

Finding the needle

How to find and remove Malware



Who am I?



Jake Johansen

UUHSC Information Security Architect

Jake.Johansen@hsc.utah.edu

What is malware?



Malware is a generic term increasingly being used to describe any form of malicious software; e.g., viruses, trojans, keyloggers, bots, malicious active content, etc.



How did it get here?

Entrance vector: **Unpatched Vulnerabilities**

- Zero day exploits
- Drive by downloads
- Vulnerabilities in available services; DCOM, RPC, p2p, Isass, etc



How did it get here?

Entrance vector: **Misconfiguration**

- No system hardening post install, unnecessary services
- No required passwords
- Default passwords
- Weak passwords
- System installed while attached to an insecure network



How did it get here?

Entrance vector: **Manual installation**

- Email attachment, opened by user or email program
- Legitimate program, trojaned or backdoors
- p2p downloads, double extensions
- Companion software to legitimate program



How did it get here?

Entrance vector: **User error**

- User has installed the malware
- Social Engineering (but it said, “I love you!”)
- Poor or nonexistent passwords



Is there a problem !?

Detecting the presence of malware

- Degraded system performance
- Anti-Virus not running
- Odd behavior, such as unexpected reboots
- Popup windows at strange time, i.e. when not browsing web
- System errors, malware typically poorly written



Is there a problem !?

- Reports of problems
 - External parties reporting issues
 - IDS/IDP
- Traffic patterns
 - Traffic analysis can uncover issues that are difficult to detect locally, such as rootkits.
 - To request an analysis
 - Campus ISO -> <http://iso.utah.edu>
 - HSC ISO -> <http://www.med.utah.edu/its/infosec/>



Basic Risk Assessment

- What type of information is on this system?
 - HIPAA - patient health information (PHI), including research
 - FERPA - student identifying data
 - GLB - student financial data, credit cards
- Is there a need to maintain forensics evidence?
- What accounts are on this system?
- Can and should this system be taken offline while forensics is performed?
- Who can help me and who should I notify?
 - Campus ISO or HSC ISO

Local Identification of malware



- Anti-virus scan while running in Safe Mode
- Audit running processes
- Audit the 'startup'
- Audit network connections
- Check the file system for files that have been hidden and REALLY hidden files
- Check for unusual services
- Audit the HOSTS file and IP Settings

Full system scan using anti-virus while running in Safe Mode



- Malware is sometimes able to hide from or disable anti-virus software.
- Most processes such as the malware will not load during the boot into 'Safe Mode', so AV software is often able to address such nefarious malware.
- Verify your AV software is effective by obtaining the latest signatures for your anti-virus scanner and running a full system scan after rebooting into 'Safe Mode'.



Audit running processes

- Close all running applications, including applications in the systray like msn messenger and other agents. Limiting legitimate processes will make it easier to audit the remaining running processes.
- Start the windows Task manager
winkey + R | taskmgr | Processes Tab
('Show processes from all users' should be checked)



Audit running processes

Look for odd processes such as;

- normal service name but is misspelled, svchost.exe is expected, scvhost.exe is NOT.
- random character file names.
- unusual processes with high CPU utilization
- seemingly legitimate process names but are unexpected on this system



Audit running processes

Searching the web using process names you are unsure about will give clues to the legitimacy of individual processes. There are a few sites that are building process databases which will give a detail listing of processes.

- <http://www.processlibrary.com/>
- <http://startup.iamnotageek.com/>



Audit running processes

Links: **useful process monitoring tools**

- GUI Process Explorer from Sysinternals
<http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>
- CLI Process Tools Suite from Sysinternals
<http://www.sysinternals.com/ntw2k/freeware/pstools.shtml>



Audit the 'startup'

Look for odd entries in the "startup" sections of the registry. Keep in mind that legitimate programs are seldom found in multiple start locations, such as run and runservices.

winkey + R | msconfig | Startup Tab

or

winkey + R | regedit | check the following

Audit the 'startup'



Most commonly used startup locations in the registry

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\microsoft\windows\CurrentVersion\Run
- HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run



Audit the 'startup'

Links: Useful startup tools

GUI HijackThis

<http://www.spywareinfo.com/~merijn/>

GUI Auto runs from sysinternals

<http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml>

Audit network connections



Close all running programs, including programs in the system tray like MSN Messenger. This will limit open connections making it easier to spot unexpected connections. As you identify running legitimate programs, stop them if possible to further narrow the search field.



Audit network connections

winkey + R | cmd | netstat -nao

- connections continually in 'SYN sent' state on 445, 139, or other
- established connections on odd ports, such as 6667(IRC)
- established connections on typical but unexpected ports such as FTP, TELNET, even 80(http)



Audit network connections

C:\netstat -nao (-o lists PID but only on XP)

```
C:\WINDOWS\system32\cmd.exe
C:\>netstat -nao
Active Connections

```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	155.100.151.158:139	0.0.0.0:0	LISTENING	4
UDP	0.0.0.0:445	**:		4
UDP	0.0.0.0:500	**:		1184
UDP	0.0.0.0:1032	**:		1788
UDP	0.0.0.0:1036	**:		1788
UDP	0.0.0.0:1038	**:		1788
UDP	0.0.0.0:1044	**:		1788
UDP	0.0.0.0:1457	**:		1724
UDP	0.0.0.0:4500	**:		1184
UDP	127.0.0.1:123	**:		1564
UDP	127.0.0.1:1040	**:		1724
UDP	155.100.151.158:123	**:		1564
UDP	155.100.151.158:137	**:		4
UDP	155.100.151.158:138	**:		4



Audit network connections

- Correlate PID from 'netstat -nao' with PID in taskmgr

Image Name	PID	User Name	CPU	Mem Usage	Peak Mem Usage
wdfmgr.exe	752	LOCAL SERVICE	00	1,588 K	1,740 K
svchost.exe	1876	LOCAL SERVICE	00	3,656 K	3,668 K
svchost.exe	1448	NETWORK SERVICE	00	4,700 K	4,700 K
svchost.exe	1788	NETWORK SERVICE	00	3,748 K	3,868 K
System Idle Process	0	SYSTEM	87	16 K	0 K
System	4	SYSTEM	00	220 K	2,616 K
FrameworkService...	188	SYSTEM	00	5,468 K	5,568 K
Mcshield.exe	256	SYSTEM	00	22,128 K	24,080 K
naPrdMgr.exe	320	SYSTEM	00	1,796 K	2,232 K
VsTskMgr.exe	336	SYSTEM	00	344 K	2,828 K
PGPsdkserv.exe	476	SYSTEM	00	2,460 K	2,460 K
SMAgent.exe	720	SYSTEM	00	1,512 K	1,660 K
smss.exe	840	SYSTEM	00	368 K	388 K
spoolsv.exe	932	SYSTEM	00	5,016 K	6,568 K
csrss.exe	992	SYSTEM	00	2,872 K	5,268 K
winlogon.exe	1128	SYSTEM	00	5,368 K	10,672 K
services.exe	1172	SYSTEM	02	4,284 K	4,304 K
lsass.exe	1184	SYSTEM	00	2,328 K	7,216 K
ati2evxx.exe	1340	SYSTEM	00	2,088 K	2,088 K

Processes: 43 CPU Usage: 15% Commit Charge: 326M / 1134M



Audit network connections

Links: useful network connection viewers

- GUI & CLI, TCPView and tcpvcon -> <http://www.sysinternals.com/ntw2k/source/tcpview.shtml>



Check for hidden files

There are files that are required for your system to run, many of these are hidden from accidental deletion. Malware takes advantage of such file attributes to hide from standard file searches, but the following command will list any HIDDEN, SYSTEM and READONLY file on your system. When performing this search pay particular attention to directories in the %PATH% variable such as C:\windows\system32, most malware seems to be placed in the path and loaded via the registry without an absolute path. DO NOT delete any of the files listed by this command unless you are positive they are malware, you can easily break a functional system by doing so.



Check for hidden files

From a command shell, C:\attrib /s | findstr SHR

```
C:\WINDOWS\system32\cmd.exe
C:\>attrib /s | findstr SHR
A SHR C:\Novell\GroupWise\USESHR.DLL
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\instance_Professional_32_1033.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_1.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_2.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_3.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_4.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_5.cab
SHR C:\WINDOWS\pchealth\helpctr\PackageStore\package_6.cab
A SHR C:\WINDOWS\system32\drivers\HP_HP_CPQ nx7000 <DL855A ABA>_YN_U_QCND347_E_4_I0860_
B68BAL Ver. F.42_T040507_WXP2_L409_M1280_J60_7Intel_8Pentium M_91.59_111063044_M10EC8139_P15
_U808624C2.MRK
SHR C:\WINDOWS\system32\Restore\filelist.xml
A SHR C:\boot.ini
A SHR C:\IO.SYS
A SHR C:\MSDOS.SYS
A SHR C:\NTDETECT.COM
A SHR C:\ntldr
C:\>_
```



Check for hidden files

Alternate Data Streams, the really hidden files.

NTFS allows for multiple data streams for each file descriptor, though no native tools are available to view or list what alternate data streams are on a system. This allows malware to hide files of any size 'behind' any file on an NTFS system. This is not used very often yet. Not all applications can use ADS, e.g. copy will not but cp from resource kit will.

Example, the following will create an ADS from a command shell; C:\>notepad C:\boot.ini:ADS.txt



Check for hidden files

Links: Alternate Data Stream tools

- CLI - FoundStone SFind in The Forensic Toolkit v2.0 <http://www.foundstone.com/>
- CLI – Sysinternals Streams
<http://www.sysinternals.com/ntw2k/source/misc.shtml>



Audit Services

Some malware will install as a service, often using an application wrapper such as firedaemon to do so. While removal of services is more difficult, you can easily disable them for temporary clean up.

- winkey + R | msconfig | Services Tab
- winkey + R | services.msc |
- Command shell -> tasklist, taskkill, tasklist /svc



Removal notes

Once malware has been identified, it is best to remove it while in safe mode. Some malware has additional processes that strive to stop you from removing it. Deleting startup locations and files while in safe mode, you can usually restore a system to working condition but not necessarily trusted state.



Post removal cleanup

Remember that a machine compromised by malware has effectively been 'hacked' and that it is usually best to return the machine to a trusted state by removing important data and rebuilding using best practices.

Keep in mind the following;

- Change all Passwords associated with this machine
- Hardening
- Patching

Questions ?

