

The State of Incident Response

Presented by
Kevin Mandia

August 2, 2006



Agenda

- How Organizations are Detecting Attacks
- What Attackers are Doing
- How Current Attack Trends are Influencing the Incident Response Process



Who Are We?

- Specializing in:
 - Application Security
 - Network Security
 - Incident Response
 - Computer Forensics
 - Professional Education
 - R & D



Who Are We?

- Last 3 Years
 - Responded to over 300 Potentially Compromised Systems.
 - Responded to Intrusions at Over 40 Organizations.
 - Created IR Programs at Several Fortune 500 Firms.



The State of Incident Response

1. The Sophistication of Attack Tools Can Outweigh the Sophistication of our Response Tools.
2. Reporting Requirements Major Top-Brass Concern:
 - Disclosure to Clients
 - Disclosure to Shareholders
3. Incident Owners have to Be Politically Savvy to Achieve Corporate Goals
 - Incident Response “Owners” are not High Enough on the Food Chain to be the *Deciderers*.
4. Diligent IR Does Not Always Parallel Management Objectives.



The State of Incident Response

5. Inexperienced Personnel.
 - Ad-Hoc Approach.
 - Not Enough Rotations.
 - Lack Sophisticated Skill Sets
6. Methods to Gather Live Response Data are too Time Consuming, Cumbersome, and May Even be Ineffective.
7. Technology Wicketness.
8. Resolution Always Requires more Resources than Expected.



The State of Incident Response

9. Lack of Formal Documentation
10. Windows is the Primary Victim/Target
11. Kernel Level Rootkits More Common ???



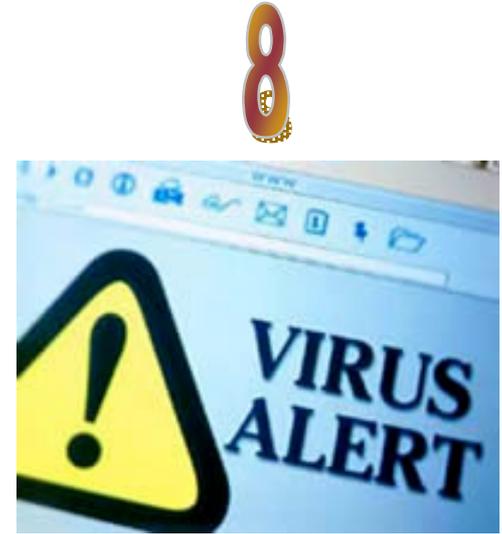
How Organizations are Detecting Attacks



1. How are Organization's Detecting Incidents?

▪ Antivirus Alerts?

- Perhaps, but do not Count on It...
- Alerts are Often Ignored – and Perhaps Value-less without an In-Depth Review of the System.
- Quarantined Files Often Remain a Mystery



Anti-Virus Merely Alerts an Organization that Something Bad Might have Occurred. No Confirmation. Potential Loss of Critical Data

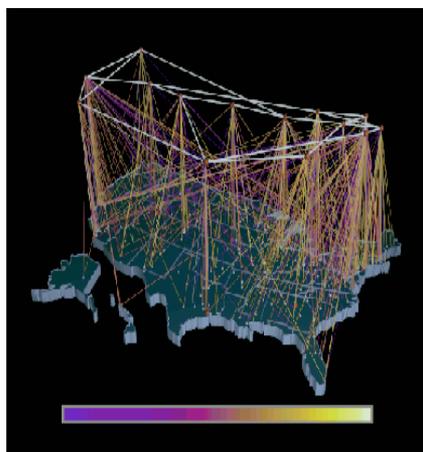
Findings – Ongoing Intrusion

- The Review of 10 Malicious Executable Files Yielded:
 - 12/12 Files were NOT Publicly Available
 - 12/12 Files were NOT Detected by AV
 - 11/12 Files Reviewed were Packed via 2(5) Different Methods

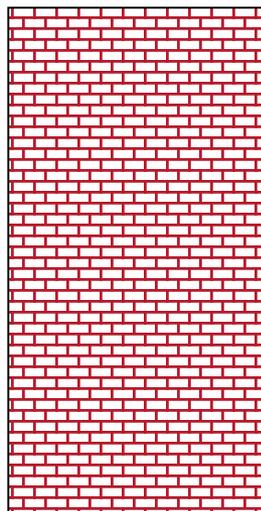
It is Highly Unlikely AV will ever Trigger on Microsoft Tools or Sysinternal Tools.

2. How are Organization's Detecting Incidents?

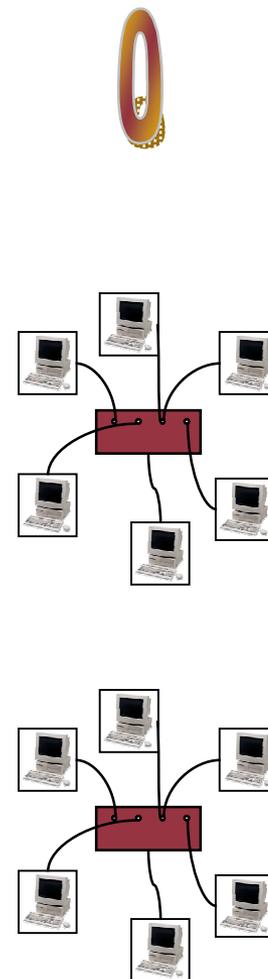
- IDS Alerts?
 - Rare Detection Mechanism.



Port 22
Port 443
VPN



Port 22
Port 443
VPN



3. How are Organization's Detecting Incidents?



▪ Clients (Outside Company)

- More Often than Pro-Active Countermeasures.
- Malicious Software Discovered on Compromised End-User Systems.
- Recently (December 2005) Found a Keylogger Configuration File that Contained Approximately 1,157 Keyword Search Terms, and URL's for Approximately 74 Online Banking Facilities.

Something Wrong Here?

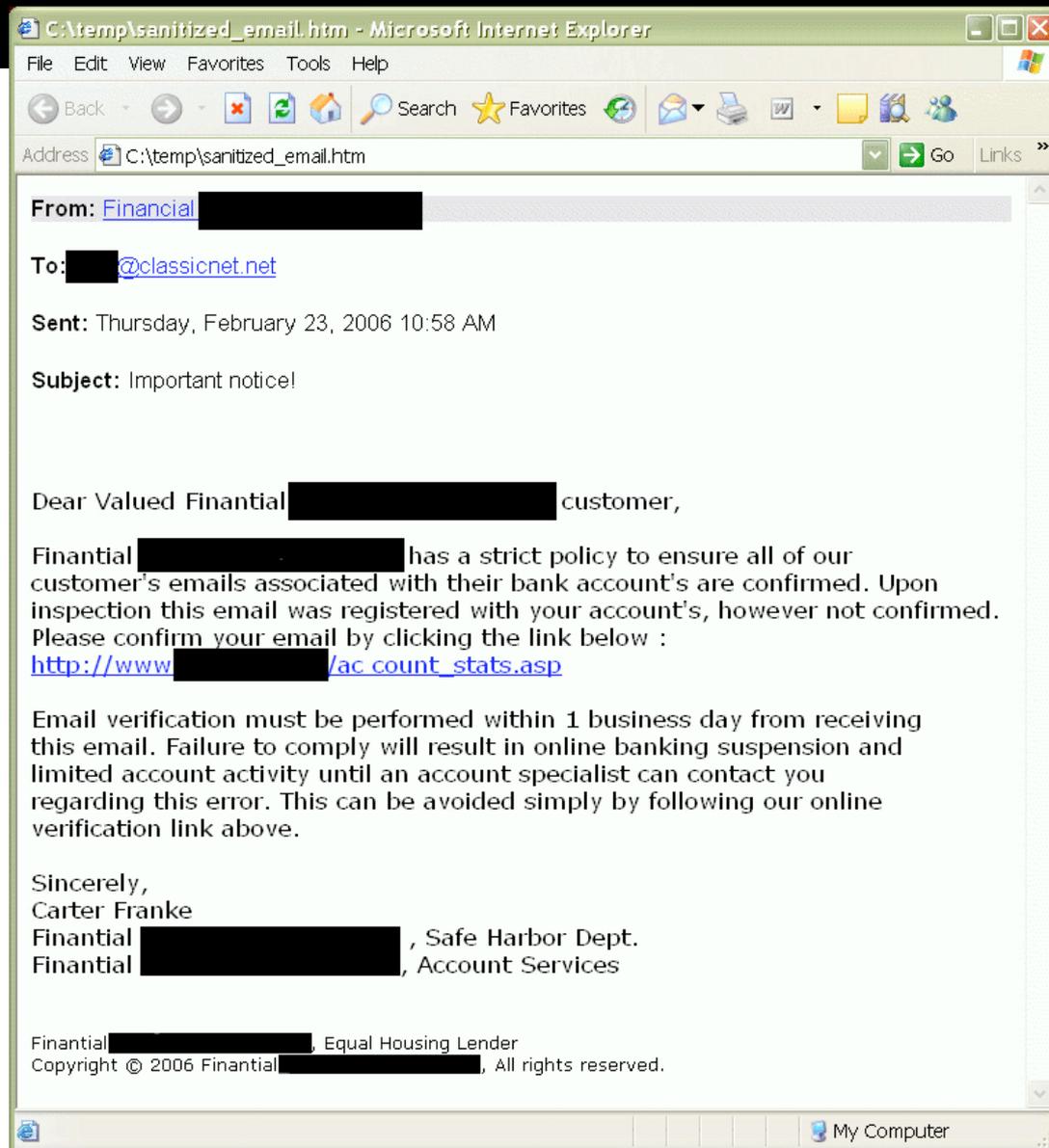
Security Confirmation

To continue with Online Banking, please provide the information requested below.

Enter Account Holder Information	
FirstName	<input type="text"/>
LastName	<input type="text"/>
Date of Birth (mm/dd/yyyy)	<input type="text"/> / <input type="text"/> / <input type="text"/>
Social Security Number	<input type="text"/> - <input type="text"/> - <input type="text"/>
Mother's Maiden Name (for security)	<input type="text"/>
E-mail	<input type="text"/>
ATM, Check Card Information	
Card Number	<input type="text"/>
Card Expiration Date (mm/yyyy)	<input type="text"/> / <input type="text"/>
Card CVV2	<input type="text"/>
ATM PIN	<input type="text"/>
Banking Account Information	
Primary checking account number	<input type="text"/>
Routing number	<input type="text"/>

submit changes

reset



4. How are Organization's Detecting Incidents?

34

▪ End Users (Internal)

- Continual Termination of Antivirus Software.
- Installing New Applications Simply Does Not Work.
- Commonly Used Applications Do Not Run.
- You Cannot "Save As".
- Task Manager Closes Immediately When You Execute It.



5. How Are Organization's Detecting Incidents?

- Something Obvious ...

What Attackers Are Doing



What Attackers are Doing Now

- Depends on Attack Type
 1. **Attacks for Money**
 2. **Attacks for Information**
 3. Attacks for Access
 4. Attractive Nuisances
 5. Information Warfare



Attacks for Money

- Primarily Attack Client-Side Applications or Individuals
- Target:
 - Personal Information (from Databases)
 - SSN
 - CC Numbers
 - Private Bank Account Numbers
 - Routing Numbers
 - Emails (to Phish)
 - Credentials
 - User IDs and Passwords



Attacks for Money

- Technical Characteristics:
 - Involve Email Attack Vector (Phishing) Merged With WWW Technology (Browser Issues)
 - Dependence on Keystroke Logging
 - Dependence on Client Solicitation
 - May Implement Wanton Propagation
 - Use of Spreader Mechanism
 - Persistence of Malware on Victim System Often not a Concern



Often a Decentralized Security Problem.

Case Study One

Attack for Profit



Attacks for Information

- Target:
 - Target Specific Organizations
 - Wanton Spreading Less Common
 - Information of Interest:
 - Intellectual Property
 - Databases
 - Documents
 - Spreadsheets
 - ????



Attacks for Information

- Technological Characteristics:
- Rely on Continued Access
 - Valid Credentials
 - Persistent Backdoors
- Post Exploitation Sophistication - Malicious Code More Persistent
 - In-Memory Library Injection in Windows Expanding
- Requires *Surreptitious* Theft of Data
 - Highly Used Ports
 - Web Traffic
 - Segmentation of Files (rar)
- Often Move Fast



Often a Centralized Security Problem.

Case Study Two

Information Pilfering





How Current Attack Trends are Influencing the Incident Response Process



How Current Attack Trends are Influencing the Incident Response Process

1. The Need to Acquire and Analyze the Contents of RAM
2. The Need to Locate Well-Hidden, User Space Malicious Code
 - Review of System Volume Restore
 - Windows Services Mayhem
 - Altering the Image Path
 - Replacing Legitimate Services
 - Using SVCHOST Invocation
3. The Need for Malware Triage
 - Identification and Remediation
4. The Need for Speed

The Need to Acquire and Analyze the Contents of RAM



Obtaining Memory Dumps and Process Space

- ☑ ■ Contents of Physical Memory
 - \device\PhysicalMemory
- ☑ ■ Pagefile
 - pagefile.sys
 - Could be More than One
- ☑ ■ Memory from Individual Processes
 - Userdump



Obtaining Physical Memory (Ram)

- **Unix – Simple**
 - `/dev/kmem`
 - `/dev/mem`
 - `/dev/kcore`
- **Windows – Not as Simple.**
 - Windows Operating Systems do not Provide Such a File Objects.
 - Windows Does have a “/Device/PhysicalMemory” Section Object.
 - Use “dd”, by Mr. George M. Garner, Jr.
 - <http://users.erols.com/gmgarner/forensics>.

Obtaining RAM – “dd” Command Line

```
E:\>dd.exe if=\\.\physicalmemory of=f:\win2khost-  
physicalmemory.dd bs=4096
```

```
Forensic Acquisition Utilities, 3, 16, 2, 1030
```

```
dd, 1, 0, 0, 1030
```

```
Copyright (C) 2002 George M. Garner Jr.
```

```
Command Line: dd.exe if=\\.\physicalmemory of=f:\win2khost-physicalmemory.dd bs=4096
```

```
Based on original version developed by Paul Rubin, David MacKenzie, and Stuart Kemp
```

```
Microsoft Windows: Version 5.0 (Build 2195.Professional)
```

```
26/02/2003 03:48:35 (UTC)
```

```
25/02/2003 22:48:35 (local time)
```

```
Current User: WIN2K\Administrator
```

```
Total physical memory reported: 523760 KB
```

```
Copying physical memory...
```

```
E:\dd.exe:
```

```
    Stopped reading physical memory:
```

```
The parameter is incorrect.
```

```
Output e:\win2khost-physicalmemory.dd 536801280/536801280 bytes  
(compressed/uncompressed)
```

```
131055+0 records in
```

```
131055+0 records out
```

Obtaining the Page/Swap File

- Cannot Copy this File from a Live Windows System – You Receive an `Access Denied` Error.
- By copying `\\.\physicaldrive0`, You Obtain the Entire Contents of the First Physical Disk—including the Page File.
- Access Data has a tool to do this.



Obtaining Specific Process Memory

- By Obtaining a Memory Dump of the Suspect Application, One Can:
 - Determine the Purpose of the Application
 - View the Command Line Used to Launch the Application
 - View the Application's Data Stored in Memory
 - Reveal Potential Commands Executed or Spawned
 - Process Memory Dump of cmd.exe

Obtaining Process Space – “Userdump” Command Line

- “Userdump.exe” is Part of the OEM Support Tools for Windows:
 - <http://download.microsoft.com/download/win2000srv/Utility/3.0/NT45/EN-US/Oem3sr2.zip>
- Note that Userdump has Several Useful Options.
 - Capture of Multiple Processes on a Single Command Line and Displaying Running Processes

```
E:\>userdump 744 f:\svchost_PID744.dmp
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights
reserved.
Dumping process 744 (svchost_.exe) to
f:\svchost_PID744.dmp...
```

Using userdump

- E:\>userdump 1272 f:\cmd_1272.dmp
- E:\>userdump 1372 f:\ftp_1372.dmp
- E:\>userdump 1160 f:\cmd_1160.dmp

cmd	1272	8	1	25	984	0:00:00.020	0:00:00.030	2:41:15.969
ftp	1372	8	1	39	1176	0:00:00.020	0:00:00.020	2:39:05.861
cmd	1160	8	1	28	976	0:00:00.020	0:00:00.010	2:24:25.536
nc	1424	8	3	40	1012	0:00:00.010	0:00:00.040	2:23:39.800
cmd	1092	8	1	34	968	0:00:00.010	0:00:00.020	2:22:03.992
cmd	1468	8	1	30	984	0:00:00.030	0:00:00.030	2:00:02.272
cmd	496	8	1	24	964	0:00:00.020	0:00:00.090	0:00:00.841
T_NC	1348	8	1	28	1004	0:00:00.020	0:00:00.030	0:00:00.821
T_PSLIST	1484	8	2	87	1216	0:00:00.040	0:00:00.030	0:00:00.050

CMD_1272

```
0011D68E 0000 0000 0066 7470 2039 352E 3230 382E 3132 332E 3634 0DOA 0032 .....ftp 95.208.123.64...2
0011D6A8 5C64 6C6C 3E00 2C34 3533 2C34 3536 2C33 3834 2062 7974 6573 2066 \dll>.,453,456,384 bytes f
0011D6C2 7265 650D 0A00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ree.....
0011D6DC 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
0011D6F6 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
0011D710 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

CMD_1468

```
00008110 | 0000 0000 0000 0000 0000 0000 0000 0000 0000 | .....
00008120 | 0000 0000 0000 0041 646D 696E 6973 7472 | .....Administr
00008130 | 6174 6F72 3A35 3030 3A39 6450 9AFC 7767 | ator:500:9dP..wg
00008140 | 9AFC 7788 A713 0000 1000 0000 0000 0033 | ..w.....3
00008150 | 3562 3543 003A 0000 003A 6362 3863 3537 | 5b5C.:...:cb8c57
00008160 | 3035 6639 3264 6539 6438 6431 3136 3478 | 05f92de9d8d1164x
00008170 | 0113 00E0 A713 0062 3732 3A3A 3A0D 0A40 | .....b72:::..@
00008180 | F612 0009 0000 00D3 43F9 7738 0813 0000 | .....C.w8....
00008190 | 0013 0009 0000 0050 A213 0018 F612 0000 | .....P.....
000081A0 | 0200 00D0 F712 00DB 80FB 7718 44F9 77FF | .....w.D.w.
000081B0 | FFFF FFE0 F712 0016 98FC 7738 0813 0003 | .....w8....
000081C0 | 0000 0040 0000 0000 0000 003A 3A0D 0A49 | ...@.....:..I
000081D0 | 5553 525F 4A42 5257 5757 3A31 3030 303A | USR_JBRwww:1000:
000081E0 | 6239 3336 3938 3662 6131 6335 3633 3662 | b936986ba1c5636b
000081F0 | 3066 3238 6430 3534 3966 3461 3763 3130 | 0f28d0549f4a7c10
00008200 | 3A31 3337 6330 3435 6331 6361 6361 6534 | :137c045c1caca4
00008210 | 6230 3763 3663 3362 3838 6266 3063 6536 | b07c6c3b88bf0ce6
00008220 | 643A 3A3A 0D0A 4957 414D 5F4A 4252 5757 | d:::..IWAM_JBRww
```

FTP_1372

```
00004010 | 0020 F706 00FA 1401 7855 5345 5220 6674 | . . . . .xUSER ft
00004020 | 700D 0A00 0000 0007 000A 0000 0000 0000 | p. . . . .
00004030 | 003C EF06 0000 0200 0088 EF06 0002 0000 | .<. . . . .
00004040 | 00D3 43F9 77E8 0607 0000 0007 0002 0000 | ..C.w. . . . .

000FDFE0 | 0000 0000 0033 3331 2041 6E6F 6E79 6D6F | .....331 Anonymo
000FDFE0 | 7573 2061 6363 6573 7320 616C 6C6F 7765 | us access allowe
000FE000 | 642C 2073 656E 6420 6964 656E 7469 7479 | d, send identity
000FE010 | 2028 652D 6D61 696C 206E 616D 6529 2061 | (e-mail name) a
000FE020 | 7320 7061 7373 776F 7264 2E0D 0A00 0000 | s password.....
```



The Need to Locate Well-Hidden, User Space Malicious Code



User Space Hiding Techniques

- Malware named after Legitimate Windows Services
 - Swupdtmr.exe
 - symwsc.exe
 - Spoolsv.exe
 - Svchost.exe
- Malware Named Something Similar to Legitimate Windows Services
 - Winservices.exe
- Use of Windows Services to Hide/Start Malware
- Use of Malicious dlls
- Most Malware Placed in %systemroot% or Subdirs

Case 1: Altering the Image Path

1. The Existing “sysmonlog” Service is Stopped.
2. The Backdoor File was Copied to:
“%SYSTEMROOT%\system32\drivers\”
3. The New File was Modified to have the Same Time Stamps as
%SYSTEMROOT%\system32\kernel32.dll.
4. The Registry Value
“HKLM\System\CurrentControlSet\Services\Sysmonlog\imagePath” was changed to
“%SystemRoot%\system32\drivers\smlogsvc.exe”

Case 1: Altering the Image Path

1. The Registry Value

“HKLM\System\CurrentControlSet\Services\Sysmonlog\Start” is Set to 2

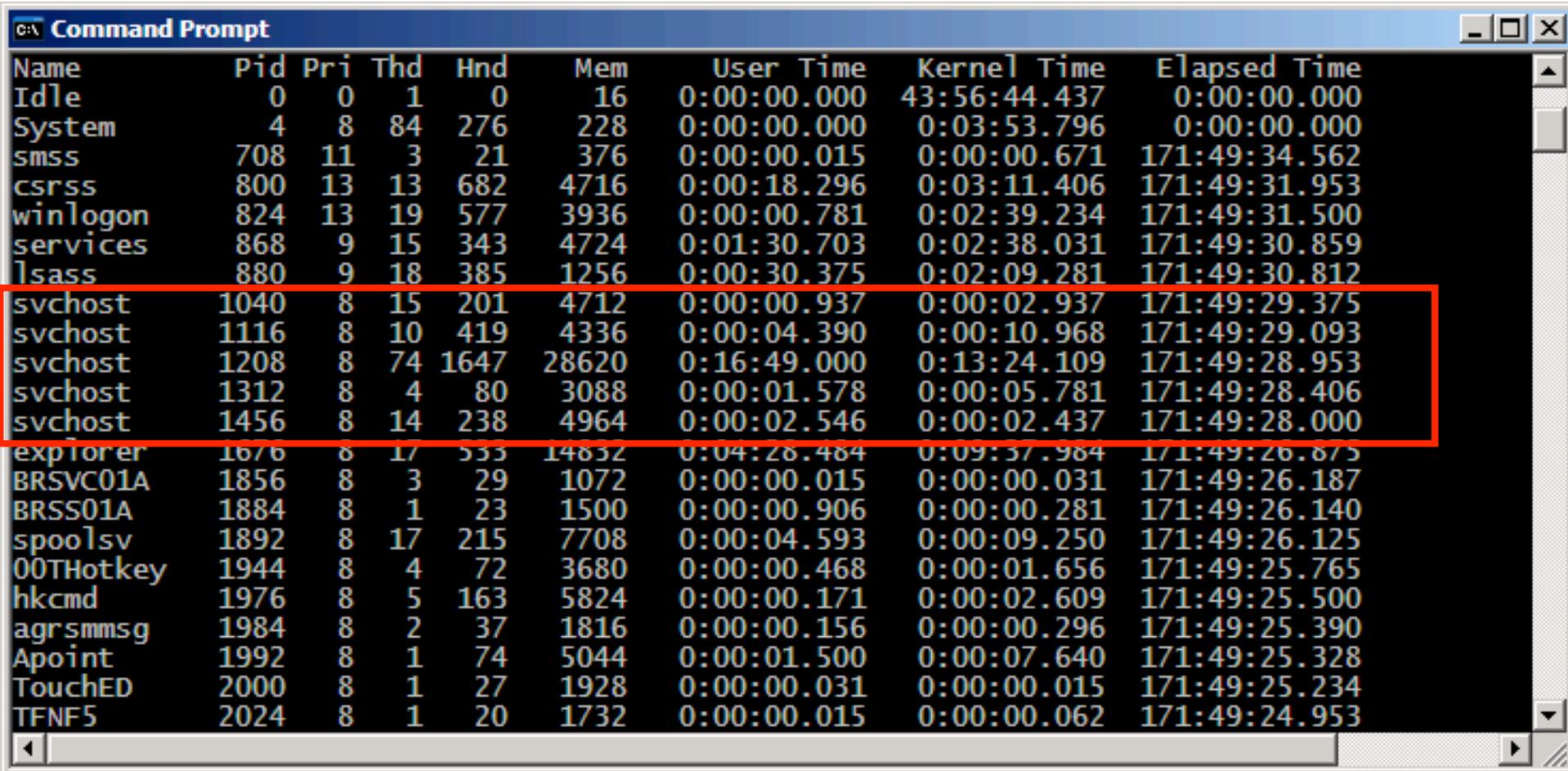
- Ensures that the Service Starts Automatically Upon Reboot.

2. The Registry Value

“HKLM\System\CurrentControlSet\Services\Sysmonlog\ObjectName” is set to “LocalSystem”.

- Causes the Backdoor Service to Run with the Privileges of the “LocalSystem” Account.

The Nuisance of SVCHOST



A screenshot of the Windows Task Manager window, showing a list of running processes. The processes are sorted by CPU usage. The svchost processes are highlighted with a red box, indicating they are the focus of the slide. The svchost process with PID 1208 is the most CPU-intensive, using 1647% of the CPU.

Name	Pid	Pri	Thd	Wnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	16	0:00:00.000	43:56:44.437	0:00:00.000
System	4	8	84	276	228	0:00:00.000	0:03:53.796	0:00:00.000
smss	708	11	3	21	376	0:00:00.015	0:00:00.671	171:49:34.562
csrss	800	13	13	682	4716	0:00:18.296	0:03:11.406	171:49:31.953
winlogon	824	13	19	577	3936	0:00:00.781	0:02:39.234	171:49:31.500
services	868	9	15	343	4724	0:01:30.703	0:02:38.031	171:49:30.859
lsass	880	9	18	385	1256	0:00:30.375	0:02:09.281	171:49:30.812
svchost	1040	8	15	201	4712	0:00:00.937	0:00:02.937	171:49:29.375
svchost	1116	8	10	419	4336	0:00:04.390	0:00:10.968	171:49:29.093
svchost	1208	8	74	1647	28620	0:16:49.000	0:13:24.109	171:49:28.953
svchost	1312	8	4	80	3088	0:00:01.578	0:00:05.781	171:49:28.406
svchost	1456	8	14	238	4964	0:00:02.546	0:00:02.437	171:49:28.000
explorer	1676	8	17	533	14832	0:04:28.484	0:09:37.984	171:49:26.875
BRSVC01A	1856	8	3	29	1072	0:00:00.015	0:00:00.031	171:49:26.187
BRSS01A	1884	8	1	23	1500	0:00:00.906	0:00:00.281	171:49:26.140
spoolsv	1892	8	17	215	7708	0:00:04.593	0:00:09.250	171:49:26.125
00THotkey	1944	8	4	72	3680	0:00:00.468	0:00:01.656	171:49:25.765
hkcmd	1976	8	5	163	5824	0:00:00.171	0:00:02.609	171:49:25.500
agrsmmsg	1984	8	2	37	1816	0:00:00.156	0:00:00.296	171:49:25.390
Apoint	1992	8	1	74	5044	0:00:01.500	0:00:07.640	171:49:25.328
TouchED	2000	8	1	27	1928	0:00:00.031	0:00:00.015	171:49:25.234
TFNF5	2024	8	1	20	1732	0:00:00.015	0:00:00.062	171:49:24.953

Case 2: Altering the ImagePath

- The Following Key Contained the Location of the Backdoor “dll”.
 - Note: The Backdoor Will Be in the “%SYSTEMROOT%” Directory Instead of the “%SYSTEMROOT%\system32” Directory.

HKLM\SYSTEM\ControlSet001\Services\\ImagePath

Case 3: Hiding Backdoors Yet Again

- The Legitimate service named BITS (the Background Intelligent Transfer Service) is Modified to Load the Backdoor Program (“qmgrxxx.dll”) instead of the legitimate service (“qmgr.dll”).
- The BITS Service was Configured to Start Automatically upon System Initialization.

Case 3: Hiding Backdoors Yet Again

- Reviewing Running Services Configuration Data does not Assist you in Finding this Backdoor:

```
C:\psservice config bits
```

```
<Text Omitted>
```

```
BITS has been disabled.
```

```
TYPE                : 20 WIN32_SHARE_PROCESS
START_TYPE          : 2  AUTO_START
ERROR_CONTROL       : 1  NORMAL
BINARY_PATH_NAME    : C:\WINDOWS\System32\svchost.exe -k netsvcs
LOAD_ORDER_GROUP    :
TAG                 : 0
DISPLAY_NAME        : Background Intelligent Transfer Service
DEPENDENCIES        : Rpcss
SERVICE_START_NAME: LocalSystem
FAIL_RESET_PERIOD   : 0 seconds
FAILURE_ACTIONS     : Restart      DELAY: 60000 seconds
                   : Restart      DELAY: 60000 seconds
                   : Restart      DELAY: 60000 seconds
```

Case 3: Hiding Backdoors Yet Again

- You Must Review the Registry for ServiceDLL Information

BITS

```
Type = REG_DWORD 0x00000020
Start = REG_DWORD 0x00000002
ErrorControl = REG_DWORD 0x00000001
ImagePath = REG_EXPAND_SZ
%SystemRoot%\System32\svchost.exe -k netsvcs
DisplayName = Background Intelligent Transfer Service
DependOnService = REG_MULTI_SZ "Rpcss"
DependOnGroup = REG_MULTI_SZ
ObjectName = LocalSystem
Description = <removed text>
Parameters
ServiceDll = REG_EXPAND_SZ
C:\WINDOWS\System32\qmgr.dll
Security [17 1]
```

The Need for Malware Triage

Elf file type is EXEC (Executable file)

Entry point 0x8048080

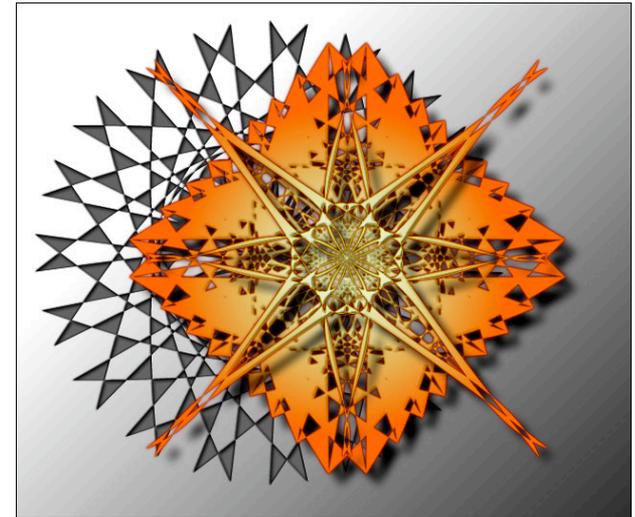
There are 2 program headers, starting at offset 52

Program Headers:

Type	Offset	VirtAddr	PhysAddr	FileSiz	MemSiz	Flg	Align
LOAD	0x000000	0x08048000	0x08048000	0x00590	0x00590	R E	0x1000
LOAD	0x000590	0x08049590	0x08049590	0x0002c	0x0002c	RW	0x1000

Malware Triage Answers ...

- What is the Intent and Capability of the Attacker?
- Did the Attacker Take Stuff?
- How Can We Find Him on our Network?
 - Host-Based Signatures?
 - Network-Based Signatures?
- How Can We Keep the Attacker Out? Minimize His Impact?



Performing Malware Analysis

- Keep Your Goals in Mind:
- WHAT IS THE TOOL?
 - Network Listener / Backdoor
 - Network Listener / Sniffer
 - Network Scanner
 - Port Redirector
 - Password Cracker
 - Password Dumper
 - Keylogger





Our Goal During Presentation

- Demonstrate Methods to Quickly Identify and Categorize Malware by Performing a:
 - Review of IAT
 - Review of Disassembled Code for Recognizable Constructs



Our Goal During Presentation

- Realization that Disassembly and Debugging are Activities Currently Reserved for a Few Brave Men/Women.
- Most Firms do not want to Expend the Resources to fully Analyze Malicious Code
- There is a Need for Quick Strike Identification and Development of Countermeasures

Static Analysis

- File “FingerPrinting”
- Virus Scan
- Packed or Not Packed?
- Strings
- Hex Editor
- Web Searching
- Disassembly



File Fingerprinting

- Fingerprint the Files you are Examining so that You will Know if they Change during Your Analysis
 - MD5Sum
 - File Size
 - File Name
 - Time/Date Stamps
 - Resource Section
 - Compile Date
- Use `md5deep` or Cygwin's `md5sum`



```
md5sum hello* > md5sum_hello_files.txt
cat md5sum_hello_files.txt
611957bd6a2ad9642027904a65f3638e  hello
7ab03b44ac6a20b0fa0cc80b636b0f51  hello.c
```

- When you have Completed your Analysis (or at various points along the way) you Should Check the md5sums to Ensure the Values have not Changed!
`md5sum -c md5sum_hello_files.txt`

Virus Scan

- Always Scan New Malware with an Up to Date Virus Scanner.
- Someone Else may have Already Discovered and Documented the Program you are Investigating!!

- Norton AntiVirus version 10.0.1.13
- Sophos Anti-Virus 5.0.2
- Microsoft AntiSpyware (Beta1) version 1.0.509
- Ad-Aware SE build 1.06r1
- Etrust PestPatrol version 5.0.1.5.

Viruscan.jotti.org

Jotti's malware scan 2.99-TRANSITION_TO_3.00

File to upload & scan:  

Service

Service load: 0%  100%

File: as.exe

Status: OK

MD5 3a0de7652a5832ecccc91d38e13c3cc1

Packers detected: -

Scanner results

AntiVir	Found nothing
ArcaVir	Found nothing
Avast	Found nothing
AVG Antivirus	Found nothing
BitDefender	Found nothing
ClamAV	Found nothing
Dr.Web	Found nothing
F-Prot Antivirus	Found nothing
Fortinet	Found nothing
Kaspersky Anti-Virus	Found nothing
NOD32	Found nothing
Norman Virus Control	Found nothing
UNA	Found nothing
VBA32	Found nothing

Comparison with 14 Different AV Products

Armor Features

- Encryption
- Compression
- Obfuscation
- Anti-Patching
 - CRC Checking
- Anti-Tracing
 - SoftICE, ICEDump Detection Code.
 - Crashes OS if they are Found in Memory
- Anti-Unpacking
- Restrictive Runtimes
- Restrictive Dates
- Password Protected
- Configuration Files
- Configuration Configurations

Packers

- UPack by [Dwing](#). 08.IV.2005.
- Mew by [Northfox](#). 22.IX.2004.
- UPX by [Laszlo & Markus](#). 03.VII.2004.
- Packman by [bubba](#). 27.II.2005.
- EZIP by [Jonathan Clark](#). 21.VII.2001.
- PE-PaCK by [ANAKiN](#). 12.I.1999.
- FSG by [bart](#). 24.V.2004.
- Dropper by [Gem](#). 13.III.2005.
- CExe by [Scott](#). 20.III.2003.
- PE Diminisher by [tERAPHY](#). 11.IX.1999.
- PECRYPT32 by [random](#), [kill](#) and [acpizer](#). 12.I.1999.
- PESpin by [cyberbob](#). 09.III.2005.
- NSPack by [North star Tech](#). 05.VI.2005.
- eXPressor by [CGSoftLabs](#). 28.III.2005.
- Thinstall by [Jonathan Clark](#). 29.III.2005
- PEBundle by [Jeremy Collake](#). 12.III.2004.
- PECompact by [DevelTek](#). 06.IV.2005.
- AS-Pack (shareware) by [Solodovnikov Alexey](#). 07.I.2002.
- NeoLite (shareware) by [NeoWorx Inc](#). 04.IV.1999.
- WWPack 32 by [Piotr Warezak](#). 07.VII.2000.
- ARM Protector by [SMoKE](#). 22.IX.2004.

Packed or Not Packed -- PEiD

- PEiD is a Free Program that Identifies Signatures Associated with Over 450 Different “packers” and Compilers.

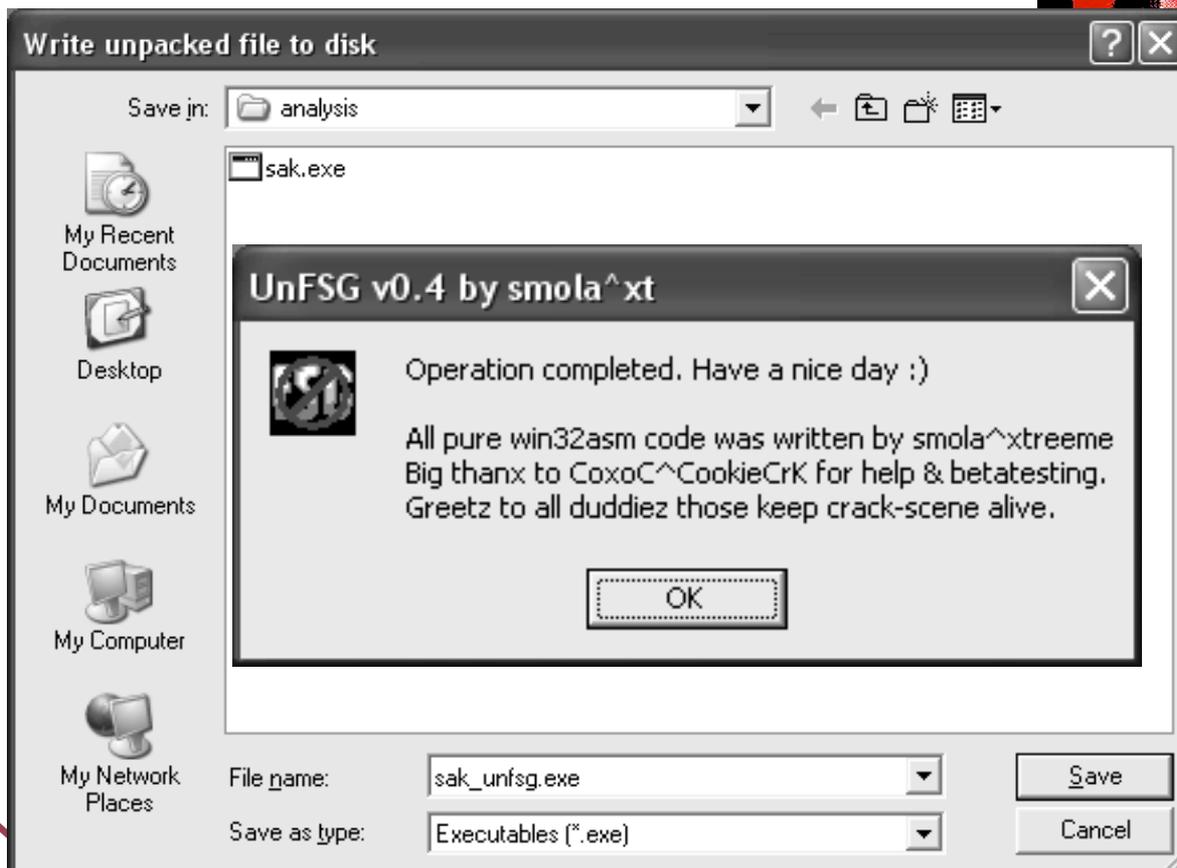


Unpackers

- Ollydbg with the Ollydump plugin.
- IDAPro with the “Universal Unpacker Plugin”.
- Generic Unpacker Win32 by Christoph Gabler. 31.VII.2001.
Win32 Intro by [Vitaly Evseenko](#). 21.IX.1999.
- UN-PACK by Snow Panther. 21.IV.2003.
- UNPE-SHiELD by G-RoM. 1.VI.1999 de-CodeCrypt by xOANINO.
10.V.2000.
- Ni2Untelock by [Ni2](#). 31.XII.2000.
- DeYoda by C-ripper. 18.II.2001.
- UnPEProt by Lorian. 23.I.1999.
- DePE-PACK by Unknown One. 03.V.2002.
- Un-FSG by [SMoKE](#). 12.I.2003.
- un-ASPack by dtg. 26.VIII.1999.
- StealthKiller by Snow Panther. 04.IX.2002.

Unpacking FSG - UnFSG

- UnFSG
- Conduct a Google Search for “unpack” and “FSG”
- Downloaded UnFSG by “smola”



Unpacking with UPX

```
C:\Mandia\toolanalysis>upx -d as.exe -o unpackedas.exe
      Ultimate Packer for eXecutables
  Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
  UPX 1.25w      Markus F.X.J. Oberhumer & Laszlo Molnar      Jun 29th

      File size      Ratio      Format      Name
-----
  32768 <- 14848  45.31%  win32/pe  unpackedas.exe

Unpacked 1 file.
```

Strings

```
C:\analysis>strings
```

```
Strings v2.1
```

```
Copyright (C) 1999-2003 Mark Russinovich
```

```
Systems Internals - www.sysinternals.com
```

```
usage: strings [-s] [-n length] [-a] [-u] [-q] <file or directory>
```

```
-s Recurse subdirectories
```

```
-n Minimum string length (default is 3)
```

```
-a Ascii-only search (Unicode and Ascii is default)
```

```
-u Unicode-only search (Unicode and Ascii is default)
```

```
-q Quiet (no banner)
```

Conducting Web Research

- Look at Unique Strings, Email Addresses, Network Info
- Search the Web
 - Be Careful → Google Cache Does Not Equal Anonymous
 - You Might Find other Victims, or Complete Analysis
 - Do not Forget Newsgroups
- It Helps if you Know Chinese (or Russian)
http://www.google.com/language_tools?hl=en

Disassembly

- Executable File Formats

- Windows: PE (Portable Executable)

www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx

- Linux: ELF (Executable and Linking Format)

www.skyfree.org/linux/references/ELF_Format.pdf



DisAssembly Cheat Sheet

- Quick Snapshot of Recognizing “likely evil” Constructs in Disassembled Code
 - Use of the Network
 - Use of Raw Sockets
 - Use of Encryption
 - Use of XOR Encoding
- No Hardcore Reversing Skills Necessary





The Need for Speed





Questions?