Malware Forensics: Detecting The Unknown

- *"There are known knowns; there are things we know that we know. There are known unknowns; that is to say, there are things that we now know we don't know. But there are also unknown unknowns; there are things we do not know we don't know."*

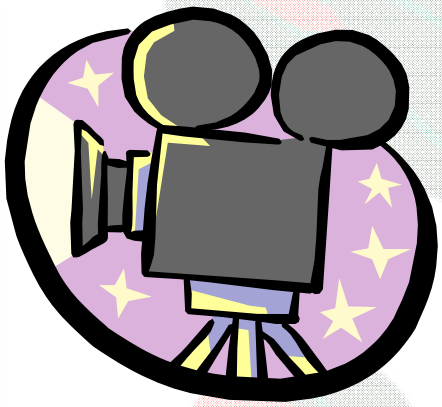
  —United States Secretary of Defense Donald Rumsfeld

Martin Overton – IBM Security Services

Malware/Anti-Malware SME, Forensics, Ethical Hacker, etc.

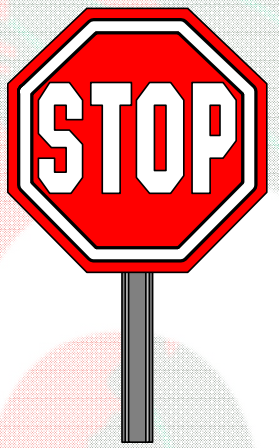
All my published papers and articles can be downloaded from: http://momusings.com/papers/

Agenda



- **Disclaimer**
- **Solutions**
  - Steps 1-6
  - Real World Examples
  - Conclusions
- **Questions**

Disclaimer

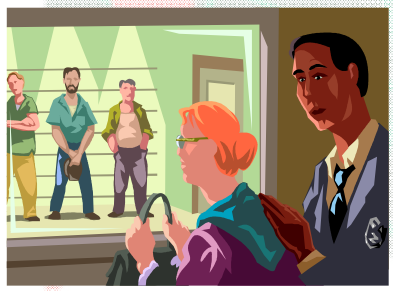


- Products named in this presentation are used as examples only, and should not be taken as any form of endorsement by IBM or ISS.

- All trademarks and copyrights are acknowledged.

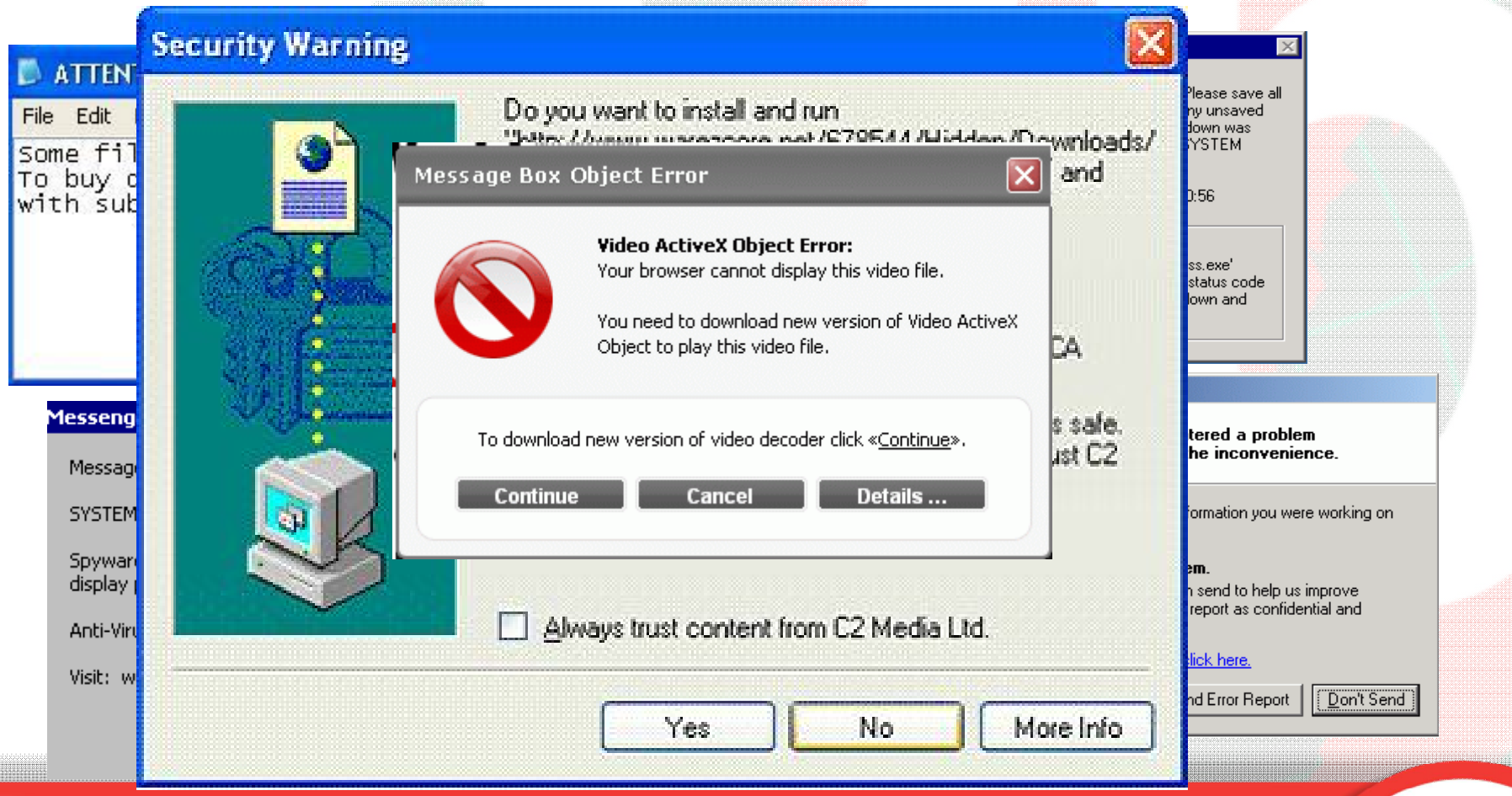
Solutions……

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].

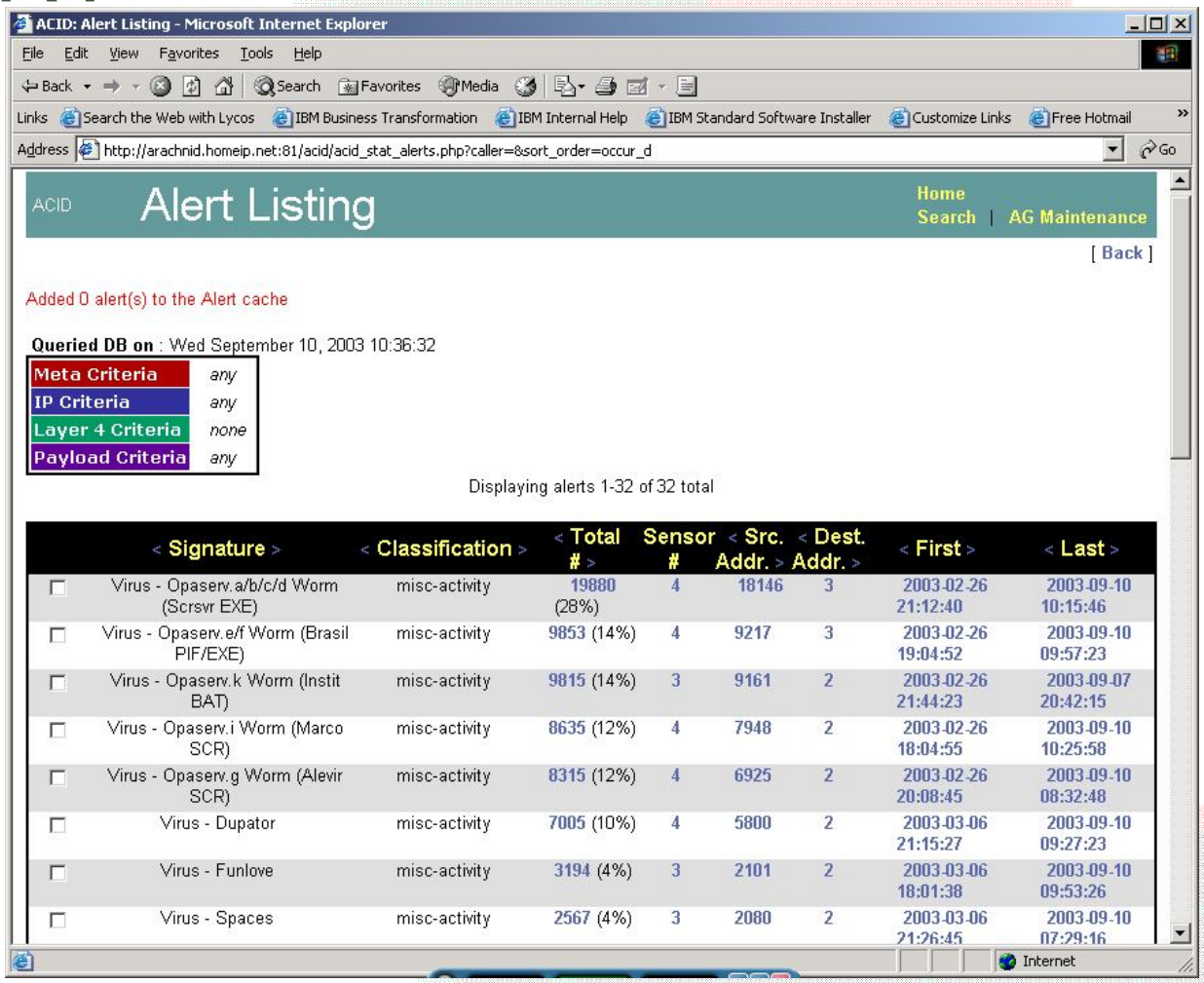
Error Messages Are Your Friends



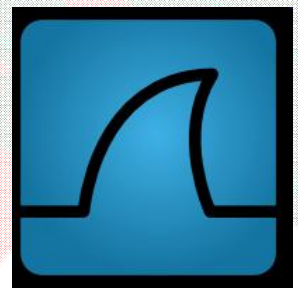
Step 1: Identifying Suspect Systems…cont.

- 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.

SNORT

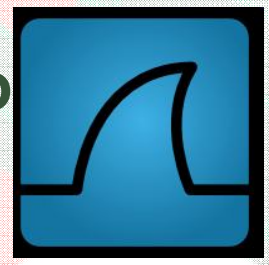

ACID: Alert Listing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links Search the Web with Lycos IBM Business Transformation IBM Internal Help IBM Standard Software Installer Customize Links Free Hotmail
Address http://arachnid.homeip.net:81/acid/acid_stat_alerts.php?caller=&sort_order=occur_d
Go
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
Internet

Wireshark - Win32/Sality.nar - DNS



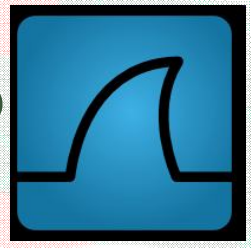
No.	Time	Source	Destination	Protocol	Info
70	234.159163	192.168.11.11	80.77.240.31	DNS	Standard query A www.kjwre9tqwieluoi.info
71	234.564516	80.77.240.31	192.168.11.11	DNS	Standard query response, No such name
72	234.820249	192.168.11.11	80.77.240.31	DNS	Standard query A kukutrustnet777.info
73	235.182315	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



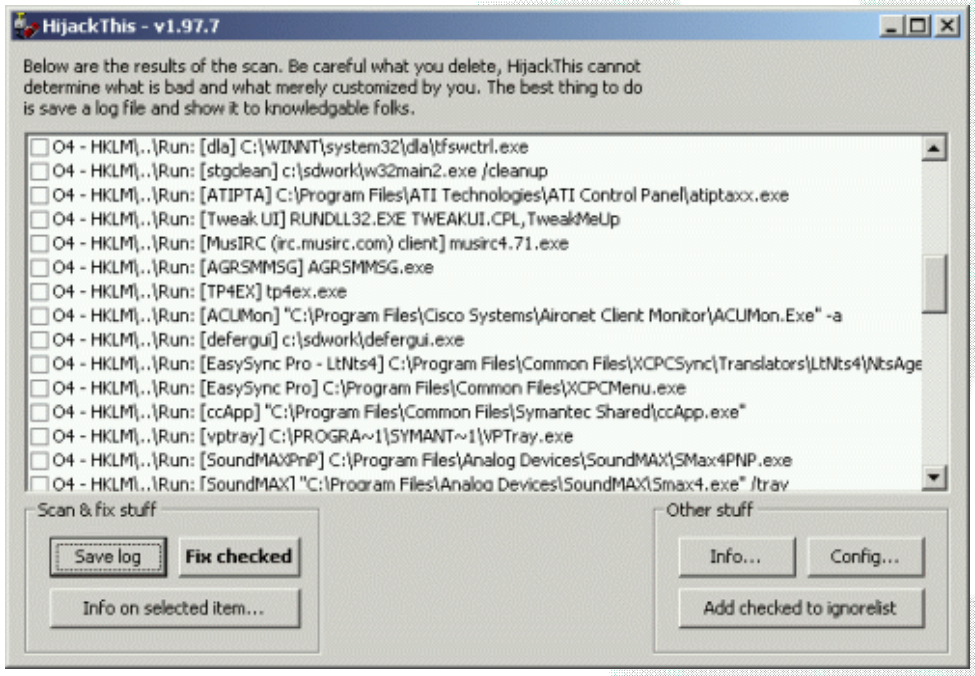
No.	Time	Source	Destination	Protocol	Info
86	257.408508	192.168.11.11	78.110.50.107	HTTP	GET /img/logoh.gif?32ae9c=23250500 HTTP/1.1
96	257.596138	78.110.50.107	192.168.11.11	HTTP	HTTP/1.0 200 OK
103	259.787076	192.168.11.11	78.110.50.107	HTTP	GET /img/logos.gif?32b90b=16620855 HTTP/1.1
113	259.972191	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

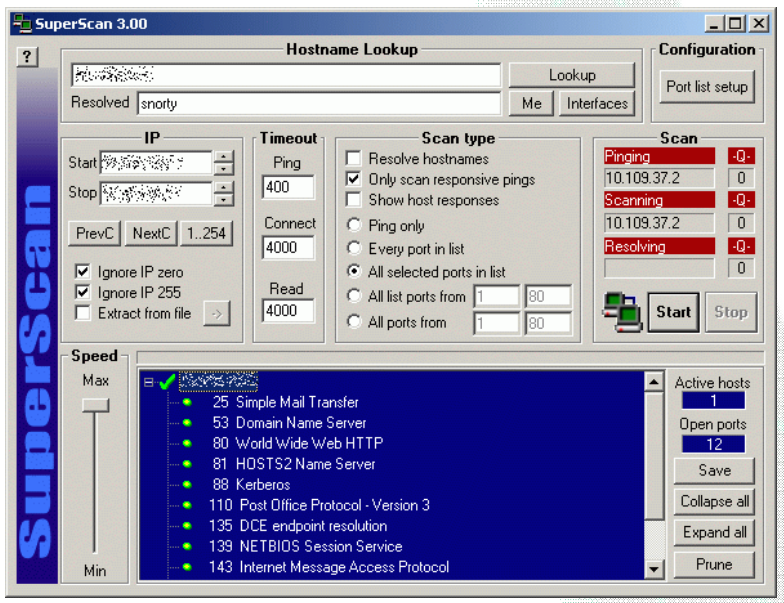


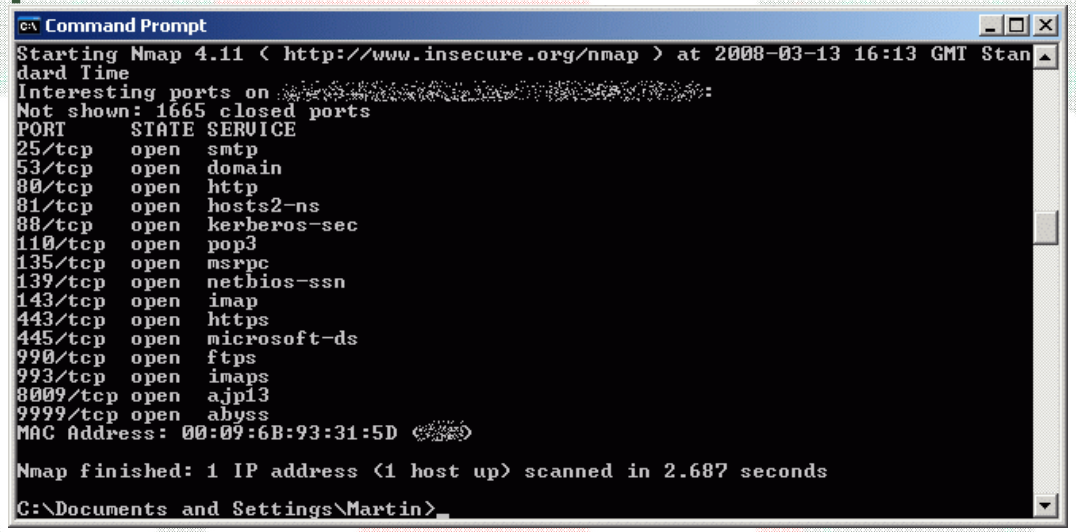
No.	Time	Source	Destination	Protocol	Info
437	266.729739	192.168.11.11	72.232.11.26	TCP	cognex-insight > http [ACK] Seq=1 Ack=1 Win=65250 Len=0
439	266.934442	72.232.11.26	192.168.11.11	TCP	http > cognex-insight [ACK] Seq=1 Ack=133 Win=6432 Len=0
441	266.934881	72.232.11.26	192.168.11.11	TCP	http > cognex-insight [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

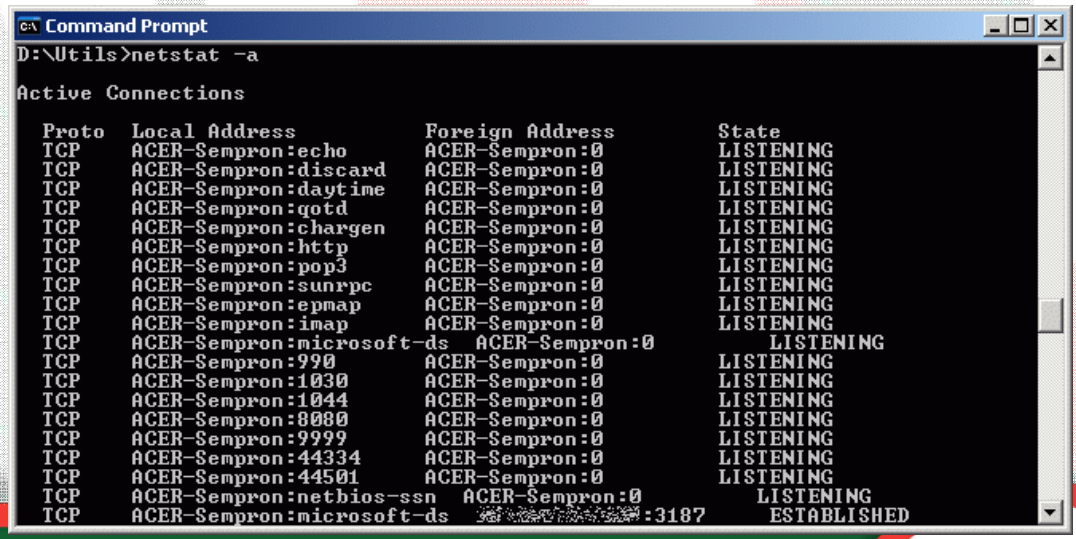
HijackThis, WinPatrol



SuperScan, Nmap, Netstat





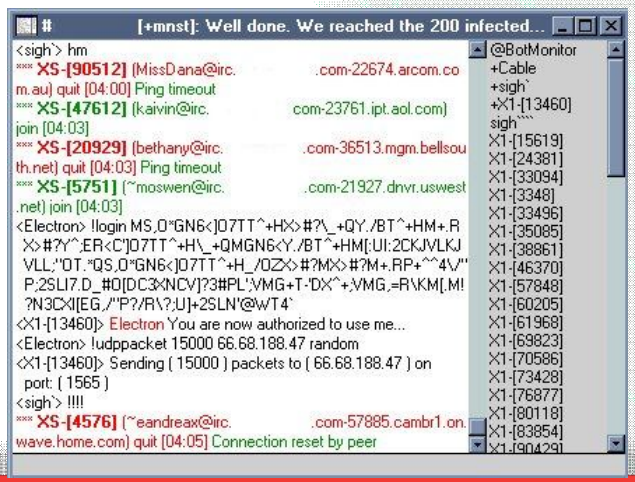


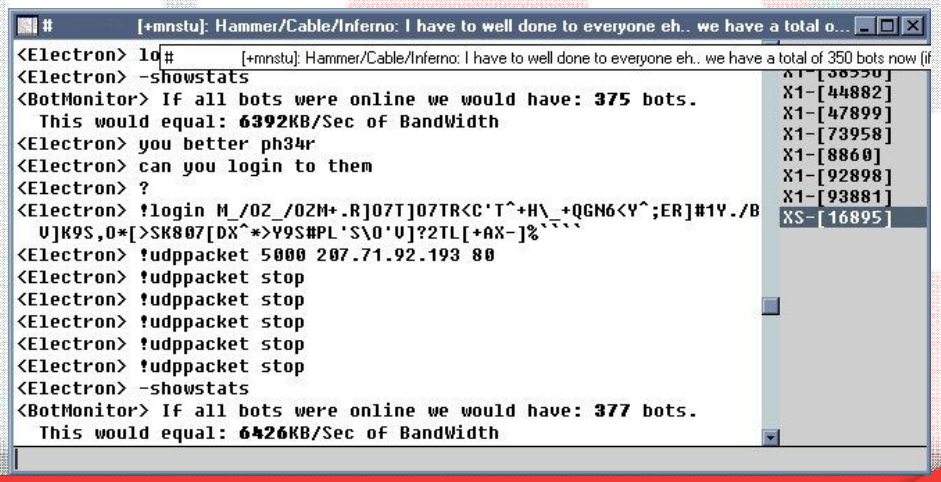
Step 2: Analyse The Data (Part 1)

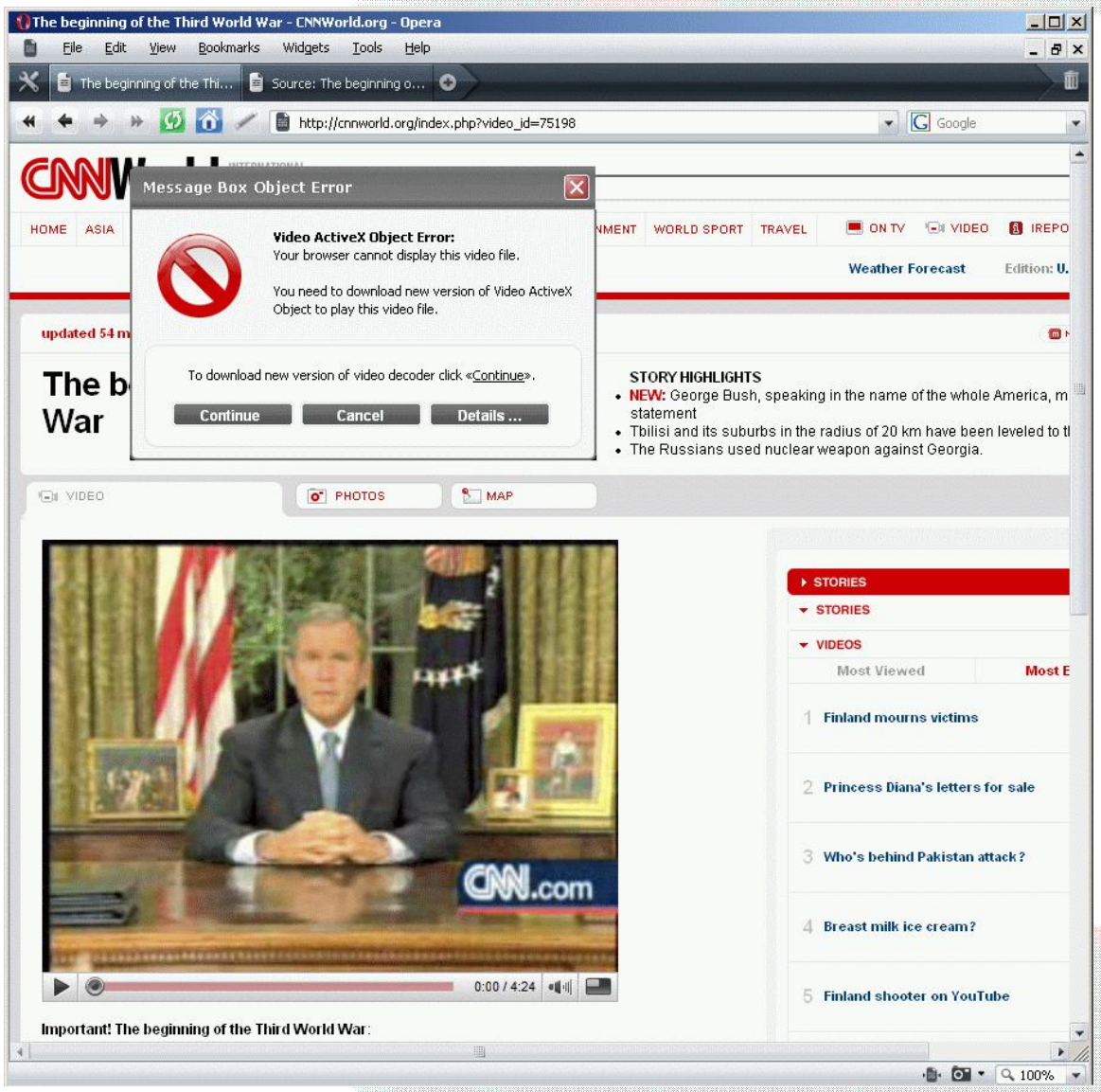
- At this point you may already be able to state with some level of confidence that the system is infected by a malcode which *phones-home.*
  - Examples of these include bot clients, or a Trojan or multi-component malcode [such as a dropper] that has contacted one or more websites to download other 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.

Step 2: Analyse The Data (Part 1)…cont.

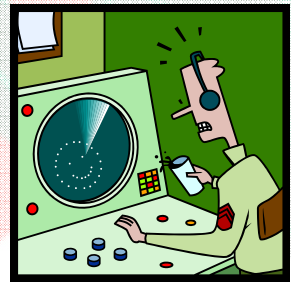
- In either case, you could, visit the websites, FTP sites or IRC channels used to gather more information or even a *fresh* sample [or samples, scripts, etc.] of what you are fighting.
  - This will help in your remediation, as well as allowing you to supply your anti-malware vendor with something to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





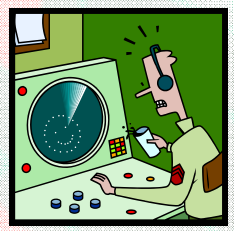


Step 3a: Scan The System



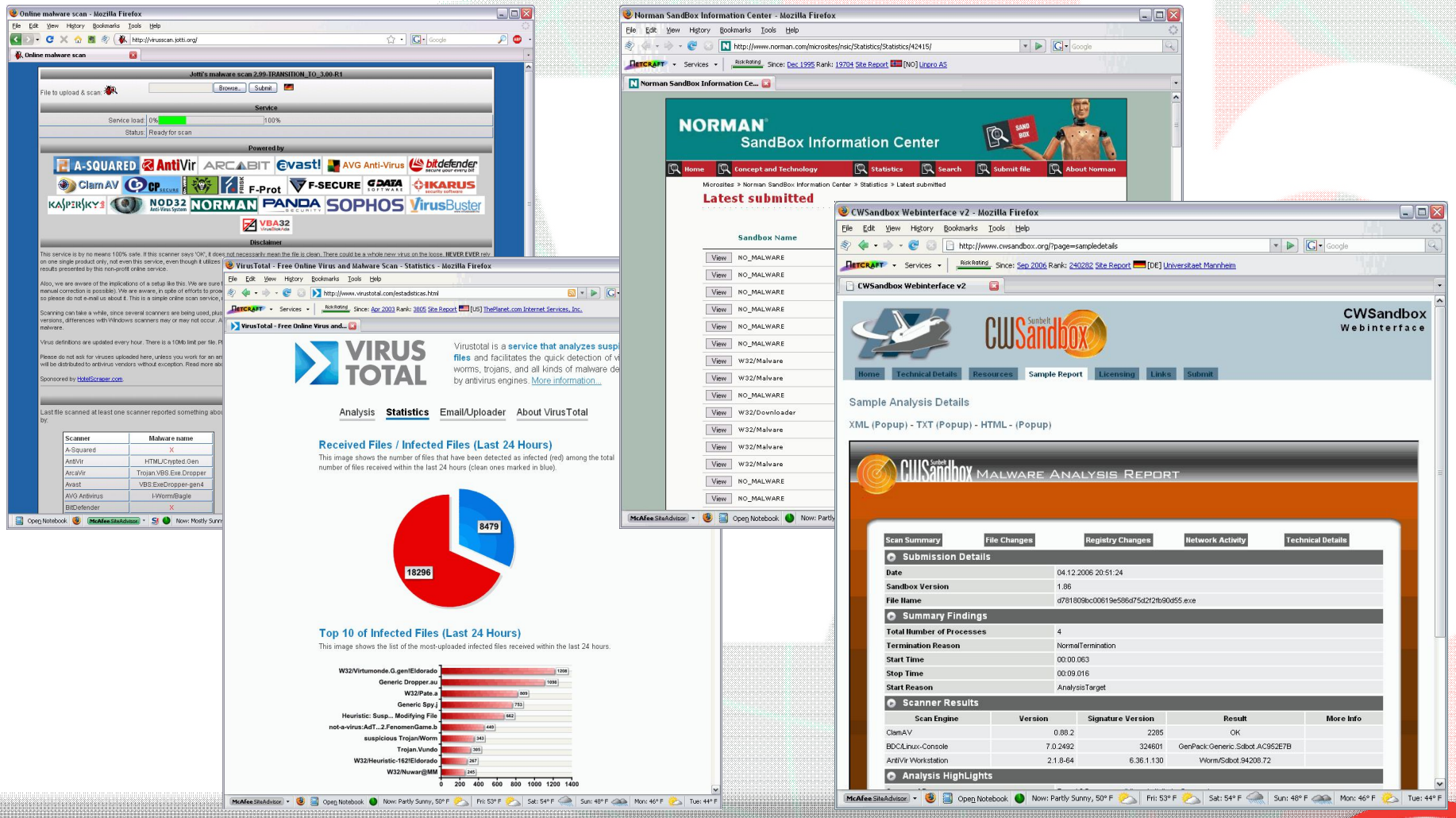
- Scan with up-to-date anti-malware tools and see if anything is identified, ensure that heuristics and generic detection features are enabled. Preferably you should use at least two different products from each category, after all the anti-malware solution you have deployed didn't detect it, did it?
- 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.

Step 3a: Scan The System…cont.

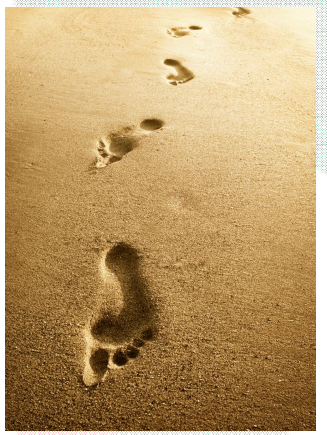


- As with *Step 2*, if you now have some suspected files, send them to your anti-malware vendor for analysis, however, this does not stop you analysing the files yourself.
- Place suspect files into a password protected zip file [use the password of *infected*] and send them to your preferred anti-malware 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.
- 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 & Sandboxes

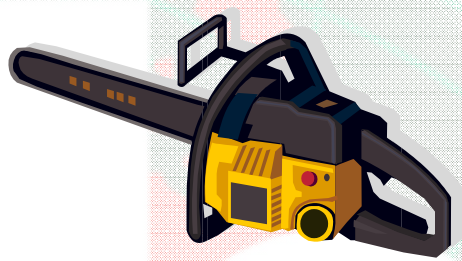


Sample CWSandbox Output – Real Malware



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

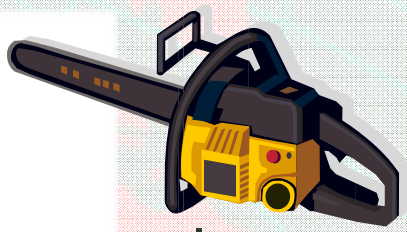
Step 3b: D-I-Y Sample Analysis



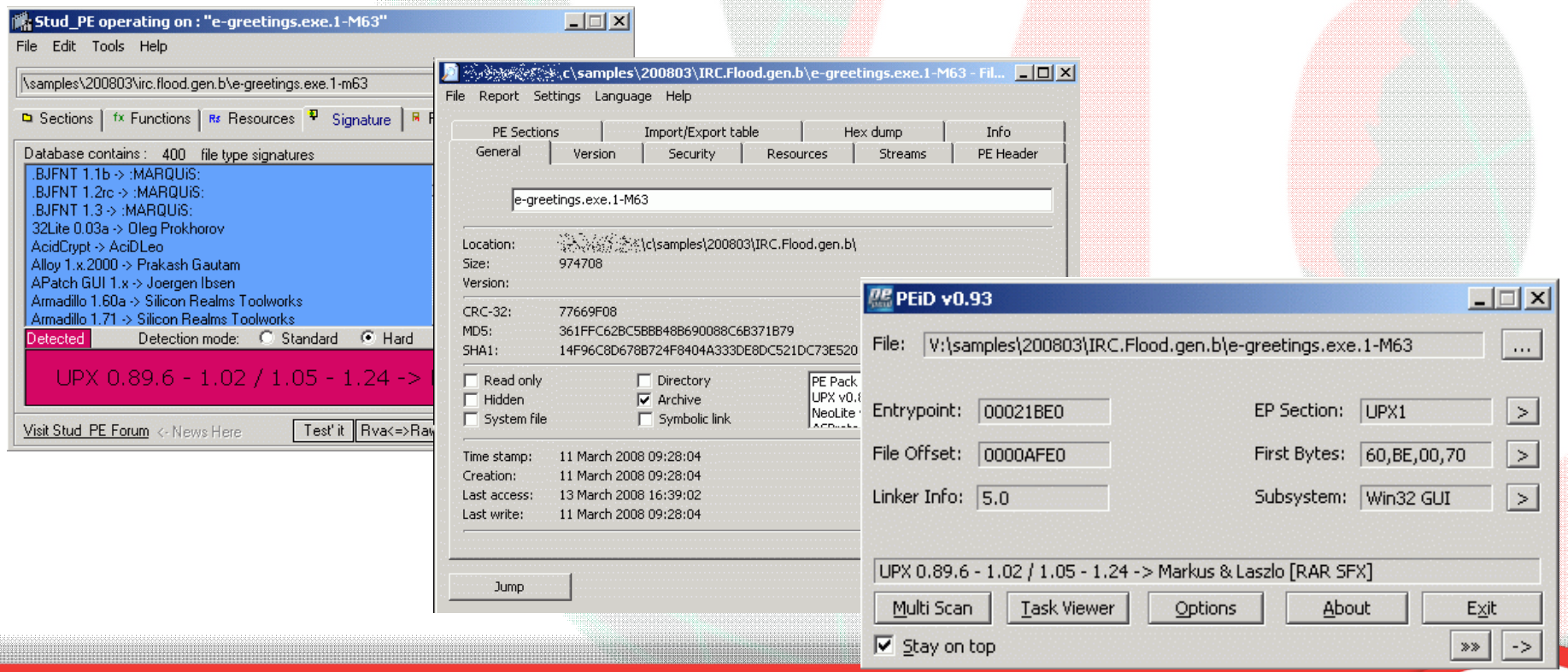
- Assuming you have the relevant skills and tools and have been given permission from your security manager/director to do so, you could analyse the files yourself.
- I would recommend that this is done on a system that is not connected to the network, and ideally this is a system that you will either 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.

```
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
```

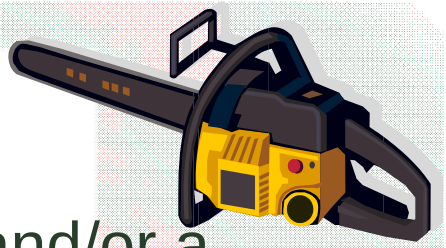
Step 3b: D-I-Y Sample Analysis…cont.



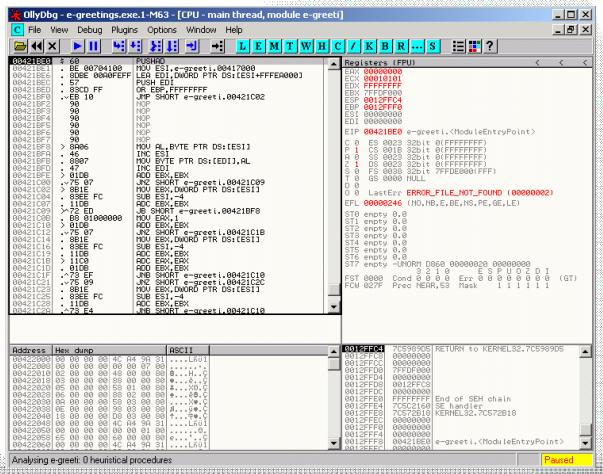
- Once this has been setup, you can use whatever tools you prefer to carry out the analysis, such as, using static analysis tools, like PEiD, Strings, File Alyzer and so on

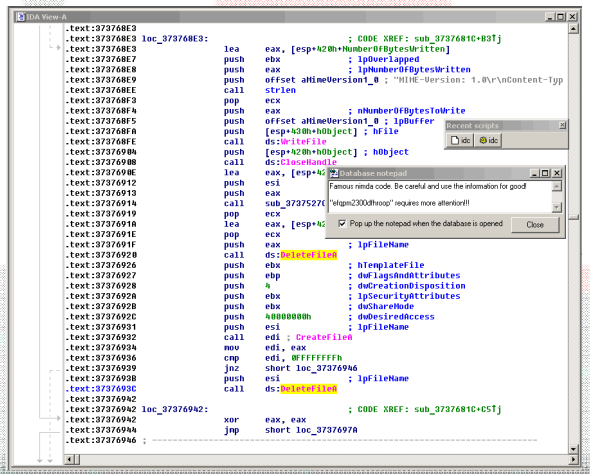


Step 3b: D-I-Y Sample Analysis…cont

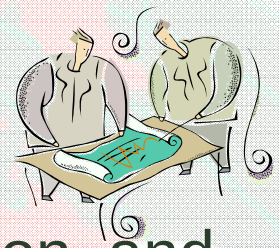


- You could also examine the file in a hex editor and/or a debugger. This is only advised if you are able to understand assembler code and you are sure that the file to be debugged does not contain and anti-debugging code which may be triggered during examination.
- This is also a good time to try out any remediation scripts or tools you have created as a quick-n-dirty solution to the problem [obviously only on a test system].



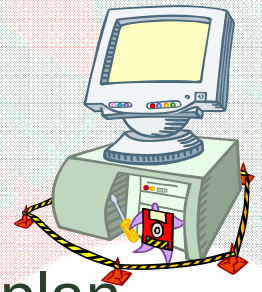


Step 4: Analyse The Data (Part 2)



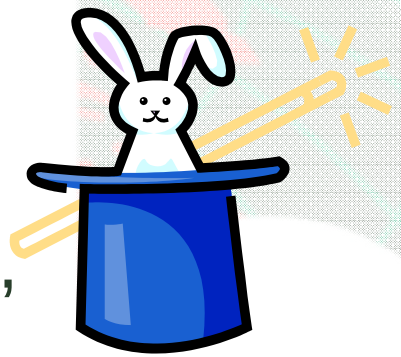
- By now you should have a good idea what is going on, and what any malcode is doing to the affected systems and what network traffic is being generated by it [or them].
- If you haven't then you should now take time to go over all the data you have acquired during the first three steps. You could use 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.

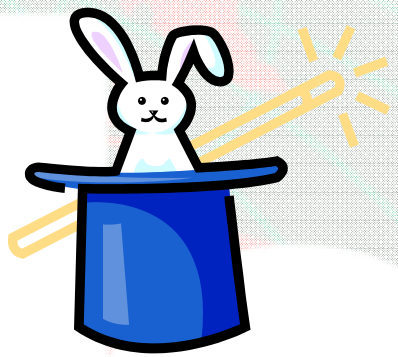
Tricks



- VB Scripting for quick and dirty cleanup, example:

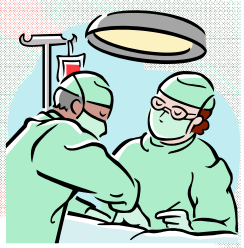
```
'RemSdbot2.vbs - SDbot remover for specific variant.
'© Martin Overton, 2007 (martin@arachnophiliac.com)
'Verson 0.99.2'
'Created to detect and remove an infection of the following
Sdbot variant
'
'FileName: rundll.exe
'FileDateTime: 19/01/2007 14:05:00
'Filesize: 1364992
'MD5: 71fd1205f6d7550967bda6bf4491a50a
'CRC32: 36E8176E
'File Type: PE Executable

... [For the rest see the paper]
```

Tricks…cont.



- 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.

Step 6: Post Mortem…cont.

- 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 must 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. If in doubt seek legal guidance first, before proceeding.*

Real World Examples

- **Real World Example 1**
  - User noticed that their anti-virus was disabled, and so reported it to the helpdesk of the company affected.
  - The local support teams noticed that the system that had its anti-virus software disabled was making lots of outbound DNS lookups for odd websites that were not business related.
  - Further investigation of the suspected system found a file that looked to be involved, a sample was acquired and analysed in several sandboxes as well as tested against 30+ anti-malware tools; very few reported the file as either suspicious or infected.

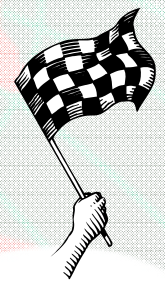
See the paper for a full description and analysis of each example.

Real World Examples…cont.

- **Real World Example 2**
  - An unknown malware was causing clients running anti-virus on a network to lose connection to the anti-virus management server. So, with the help of local resources on site we managed to obtain a sample which was suspected to be the culprit.
  - The anti-virus deployed on the network and workstations did not detect the malware as it was brand new.
  - The data acquired from analysing the sample allowed me to understand what the malware was doing and from this clean-up scripts could be created as well as blocking the infection vector used by the malware.

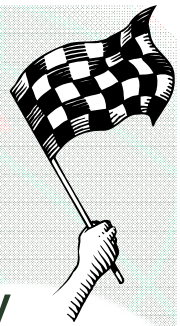
See the paper for a full description and analysis of each example.

Conclusions



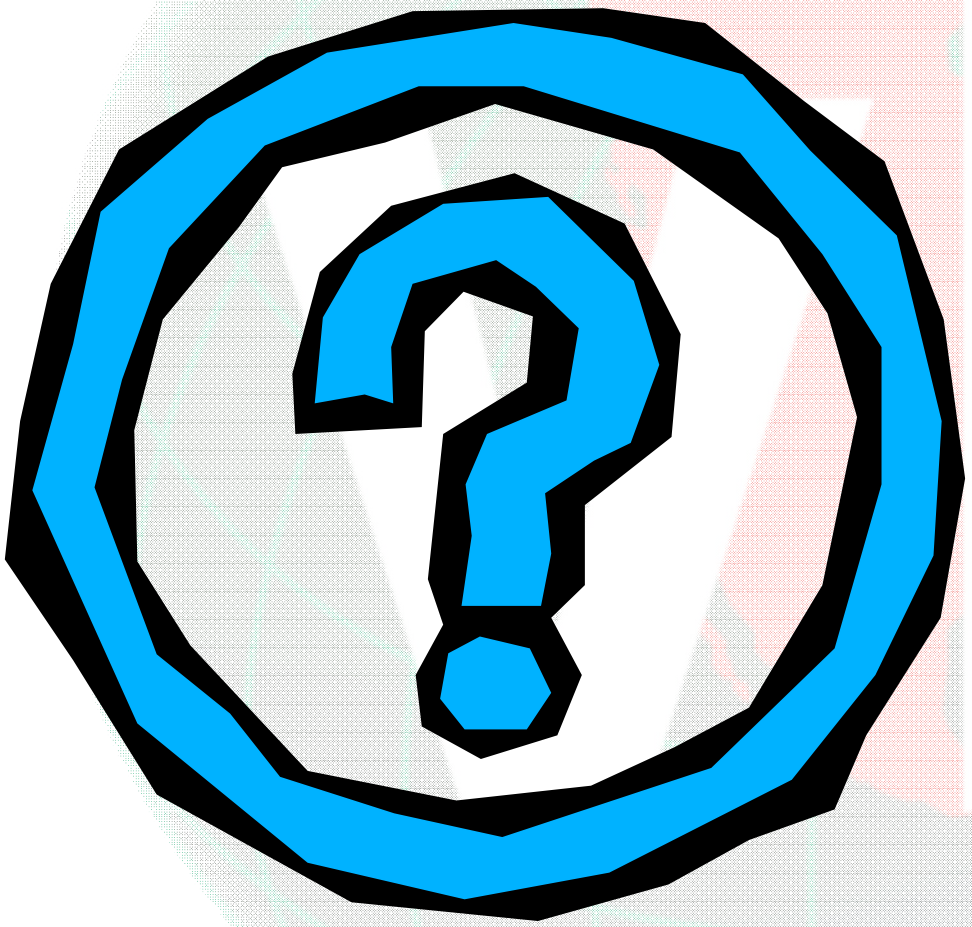
- Hopefully I have shown you that even if you are faced with a new malware threat that isn't detected by your anti-malware defences you can still, in most cases, find the infection, how it got in, how it communicates and with the right tools and methodologies even remove it safely before your anti-malware vendor comes up with a solution.
- As with other security threats, especially malware related ones, you need to deploy a multi-layered approach
- 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.

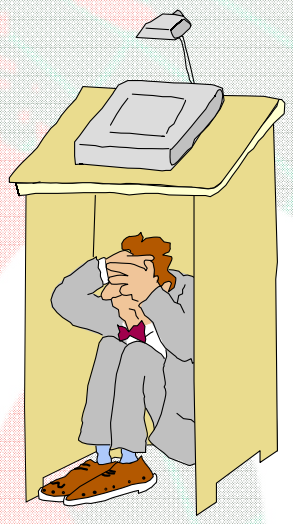
Conclusions…cont.



- 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.

Questions?





Contact details…..

Martin Overton
Malware/Anti-Malware SME
IBM Security Services

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

All my published papers and articles can be downloaded from:
http://momusings.com/papers/