DRZW.dropper	Application	OK
View	W32/Malware	NO_VIRUS	Application	OK
View	W32/Malware	NO_VIRUS	Application	OK
View	NO_MALWARE	Agent.CKIK.dropper	Application	OK
View	W32/Downloader	DLoader.ATCD.dropper	Application	OK
View	W32/Malware	W32/Suspicious_C.gen	Application	OK
View	W32/Malware	NO_VIRUS	Application	OK
View	W32/Malware	NO_VIRUS	Application	OK
View	NO_MALWARE	W32/WinFixer.AYK	Application	DAMAGED
View	NO_MALWARE	W32/Virtumonde.NLZ	Library(DLL)	OK


CWSandbox Webinterface v2 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.cwsandbox.org/?page=sampledetails
Services
Since: Sep 2006 Rank: 240282 Site Report [DE] Universitaet Mannheim
CWSandbox Webinterface v2
CWSandbox
Webinterface
Home
Technical Details
Resources
Sample Report
Licensing
Links
Submit
CWSandbox MALWARE ANALYSIS REPORT
Scan Summary
File Changes
Registry Changes
Network Activity
Technical Details
Open Notebook
Now: Partly Sunny, 50° F
Fri: 53° F
Sat: 54° F
Sun: 48° F
Mon: 46° F
Tue: 44° F

Sample Analysis Details

XML (Popup) - TXT (Popup) - HTML - (Popup)

Submission Details

Date	04.12.2006 20:51:24
Sandbox Version	1.86
File Name	d781809bc00619e586d75d2f2fb90d55.exe

Summary Findings

Total Number of Processes	4
Termination Reason	NormalTermination
Start Time	00:00.063
Stop Time	00:09.016
Start Reason	AnalysisTarget

Scanner Results

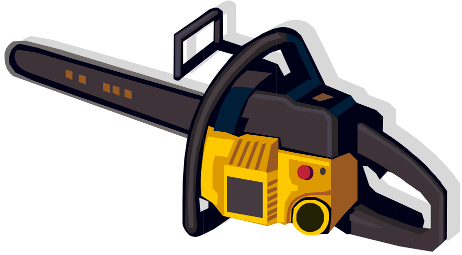
Scan Engine	Version	Signature Version	Result	More Info
ClamAV	0.88.2	2285	OK	
BDC/Linux-Console	7.0.2492	324601	GenPack:Generic.Sdbot.AC952E7B	
AntiVir Workstation	2.1.8-64	6.36.1.130	Worm/Sdbot.94208.72	

Analysis HighLights

Sample CWSandbox Output – Real Malware

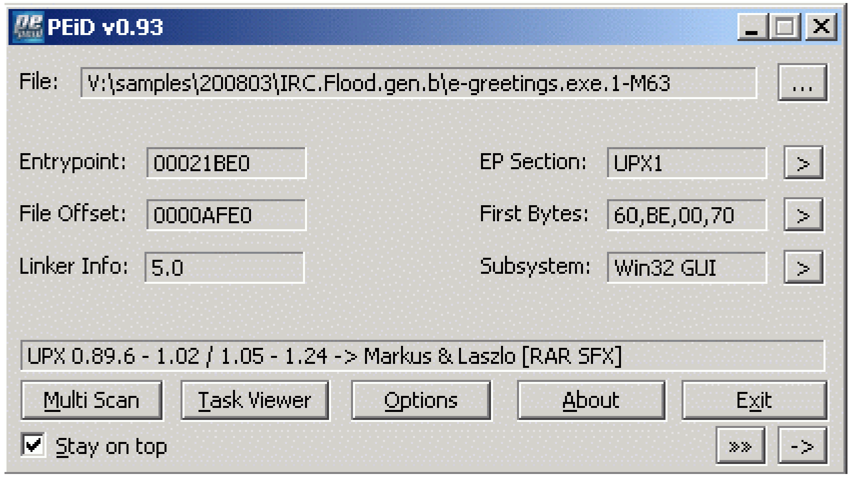
```
Filesystem
New Files
C:\WINDOWS\System32\crsss.exe
Opened Files
\SystemRoot\AppPatch\sysmain.sdb
\SystemRoot\AppPatch\systest.sdb
\Device\NamedPipe\ShimViewer
C:\WINDOWS\System32\crsss.exe
Chronological order
Copy File: c:\temp\ff37e574c7694879ff73777886a82dee.exe to C:\WINDOWS\System32\crsss.exe
Open File: \SystemRoot\AppPatch\sysmain.sdb (OPEN_EXISTING)
Open File: \SystemRoot\AppPatch\systest.sdb (OPEN_EXISTING)
Open File: \Device\NamedPipe\ShimViewer (OPEN_EXISTING)
Open File: C:\WINDOWS\System32\crsss.exe ()
Find File: crsss.exe
Registry
Process Management              Creates Process - Filename () CommandLine: (C:\WINDOWS\System32\crsss.exe --install
    c:\temp\ff37e574c7694879ff73777886a82dee.exe) As User: () Creation Flags: (DETACHED_PROCESS)
Kill Process - Filename () CommandLine: () Target PID: (588) As User: () Creation Flags: ()
System Info        Get System Directory
The following process was started by process: 1
Analysis Number    2
Parent ID          1
Process ID         1020
Filename           C:\WINDOWS\System32\crsss.exe --install c:\temp\ff37e574c7694879ff73777886a82dee.exe
Filesize           215040 bytes
MD5                ff37e574c7694879ff73777886a82dee
Start Reason       CreateProcess
Termination Reason              NormalTermination
Start Time         00:03.750
Stop Time          01:00.531
```

Step 3b: D-I-Y Sample Analysis



- Assuming you have the relevant skills and tools and have been given permission from your security manager/director to do so, you could analyse the files yourself.
- I would recommend that this is done on a system that is not connected to the network, and ideally this is a system that you will either use VMWare [or some other Virtual Machine software] on, so that it can be re-imaged, or reset back to a clean image [snapshot] after running the suspected files on the test system.
- Once this has been setup, you can use whatever tools you prefer to carry out the analysis, such as, using static analysis tools, like PEiD, Strings, File Alyzer and so on, you could also examine the file in a hex editor and/or a debugger. This is only advised if you are able to understand assembler code and you are sure that the file to be debugged does not contain and anti-debugging code which may be triggered during examination.
- You could then move onto running the file and seeing what it does using tools such as InCtrl5, Windiff, PSTools or you may prefer to disassemble it using tools such as IDAPro, WinDbg or OllDbg. This is only advised if you are able to understand assembler code and you are sure that the file to be debugged does not contain and anti-debugging code which may be triggered during examination.
- This is also a good time to try out any remediation scripts or tools you have created as a quick-n-dirty solution to the problem [obviously only on a test system].

Stud_Pe, PEiD, FileAlyzer



File: V:\samples\200803\IRC.Flood.gen.b\e-greetings.exe.1-M63

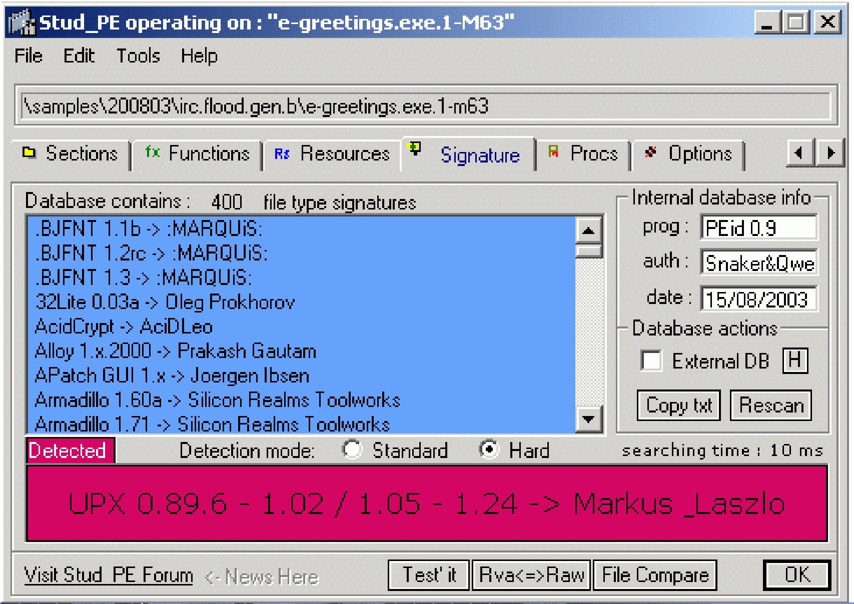
Entrypoint: 00021BE0 EP Section: UPX1

File Offset: 0000AFE0 First Bytes: 60,BE,00,70

Linker Info: 5.0 Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [RAR SFX]

☑ Stay on top



Stud_PE operating on : "e-greetings.exe.1-M63"

\samples\200803\irc.flood.gen.b\e-greetings.exe.1-m63

Database contains : 400 file type signatures

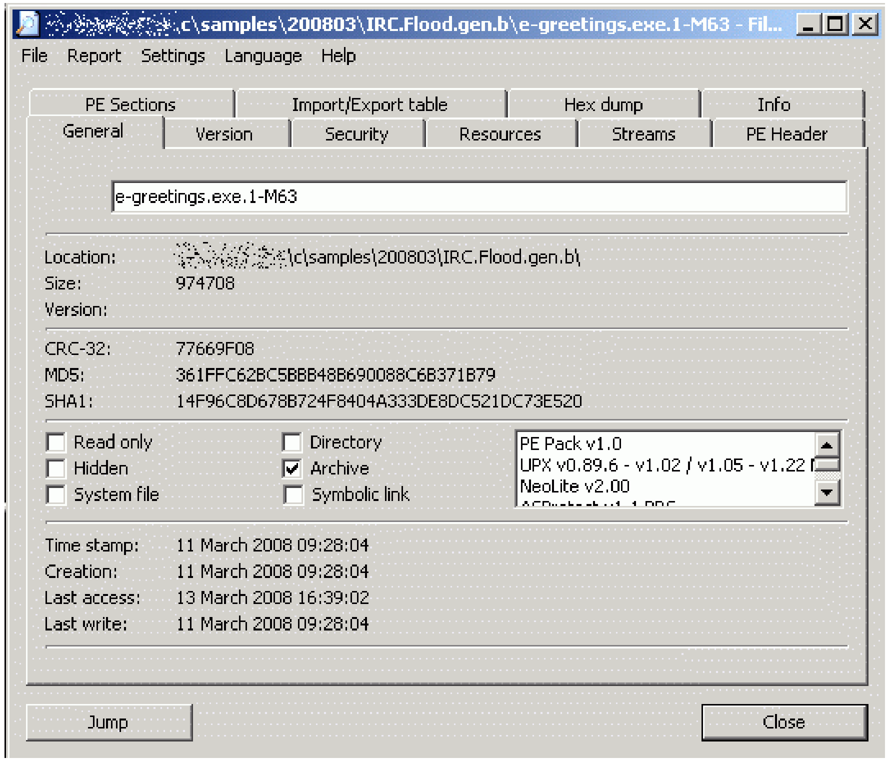
.BJFNT 1.1b -> :MARQUiS:
.BJFNT 1.2rc -> :MARQUiS:
.BJFNT 1.3 -> :MARQUiS:
32Lite 0.03a -> Oleg Prokhorov
AcidCrypt -> AciDLeo
Alloy 1.x.2000 -> Prakash Gautam
APatch GUI 1.x -> Joergen Ibsen
Armadillo 1.60a -> Silicon Realms Toolworks
Armadillo 1.71 -> Silicon Realms Toolworks

Internal database info
prog : PEid 0.9
auth : Snaker&Qwe
date : 15/08/2003

Database actions
☐ External DB H

Detected Detection mode: ○ Standard ● Hard searching time : 10 ms

UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus _Laszlo



[redacted].c\samples\200803\IRC.Flood.gen.b\e-greetings.exe.1-M63 - Fil...

e-greetings.exe.1-M63

Location: [redacted]\c\samples\200803\IRC.Flood.gen.b\
Size: 974708
Version:

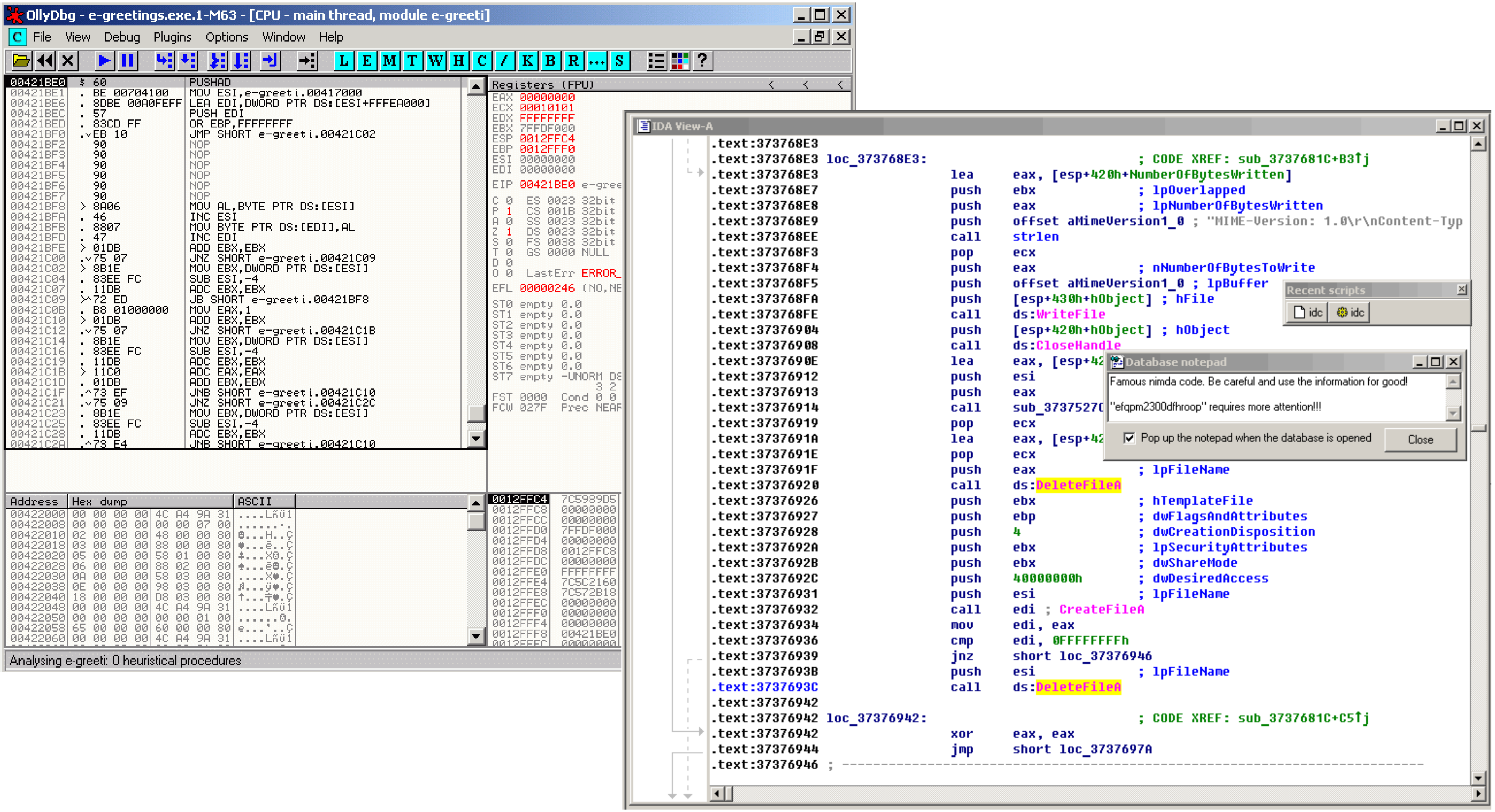
CRC-32: 77669F08
MD5: 361FFC62BC5BBB48B690088C6B371B79
SHA1: 14F96C8D678B724F8404A333DE8DC521DC73E520

☐ Read only ☐ Directory
☐ Hidden ☑ Archive
☐ System file ☐ Symbolic link

PE Pack v1.0
UPX v0.89.6 - v1.02 / v1.05 - v1.22
NeoLite v2.00

Time stamp: 11 March 2008 09:28:04
Creation: 11 March 2008 09:28:04
Last access: 13 March 2008 16:39:02
Last write: 11 March 2008 09:28:04

OllyDbg, IDAPro


OllyDbg - e-greetings.exe.1-M63 - [CPU - main thread, module e-greeti]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?
IDA View-A
Recent scripts
idc
idc
Database notepad

```
00421BE0  $ 60            PUSHAD
00421BE1  . BE 00704100   MOV ESI,e-greeti.00417000
00421BE6  . 8DBE 00A0FEFF LEA EDI,DWORD PTR DS:[ESI+FFFEA000]
00421BEC  . 57            PUSH EDI
00421BED  . 83CD FF       OR EBP,FFFFFFFF
00421BF0  .vEB 10         JMP SHORT e-greeti.00421C02
00421BF2    90            NOP
00421BF3    90            NOP
00421BF4    90            NOP
00421BF5    90            NOP
00421BF6    90            NOP
00421BF7    90            NOP
00421BF8  > 8A06          MOV AL,BYTE PTR DS:[ESI]
00421BFA  . 46            INC ESI
00421BFB  . 8807          MOV BYTE PTR DS:[EDI],AL
00421BFD  . 47            INC EDI
00421BFE  > 01DB          ADD EBX,EBX
00421C00  .v75 07         JNZ SHORT e-greeti.00421C09
00421C02  > 8B1E          MOV EBX,DWORD PTR DS:[ESI]
00421C04  . 83EE FC       SUB ESI,-4
00421C07  . 11DB          ADC EBX,EBX
00421C09  >^72 ED         JB SHORT e-greeti.00421BF8
00421C0B  . B8 01000000   MOV EAX,1
00421C10  > 01DB          ADD EBX,EBX
00421C12  .v75 07         JNZ SHORT e-greeti.00421C1B
00421C14  . 8B1E          MOV EBX,DWORD PTR DS:[ESI]
00421C16  . 83EE FC       SUB ESI,-4
00421C19  . 11DB          ADC EBX,EBX
00421C1B  > 11C0          ADC EAX,EAX
00421C1D  . 01DB          ADD EBX,EBX
00421C1F  .^73 EF         JNB SHORT e-greeti.00421C10
00421C21  .v75 09         JNZ SHORT e-greeti.00421C2C
00421C23  . 8B1E          MOV EBX,DWORD PTR DS:[ESI]
00421C25  . 83EE FC       SUB ESI,-4
00421C28  . 11DB          ADC EBX,EBX
00421C2A  .^73 E4         JNB SHORT e-greeti.00421C10
```

```
Registers (FPU)
EAX 00000000
ECX 00010101
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 00000000
EDI 00000000

EIP 00421BE0 e-gree

C 0  ES 0023 32bit
P 1  CS 001B 32bit
A 0  SS 0023 32bit
Z 1  DS 0023 32bit
S 0  FS 0038 32bit
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_

EFL 00000246 (NO,NE

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty -UNORM DE
                3 2
FST 0000  Cond 0 0
FCW 027F  Prec NEAR
```

```
Address  Hex dump                 ASCII
00422000 00 00 00 00 4C A4 9A 31 ....Lñü1
00422008 00 00 00 00 00 00 07 00 .......•.
00422010 02 00 00 00 48 00 00 80 ☻...H..Ç
00422018 03 00 00 00 88 00 00 80 ♥...ê..Ç
00422020 05 00 00 00 58 01 00 80 ♣...X☺.Ç
00422028 06 00 00 00 88 02 00 80 ♠...ê☻.Ç
00422030 0A 00 00 00 58 03 00 80 ....X♥.Ç
00422038 0E 00 00 00 98 03 00 80 ♫...ÿ♥.Ç
00422040 18 00 00 00 D8 03 00 80 ↑...╪♥.Ç
00422048 00 00 00 00 4C A4 9A 31 ....Lñü1
00422050 00 00 00 00 00 00 01 00 ......☺.
00422058 65 00 00 00 60 00 00 80 e...`..Ç
00422060 00 00 00 00 4C A4 9A 31 ....Lñü1
```

```
0012FFC4  7C5989D5
0012FFC8  00000000
0012FFCC  00000000
0012FFD0  7FFDF000
0012FFD4  00000000
0012FFD8  0012FFC8
0012FFDC  00000000
0012FFE0  FFFFFFFF
0012FFE4  7C5C2160
0012FFE8  7C572B18
0012FFEC  00000000
0012FFF0  00000000
0012FFF4  00000000
0012FFF8  00421BE0
0012FFFC  00000000
```

Analysing e-greeti: 0 heuristical procedures

```
.text:373768E3
.text:373768E3 loc_373768E3:                           ; CODE XREF: sub_3737681C+B3↑j
.text:373768E3                 lea     eax, [esp+420h+NumberOfBytesWritten]
.text:373768E7                 push    ebx             ; lpOverlapped
.text:373768E8                 push    eax             ; lpNumberOfBytesWritten
.text:373768E9                 push    offset aMimeVersion1_0 ; "MIME-Version: 1.0\r\nContent-Typ
.text:373768EE                 call    strlen
.text:373768F3                 pop     ecx
.text:373768F4                 push    eax             ; nNumberOfBytesToWrite
.text:373768F5                 push    offset aMimeVersion1_0 ; lpBuffer
.text:373768FA                 push    [esp+430h+hObject] ; hFile
.text:373768FE                 call    ds:WriteFile
.text:37376904                 push    [esp+420h+hObject] ; hObject
.text:37376908                 call    ds:CloseHandle
.text:3737690E                 lea     eax, [esp+42
.text:37376912                 push    esi
.text:37376913                 push    eax
.text:37376914                 call    sub_3737527C
.text:37376919                 pop     ecx
.text:3737691A                 lea     eax, [esp+42
.text:3737691E                 pop     ecx
.text:3737691F                 push    eax             ; lpFileName
.text:37376920                 call    ds:DeleteFileA
.text:37376926                 push    ebx             ; hTemplateFile
.text:37376927                 push    ebp             ; dwFlagsAndAttributes
.text:37376928                 push    4               ; dwCreationDisposition
.text:3737692A                 push    ebx             ; lpSecurityAttributes
.text:3737692B                 push    ebx             ; dwShareMode
.text:3737692C                 push    40000000h       ; dwDesiredAccess
.text:37376931                 push    esi             ; lpFileName
.text:37376932                 call    edi ; CreateFileA
.text:37376934                 mov     edi, eax
.text:37376936                 cmp     edi, 0FFFFFFFFh
.text:37376939                 jnz     short loc_37376946
.text:3737693B                 push    esi             ; lpFileName
.text:3737693C                 call    ds:DeleteFileA
.text:37376942
.text:37376942 loc_37376942:                           ; CODE XREF: sub_3737681C+C5↑j
.text:37376942                 xor     eax, eax
.text:37376944                 jmp     short loc_3737697A
.text:37376946 ; ---------------------------------------------------------------
```

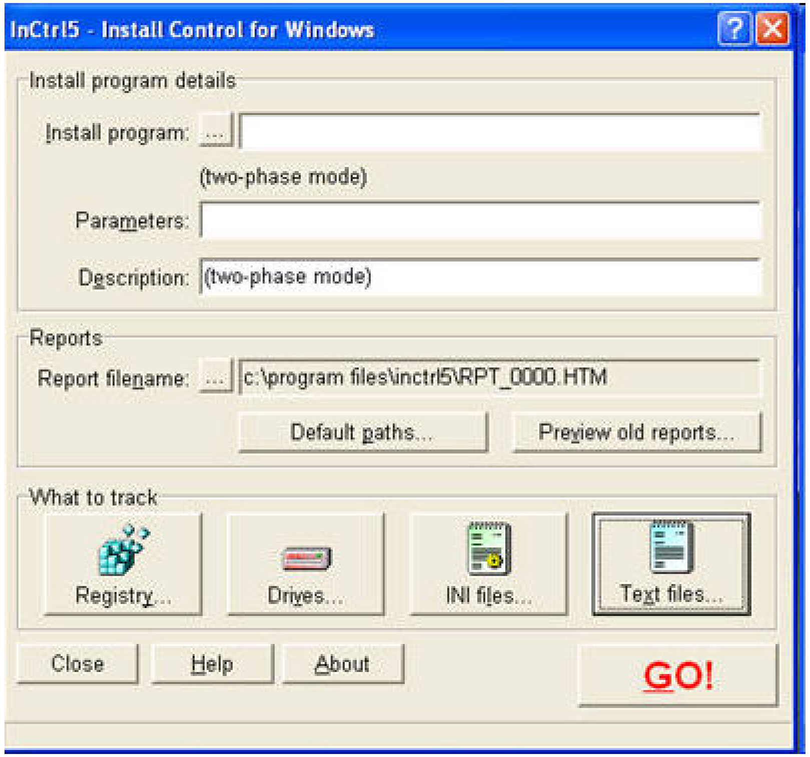
Famous nimda code. Be careful and use the information for good!

"efqpm2300dfhroop" requires more attention!!!

☑ Pop up the notepad when the database is opened

Close

VMware, etc.



InCtrl5 - Install Control for Windows

Install program details

Install program:

(two-phase mode)

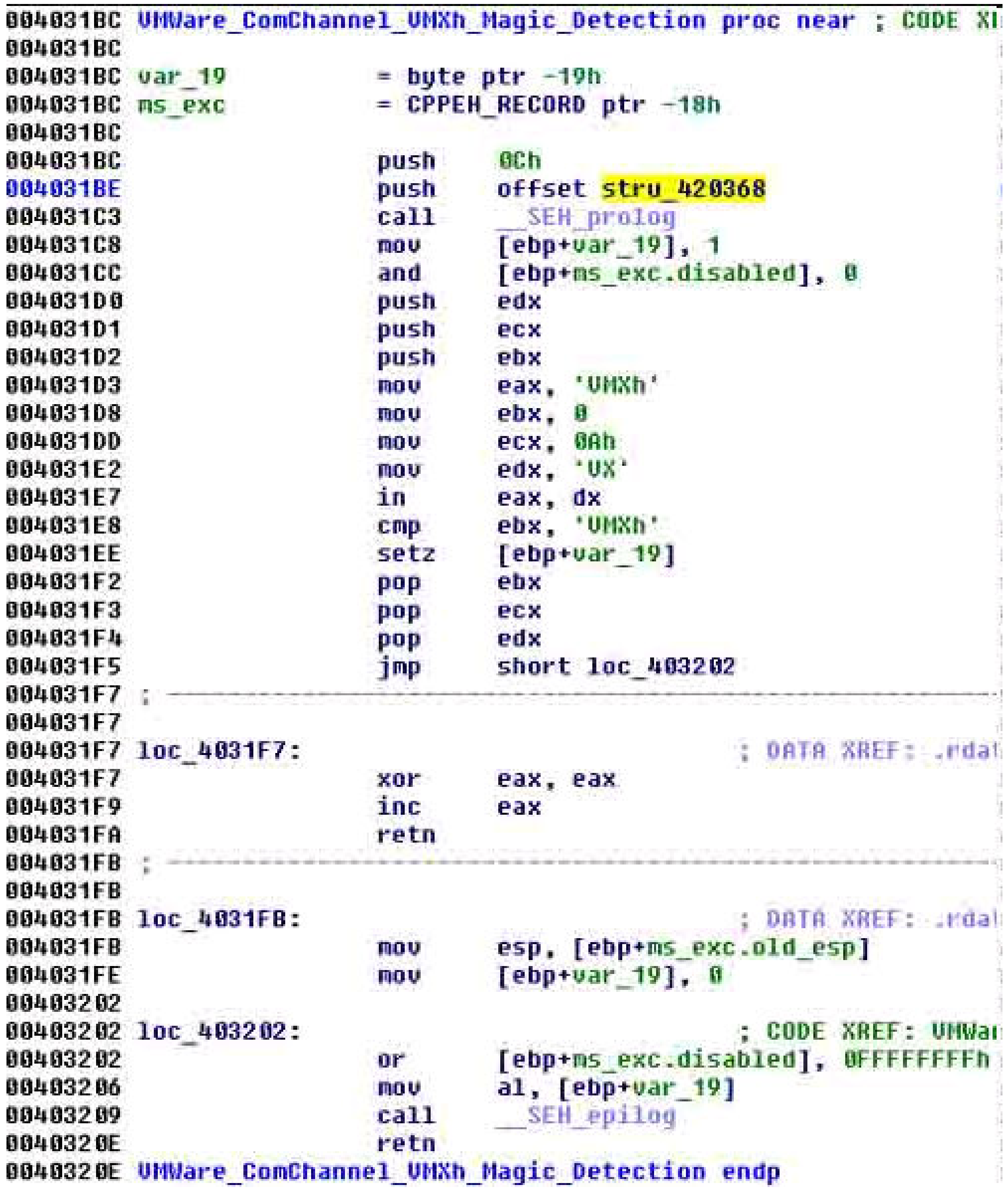
Parameters:

Description: (two-phase mode)

Reports

Report filename: c:\program files\inctrl5\RPT_0000.HTM

What to track



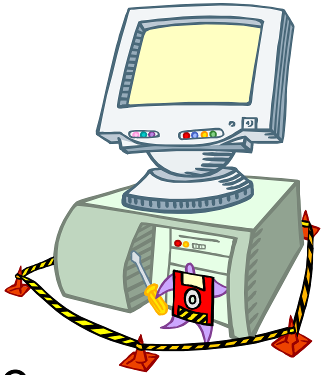
```
004031BC VMWare_ComChannel_VMXh_Magic_Detection proc near ; CODE XI
004031BC
004031BC var_19          = byte ptr -19h
004031BC ms_exc          = CPPEH_RECORD ptr -18h
004031BC
004031BC                 push    0Ch
004031BE                 push    offset stru_420368
004031C3                 call    __SEH_prolog
004031C8                 mov     [ebp+var_19], 1
004031CC                 and     [ebp+ms_exc.disabled], 0
004031D0                 push    edx
004031D1                 push    ecx
004031D2                 push    ebx
004031D3                 mov     eax, 'VMXh'
004031D8                 mov     ebx, 0
004031DD                 mov     ecx, 0Ah
004031E2                 mov     edx, 'VX'
004031E7                 in      eax, dx
004031E8                 cmp     ebx, 'VMXh'
004031EE                 setz    [ebp+var_19]
004031F2                 pop     ebx
004031F3                 pop     ecx
004031F4                 pop     edx
004031F5                 jmp     short loc_403202
004031F7 ; ---------------------------------------------------------------
004031F7
004031F7 loc_4031F7:                             ; DATA XREF: .rdat
004031F7                 xor     eax, eax
004031F9                 inc     eax
004031FA                 retn
004031FB ; ---------------------------------------------------------------
004031FB
004031FB loc_4031FB:                             ; DATA XREF: .rdat
004031FB                 mov     esp, [ebp+ms_exc.old_esp]
004031FE                 mov     [ebp+var_19], 0
00403202
00403202 loc_403202:                             ; CODE XREF: VMWar
00403202                 or      [ebp+ms_exc.disabled], 0FFFFFFFFh
00403206                 mov     al, [ebp+var_19]
00403209                 call    __SEH_epilog
0040320E                 retn
0040320E VMWare_ComChannel_VMXh_Magic_Detection endp
```

Step 4: Analyse The Data (Part 2)

- By now you should have a good idea what is going on, and what any malcode is doing to the affected systems and what network traffic is being generated by it [or them].

- If you haven't then you should now take time to go over all the data you have acquired during the first three steps. You could use a flow diagram to plot the malcode's features and activities, or you may prefer to brainstorm on a whiteboard with suitable colleagues. From here you should emerge with a clear [or fairly clear] understanding of what needs to be done to protect the rest of the network [it could be as simple as putting in a new, or changing an existing router ACL, firewall rule, or IDS/IPS signature/rule in place] which may also allow you to identify other infected systems that need to be removed from the network and remediated.

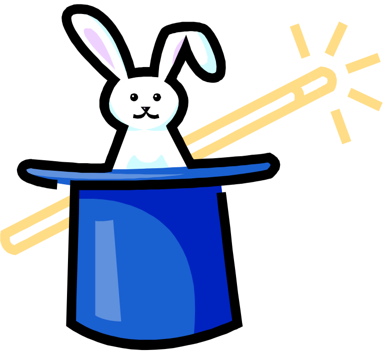
Step 5: Remediation



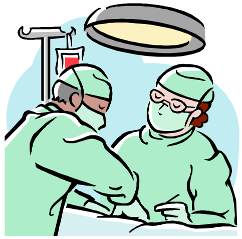
- Hopefully by now, you can either create or at least plan out the steps that you need to take to remediate all the infected systems identified. You may decide that you can create your own clean-up scripts [paper and/or code] rather than wait for your anti-malware vendors to get detection and cleanup definitions [signatures] to you. Otherwise you will have to be patient until your anti-malware vendor delivers the goods.

- The other alternative, especially if a system is heavily infected, or you can't find any sign of malcode [even when using all the tools/tricks and techniques listed in the paper], is to restore the system from the last known clean backup, or re-image it to your organisations standard desktop/server build image.

Tricks



- **VB Scripting for quick and dirty cleanup, example:**
  - 'RemSdbot2.vbs - SDbot remover for specific variant.
  - '© Martin Overton, 2007 (martin@arachnophiliac.com)
  - 'Verson 0.99.2'
  - 'Created to detect and remove an infection of the following Sdbot variant
  - '
  - 'FileName: rundll.exe
  - 'FileDateTime: 19/01/2007 14:05:00
  - 'Filesize: 1364992
  - 'MD5: 71fd1205f6d7550967bda6bf4491a50a
  - 'CRC32: 36E8176E
  - 'File Type: PE Executable
  - … [For the rest see the paper]
- **Clean Boot Disks**
  - Using live Linux or a PE boot disk, such as Bart_PE can be very handy, not only in clean booting a suspected system but also in scanning the same system with little or no risk that any malcode will still be active on it. It needs not be a CD or DVD [from an ISO image], it could also be an external USB hard disk or a USB flash drive instead.



Step 6: Post Mortem

- This is where you take stock of what has happened and decide what [if any] changes are required to improve protection of your infrastructure, your security policy and procedures and, last but not least, user education.
- The whole point of this is to help minimise the risk of another similar outbreak. The ideas that come out from this session should be wide-ranging and generic as these will generally offer the best improvements in your organisations security posture; both from the aspects of prevention and incident management.
- This is not the time for a witch-hunt to take place so that blame can be attributed to individuals and/or teams, you should focus on what went wrong [or failed] and put together solutions to minimise the chances of a similar attack being successful next time. It may also be useful to revisit your overall approach to threats and infection vectors, as they may have changed since the last time you looked.
- *A final note: If it is a criminal case then you need to follow computer forensic principals, such as the chain of custody, and follow the prevailing laws [including all guidance from law enforcement agencies that might get involved] for your country, state, or other geographical divide. Failure to do so may mean that a successful prosecution is unlikely; the case may not even get to court. If in doubt seek legal guidance first, before proceeding.*

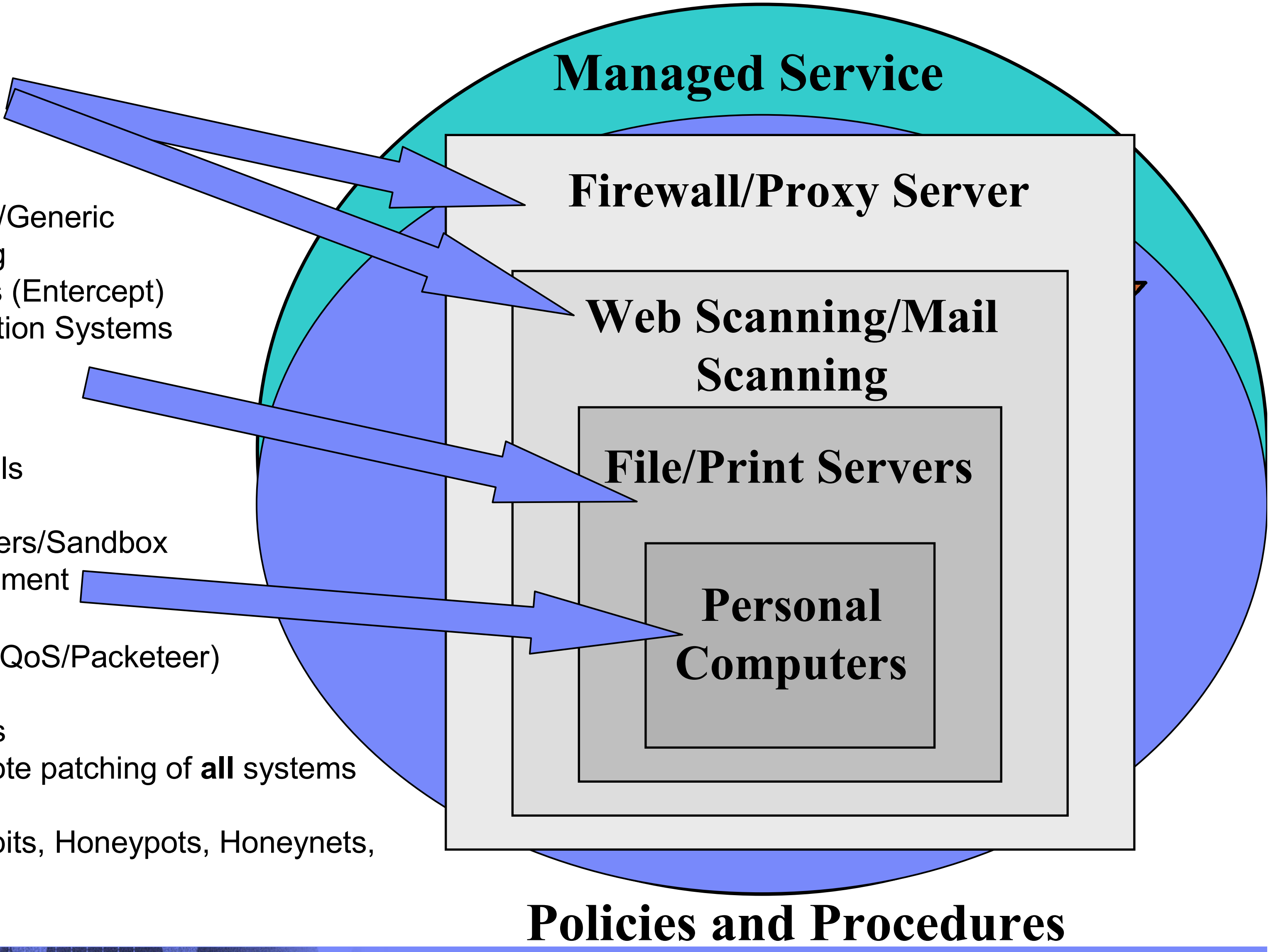
Applying a Multi-layered Anti-Malware

AV Vendor 1
IDS

AV Vendor 2
Content Filtering/Generic Blocking/Filtering
Kernel Wrappers (Entercept)
Intrusion Prevention Systems (IntruShield)

AV Vendor 3
Personal Firewalls
Personal IDS
Behaviour Blockers/Sandbox
Integrity Management

PacketShapers (QoS/Packeteer)
NetFlow (Cisco)
Layer 7 Switches
Centralised remote patching of **all** systems
Backups
SMB-Lures, Tarpits, Honeypots, Honeynets, BillyGoats



Putting it all together……

Multiple Antivirus Vendors

Workstation
Servers
Perimeter (Web, FTP and SMTP)

Malware Sensors

SMB-Lures, Tarpits, Honeypots, Honeynets, BillyGoats

IDS

Using custom malware rules/signatures

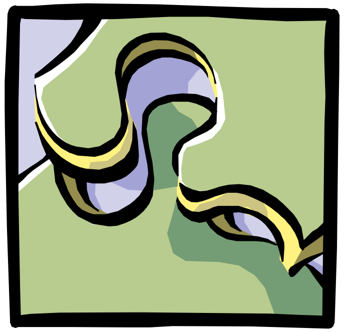
Management

Centralised, Geo-centric, or at least country-centric

Policies (What we want to achieve)
Procedures (How we are going to achieve it)
People (Who’s going to do it)
Products (The technology bit)

Automated Patching

Centralised remote patching of all systems via Tivoli, SMS, etc.



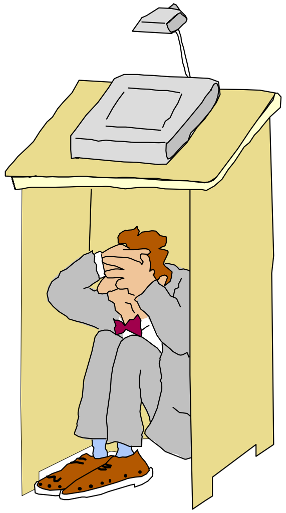
Others

Kernel Wrappers (Entercept)
Personal Firewalls (McAfee/ZoneLabs)
Personal IDS (Blackice)
Generic Blocking/Filtering
Heuristics
Backups
Intrusion Prevention Systems (IntruShield)
Behaviour Blockers/SandBox Technology (FinJan SurfinShield)
Firewalls/Proxies
PacketShapers (QoS/Packeteer)
NetFlow (Cisco)
Layer 7 Switches
Managed e-mail virus scanning, anti-spam service

Conclusions

- Hopefully I have shown you that even if you are faced with a new malware threat that isn't detected by your anti-malware defences you can still, in most cases, find the infection, how it got in, how it communicates and with the right tools and methodologies even remove it safely before your anti-malware vendor comes up with solution.
- I must make clear that this is not a solution to be used by those not already used to handling and combating malware and other related security threats; home users need not apply, however most academic campuses, large businesses and other organisations should already have at least one person [hopefully more than one] who has the required skills and experience to be able to do this. They almost certainly already work in the security team [or a related function] and have a network of colleagues outside of the main security team that they can call on; such as programmers, network specialists, server and desktop support staff.
- As with other security threat, especially malware related ones, you need to deploy a multi-layered approach to minimise the chance of malware getting onto your computers. This means not only do you need good technological solutions, and overlapping technologies at that, but these need to be backed up with good security policies, procedures, education and constant vigilance.
- Please do not see this paper as an exhaustive or complete look at detecting and combating new malware and malware forensics, to do this real justice would require enough material to fill a large book.

Questions?



Contact details…..

Martin Overton

EMEA Malware/Anti-Malware SME

IBM ISS X-Force – PSS

- **E-Mail: overtonm@uk.ibm.com**
- **Telephone: +44 (0)239 2563442**

All my published papers and articles can be downloaded from: http://momusings.co.uk/publications.aspx