Kevin Mandia
Red Cliff Consulting

Performing Effective Incident Response

During the course of 2004 and 2005, we have responded to dozens of computer security incidents at some of America’s largest organizations. Mr. Mandia was on the front lines assisting these organizations in responding to international computer intrusions, theft of intellectual property, electronic discovery issues, and widespread compromise of sensitive data. Our methods of performing incident response have altered little in the past few years, yet the attacks have greatly increased in sophistication. Mr. Mandia addresses the widening gap between the sophistication of the attacks and the sophistication of the incident response techniques deployed by “best practices.”

During this presentation, Mr. Mandia re-enacts some of the incidents; provides examples of how these incidents impacted organizations; and discusses the challenges that each organization faced. He demonstrates the “state-of-the-art” methods being used to perform Incident Response, and how these methods are not evolving at a pace equal to the threats. He outlines the need for new technologies to address these challenges, and what these technologies would offer. He concludes the presentation by discussing emerging trends and technologies that offer strategic approaches to minimize the risks that an organization faces from the liabilities the information age has brought.
Performing Effective Incident Response

By Kevin Mandia

Responding to Spreadsploit MalbotWorms and BackdoorZombieChannels
The State of the Hack

By Kevin Mandia

July 1, 2005
"They Say"

Every major financial institution has been exploited by attackers.
All outsourced software is being made with backdoors.
Every developed nation is creating cyber-warfare capabilities.
Firewalls, IDS, and Anti-Virus are not as effective as consumers thought.
There are hundreds of non-publicly available exploits in use right now.

CMA … Of Course

Hackers plot to create massive botnet

By John Leyden
Published Friday 3rd June 2006 13:49 GMT

Computer Associates has warned of a co-ordinated malware attack (CMA) described as among the most sophisticated yet unleashed on the net. The attack involves three different Trojans – Qleder, Fantibag and Mitgieler – in a co-ordinated assault designed to establish a huge botnet under the control of hackers. CA reckons that access to the compromised PCs is for sale on a black market, at prices as low as five cents per PC.

CA security researchers reckon the three items of malware have been combined to maximise the potency of the overall assault. The elements of the attack include:

digital self defense
## IRC Channel Bots

- SubSeven Bot
- Bionet Bot
- AttackBot
- GT Bot
- EvilBot
- SlackBot
- Litmus Bot
- Fantibag
- Mitglieder

## Why Are We Here?

- Initial Detection
- Discuss Case Studies
  - Examine Emerging Trends
- Incident Response
  - Host-Based - Review Live Response Techniques
- Tool Analysis
Background

The Journey So Far …

<table>
<thead>
<tr>
<th>Year</th>
<th>No</th>
<th>Description</th>
<th>Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993 - 1998</td>
<td>50+</td>
<td>Unix Compromises</td>
<td>Solaris, Irix, HP-UX, AIX, Buffer overflows, Sniffers</td>
</tr>
<tr>
<td>1998 - 2002</td>
<td>45</td>
<td>Windows Compromises</td>
<td>IIS Attacks</td>
</tr>
</tbody>
</table>
Conclusions

Attacks are Done for Money, Profit, and Gain.
Attacks Continue to Get More Sophisticated.
  - Difficult to Detect
  - Difficult to Analyze Tools
  - Faster Propagation
  - Tools not Publicly Available
End Users are More at Risk.
  - Shift in Focus from Server Attacks to People and Client-Side Attacks.
Attacks are Originating from Overseas.

Conclusions (Part Deux)

5. Wide Gap Between the Sophistication of Attack Tools vs. the Tools Used to Respond.
6. Attribution for Attacks is Getting More Difficult:
  - Fire and Forget
  - Malspreadbotwormkits
7. The Detection Mechanism that Triggers Incident Response Seems to be More Diverse …
Conclusions (Part Three)

Organizations are not Performing Effective Incident Response:
- Lack of Trained Resources
- Lack of Dedicated Resources
- Lack of Infrastructure to Compress Timeframe for Data Collection
- Lack of Trace Evidence …

Incident Detection
The State of the Hack

By Kevin Mandia

July 1, 2005
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
• What were the Circumstances Surrounding the Quarantine?
• Can you Access the Proprietary File Format to Perform Tool Analysis?

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

Holy_Father

We’re offering anti-detection service for any type of windows modules. There are many ways how to make your module undetected hence you can see below quite complicated price table with examples. To order this service write a mail with full description of what you need to holy_father@phreaker.net. I feel free to write a mail if you’re not sure how much would your order cost or if you have special demands (e.g. bypassing any detector that is not in list).

<table>
<thead>
<tr>
<th>feature</th>
<th>Morphone</th>
<th>Hacker defender</th>
<th>Hacker defender drivers</th>
<th>Other (no driver or libraries)</th>
<th>Libraries</th>
<th>Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic live</td>
<td>€ 30.00</td>
<td>€ 20.00</td>
<td>€ 15.00</td>
<td>€ 15.00</td>
<td>€ 15.00</td>
<td>€ 15.00</td>
</tr>
<tr>
<td>morphined1</td>
<td>x</td>
<td>+ € 25.00</td>
<td>x</td>
<td>+ € 25.00</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>morphined - unique3</td>
<td>x</td>
<td>+ € 25.00</td>
<td>x</td>
<td>+ € 25.00</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>per AV2</td>
<td>+ € 10.00</td>
<td>+ € 25.00</td>
<td>+ € 10.00</td>
<td>+ € 10.00</td>
<td>+ € 10.00</td>
<td>+ € 10.00</td>
</tr>
<tr>
<td>all AV2</td>
<td>x</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
</tr>
<tr>
<td>unique version4</td>
<td>+ € 20.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>source code</td>
<td>+ € 20.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
<td>+ € 25.00</td>
</tr>
<tr>
<td>no driver</td>
<td>x</td>
<td>+ € 10.00</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>special</td>
<td>x</td>
<td>special</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
How are Organization’s Detecting Incidents?

IDS Alerts?
Rare Detection Mechanism.

Port 22
Port 443
VPN

How are Organization’s Detecting Incidents?

Service Pack 2 Firewall Alerts?
Backdoors are Subverting the TCP/IP Stack.

Clients
More Often than Pro-Active Countermeasures.

Sensors Detecting Unusually High Levels of Network Activity.

End Users
Emerging as a Common Detection Mechanism.

digital self defense
How are End User’s Detecting Incidents?

System Crashes.

- Computer Hardware
- OS Kernel
- User Space

How are End User’s Detecting Incidents?

- 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.

digital self defense
How are End User’s Detecting Incidents?

Task Manager Fails to Operate Properly.

The Registry Editor (regedit) Closes Immediately When it is Invoked.

The Inability to Connect to www.nai.com, www.mcafee.com, or other Anti-Virus Web Sites. You are Redirected to Other Web Sites like www.google.com When you Attempt to Visit Antivirus Web Sites.

digital self defense
Case Studies
The State of the Hack

By Kevin Mandia
July 1, 2005

Attack Trends

End User Vulnerabilities
  Internet Explorer Attacks
  Phishing Schemes
  Brute Force Netbios Attacks

Automation
  Attribution May be More Difficult

More Kernel Level Attacks
  Less Effective Detection

digital self defense
### Incident Detected

In May of 2004, an employee of a consulting firm noticed that $20,000 had been transferred from her online banking account. She notified the financial institution, and the financial institution initiated a password change to protect the victim’s assets. An additional $20,000 was transferred out of the victim’s account within a day or so. The Victim’s user ID and Password were compromised on at least two occasions.

---

### Incident Details

<table>
<thead>
<tr>
<th>May 1</th>
<th>May 2</th>
<th>May 3</th>
<th>May 4</th>
<th>May 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Notified Credentials Changed</td>
<td>Bank Notified Credentials Changed</td>
<td>Bank Notified Credentials Changed</td>
<td>Bank Notified</td>
<td></td>
</tr>
</tbody>
</table>

---

*digital self defense*
Vulnerability? Server or Client-Side
Case Details

The Bank Did a Thorough Scrub of their Network. They Determined They Were not the Source of the Loss of the Victim’s Credentials.

So How Could the Victim Lose Her Credentials?

MS Vulnerabilities

With Leaked Source Code Many More Could be Found

digital self defense
Evidence

Review Application Event Log
   Anti-Virus Entries
   Dr. Watson Entries

Review Dr. Watson Logs

Review the File System for Known Malware:
   Norton’s anti-virus.
   EnTrust PestPatrol
   Sophos AV – 5.0.2.
   Microsoft’s Anti-Spyware (beta version).
   Ad-aware SE
   Execute Trend Micro – PC-Cillin

Review Web Browser History (Known Malicious Sites)

Phishing Scheme

digital self defense
Enticing Email Message

Dear Citibank Member,

This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the email number your Citibank ATM/Embank Card number and PIN that you use on ATM. This is done for your protection to prevent sharing of personal information.

To verify your e-mail address and access your bank account, click on the link below, then enter your username and password.

http://www.citibank.com/acs=p1Uq3027qcHw003nfuJ2@sd96v.pisem.net/3/?3X6CMW2I2uPOVQW

Thank you for using Citibank!

http://www.securityfocus.com/infocus/1745

Malicious Web Sites

http://www.citibank.com/acs=p1Uq3027qcHw003nfuJ2@sd96v.pisem.net/3/?3X6CMW2i2uPOVQW

www.citibank.com Username
ac=p1Uq3027qcHw003nfuJ2 Password
sd96v.pisem.net Destination Server

digital self defense
Evidence

Review the Web Browser History.
Focus on “POST” Operations
Review the Browser Cache.
Interview the Individual.

Forensic Analysis of the Victim’s PC

digital self defense
Data Analysis

Noticed a suspicious file within 5 minutes of examination …

On April 30, 2004 at 8:45:40AM, the file “sdsini.ini” was created. This text file was a keystroke capture log file.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>File Created</th>
<th>Entry Modified</th>
<th>Logical Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:WINDS:sdsini.ini</td>
<td>09:13:20AM</td>
<td>09:13:20AM</td>
<td>08:45:40AM</td>
<td>05:27:04</td>
<td>48.188 bytes</td>
<td>000000000000</td>
</tr>
</tbody>
</table>

Due to the location of the keystroke capture log files in the “C:\Windows” system file area and the fact that they were named with a “.ini” file extension:

The Windows operating system considered each keystroke capture log file a system file.

Therefore, analysis of the Microsoft System Restore Points could be useful.
Data Collection

<table>
<thead>
<tr>
<th>Partition Code</th>
<th>Type</th>
<th>Start Sector</th>
<th>Total Sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE</td>
<td>DELL</td>
<td>0</td>
<td>64260</td>
<td>31.4MB</td>
</tr>
<tr>
<td>07</td>
<td>NTFS</td>
<td>64260</td>
<td>80212545</td>
<td>38.2GB</td>
</tr>
</tbody>
</table>

Data Analysis

Reviewed time/date stamps around the time of the unlawful withdrawal of money.
We had a target date as a clue ...
Data Analysis

Noticed a suspicious file within 5 minutes of examination …

On April 30, 2004 at 8:45:40AM, the file “sdsini.ini” was created. This text file was a keystroke capture log file.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>File Created</th>
<th>Entry Modified</th>
<th>Logical Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\WINDOWS\sdsini.ini</td>
<td>09:13:20AM</td>
<td>09:13:20AM</td>
<td>08:45:40AM</td>
<td>09:13:20AM</td>
<td>48.188</td>
<td>210eb2450a20a3f8</td>
</tr>
</tbody>
</table>

Data Analysis

Due to the location of the keystroke capture log files in the “C:\Windows” system file area and the fact that they were named with a “.ini” file extension:

- The Windows operating system considered each keystroke capture log file a system file.

Therefore, analysis of the Microsoft System Restore Points could be useful.
System Restore is a component of Windows XP which allows a user to restore a computer to a previous state, in case a system problem is encountered.

System Restore monitors changes to system files, automatically creating restore points. These restore points, or snapshots, are created daily, at other significant times, or when a user specifically creates one.
Data Analysis

Examination of the restore folder, C:\System Volume Information\_restore\{62906183-4CC4-4211-9E5C-0D91ECCC7AE7}\, resulted in identification of 25 files containing keystroke logs totaling approximately 400 pages of content.

How the Exploit Occurred

On April 29, 2004 at 6:17:33PM, the Windows diagnostic utility Dr. Watson recorded an “access violation” in Internet Explorer.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>File Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp</td>
<td>05/27/04 08:47:57AM</td>
<td>04/29/04 06:17:33PM</td>
<td>04/29/04 06:17:33PM</td>
</tr>
<tr>
<td>C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log</td>
<td>05/27/04 08:47:57AM</td>
<td>04/29/04 06:17:33PM</td>
<td>04/29/04 06:17:33PM</td>
</tr>
</tbody>
</table>
How the Exploit Occurred

An “access violation” occurs when a process attempts to access memory already in use by another application.

While not conclusive, this is an indication of possible malicious activity.

How the Exploit Occurred

A portion of the user.dmp file indicated the error was generated while the user of the victim system visited the INBOX mail folder at the URL http://logicmail.logic.bm.

GET/data10.php?info=reply\_how=qreply&reply.x=42&passed=multi&variable=CvCsPzqsTvC@QyqmXvShN04apvCDPzScs%3B6aI%3BpYi8FPN8FTsd&variable2=&add2folder=&add2folder\_top=LOGICMAIL - Read Message - Microsoft Internet Explorer

http://logicmail.logic.bm\/emumail.cgi?folder=INBOX&passed=msg&variable=CvCsPzqsTvC%40QyqmXvShN04apvCDPzScs%3b6al%3bpYi8FPN8FTsd
&user=[441254946882509892][xxxx] HTTP/1.1
User-Agent: A-311
Host: www.xxx.xxx.xxx.xxx
Connection: Keep-Alive
How the Exploit Occurred

On April 29, 2004 at 06:13:07PM, the user of Victim Workstation was accessing her Online Mail account:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>File Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Documents and Settings\xxxxxxxx\Local Settings\Temporary Internet Files\Content.IE5\I7W2BAD\emumail[1].htm</td>
<td>05/27/04</td>
<td>04/29/04</td>
<td>04/29/04</td>
</tr>
<tr>
<td></td>
<td>08:48:22AM</td>
<td>06:13:07PM</td>
<td>06:13:07PM</td>
</tr>
</tbody>
</table>

Conclusions

The Trojan performed targeted collection involving keystroke logging to capture credit card numbers, URLs, userids, and passwords. These keystroke logs were periodically sent to an email server in Europe.

The Trojan uninstalled itself after approximately two weeks of collection, removing its executable components, registry entries, and the keystroke capture log files.
**Trojan Name:** MultiDropper-GP  
**Risk Assessment:**  
- Corporate User: Low  
- Home User: Low

**Symptoms**  
New files dropped on the target machine

**Method Of Infection**  
This multidropper trojan serves only to drop and execute other files on the target system. It does not self-replicate. Likely distribution channels for this trojan include: via IRC, via peer-to-peer file-sharing networks, as an attachment in newsgroup postings or email, etc. The file is likely to be named in order to entice the victim to run it (eg. NEW_YEAR.EXE)

Trojans may also be received as a result of poor security practices (weak username/password combination on open shares, lack of or misconfigured firewall protection), or unpatched and vulnerable systems.

---

27 August 2004  
**Trojan targets users of British online banks, Sophos warns of latest phishing attack**

Experts at Sophos have warned British computer users who bank online about a series of Trojan horses that try and steal financial information.

The Trojan Trojan horses target users of a number of online banks, including Abbey, Barclays, Cahoot, HSBC, Lloyds, NatWest, Nationwide, and Woolwich.

Running in the background, the Trojan monitors which websites are being visited — and if it recognises an online banking website it secretly captures keystrokes and takes snapshots of what is displayed on the monitor.

The information is then sent back to the remote hackers, who can use the captured data to break into bank accounts and steal money.

“This is very different from the fraudulent emails which many computer users receive everyday, trying to lure you to a bogus website. This Trojan waits for the customer to visit the real banking website, and then it captures passwords and account information making robbery a breeze,” said Graham Cluley, senior technology consultant for Sophos. “Home users and businesses large and small need to protect themselves with up-to-date anti-virus software and take extreme care to ensure their computers are kept free from Trojans like Trojan and other malware.”

Sophos recommends companies protect their email with a consolidated solution to thwart the virus and spam threats as well as secure their desktops and servers with automatically updated anti-virus protection.
A Report from the Trenches

Responding to a Zero Day Exploit

Investigation

Details from Victim Organization:
- Initial Detection by a system crash.
- Key systems compromised.
- Rogue SSH use detected.
- Attacker using Valid Credentials.
- Found two programs on the crashed system that looked suspicious.

Goals of Investigation:
- Return to Secured State
- Minimize downtime
- Maintain low profile – no disclosure or leaks
- Determine Initial Point of Entry
- Determine Damage/Data Loss

digital self defense
Data Collection

Attacker was using a kernel level tool. This required us to use Knoppix boot CDs to acquire the evidence we needed. Only 4-6 forensic duplications were made of known victim systems to attain an attack signature. 11 of 18 servers compromised.

Apache Error Logs

[Sat Jul 12 23:44:26 2004] [error] [client xxx.xxx.xxx.xxx] client denied by server configuration: /webtree
[Sat Jul 12 23:45:16 2004] [notice] child pid 15831 exit signal Segmentation fault (11)
[Sat Jul 12 23:45:16 2004] [notice] child pid 15830 exit signal Segmentation fault (11)
[Sat Jul 12 23:45:17 2004] [notice] child pid 10419 exit signal Segmentation fault (11)
### Finding Intruder’s History File

<table>
<thead>
<tr>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Written</th>
<th>Last Accessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/local/scripts/.bash_history</td>
<td>07/12/04 11:50:46PM</td>
<td>07/12/04 11:50:46PM</td>
<td>07/24/04 06:25:17PM</td>
</tr>
<tr>
<td>/var/lib/X49/sk</td>
<td>07/12/04 11:53:59PM</td>
<td>07/12/04 11:53:59PM</td>
<td>07/24/04 05:48:54PM</td>
</tr>
<tr>
<td>/sbin/mingetty</td>
<td>07/12/04 11:53:59PM</td>
<td>07/12/04 11:53:59PM</td>
<td>07/24/04 05:48:54PM</td>
</tr>
<tr>
<td>/sbin/mingettyX49</td>
<td>07/12/04 11:53:59PM</td>
<td>07/12/04 11:53:59PM</td>
<td>07/12/04 11:53:59PM</td>
</tr>
</tbody>
</table>

### Victim System History File

The following lines were found in victim system’s /usr/local/scripts/.bash_history

```
uname -a; id; w; exit
```
OpenSSLTooOpen

The Following Fragment of Code is From the Publicly Available and Widely Used Exploit Designed by Solar Eclipse. It is available at:

http://www.phreedom.org/solar/exploits/apache-

/* commands run automatically by the shell */
#define COMMAND1 "TERM=xterm; export TERM=xterm; exec bash -i"
#define COMMAND2 "uname -a; id; w;"

Intrusion Tools

/var/lib/X49/sk
Encrypted /dev/kmem ROOT KIT
Confirmed to be the SucKIT installation utility
  • SucKIT v2.0-devel-rc2 <http://hysteria.sk/sd/sk>
Password Protected
  • “Go away with that, poor boy!”
Hides Process IDs and files
Implements “Backdoors”
Inserts “parasite code”
Defeats traditional memory capture and forensic examination techniques

digital self defense
SucKIT

SucKIT v2.0-devel-rc2 <http://hysteria.sk/sd/sk>
(c) Copyright 2001-2003 sd <sd@hysteria.sk>
Use: ./sk [C|u|i|s|x|h|v|b|l] <arg1> [argN]
C..................configure
u..................uninstall
i..................install
s..................install silently
x..................make current box suckit-ed
h <pid>............make pid invisible
v <pid>............make pid visible
b <filename>.......insert parasite code
l <host[:port]>....login to remote host

in <> is required options, [] are optional
see doc/MANUAL for commands reference

Performing Live Response

July 1, 2005

Red Cliff
Intelligent Information Security

digital self defense
Goal of Today’s Backdoor

- Initiated on the Client-Side.
- Foil the Security Aspects of Network Address Translation.
- Bypass Firewall Rulesets.
- Encrypted Channels.
- Loss of Exfiltration Data
- Difficult to Determine Capability, Purpose of an Attack.
- Rely on Port Redirection
  - Foils Network Based Detection (Innocuous IPs).
  - Obfuscates True Origin of Connection.
  - Complicates Attribution.
- Command and Control
- Kernel/Driver Level.
  - Thwart Detection via Live System Review or Anti-Virus.
- Self Propagate or Install?

What Are These Backdoors?

The Review of 54 Malicious Executable Files in a recent case:
- Wide Variety of Tools With Widespread Purpose.
  - 29 / 54 Files Reviewed were not Publicly Available
  - 44 / 54 Files Reviewed were not Detected by AV
  - 10 / 54 Files Reviewed were Packed via 4 Different Methods
- Size of Toolkits is Large.
  - 85 Unique Tools.

*digital self defense*
Goals for Responder

Determine the Host-Based signatures of the malware.
Determine the network-based signatures of the attack.
Review What Data may have been Compromised.
Minimize Undue business Disruption and Loss.
Quickly Confirm or Dispel if Trigger is for a Real Incident.

Incident is Detected

Incident Detected on Host 1
Corporate Network
Backdoor Channel
Internal Propagation

Internet

Pharmaceutical - 2004
digital self defense
Incident is Detected

IT Staff at the Hosting Site Receive an Anti-Virus Alert.
System Contained Private/Sensitive Client Data.
Was this Sensitive Data Accessed by Attackers?

Unschooled Approach
Performed wanton live review of the system.

Performing Live Response

1. Last Accessed Time of Files
2. Last Written Time of Files
3. Creation Time of Files
4. Volatile Information
5. Services Running
6. Event Logs
7. Registry Entries
8. Host Status (Uptime, Patch Level)
9. IIS and Other Application Logs

Live Data Collection Performed to Verify Incident and Determine Indicators / Signature of the Attack
Performing Live Response –
Suspected Incident

Obtain the Registry
regdump
Obtain the Event Log Files
pslogist
Obtain a List of Running Services
psservice
Obtain the Patch Level
psinfo
Obtain a List of Valid Credentials
pwdump

Performing Live Response

echo permissions;access date;access time;modification date;modification time;change date;change time;user ownership;group ownership;file size;file name

for %%d in (c d e f g h i j k l m n o p q r s t u v w x y z) do IF EXIST %%d:\ %IRPATH%\find %%d:/ -printf "%%m;%%Ax;%%AT;%%Tx;%%TT;%%Cx;%%CT;%%U;%%G;%%s;%%p\n"

digital self defense
Determine Signature of Attack

Incident Detected on Host 1

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/18/2001</td>
<td>07:52</td>
<td>&lt;DIR&gt;</td>
<td>..</td>
</tr>
<tr>
<td>10/18/2001</td>
<td>07:52</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>04/23/2003</td>
<td>03:17</td>
<td>&lt;DIR&gt;</td>
<td>TEMP2</td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:29</td>
<td>&lt;DIR&gt;</td>
<td>psexec.exe</td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:30</td>
<td>&lt;DIR&gt;</td>
<td>nbtenum.exe</td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:31</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:51</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:52</td>
<td>&lt;DIR&gt;</td>
<td>arod2wbt1.rar</td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:56</td>
<td>&lt;DIR&gt;</td>
<td>AROD2W</td>
</tr>
<tr>
<td>04/23/2003</td>
<td>03:18</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>04/23/2003</td>
<td>03:18</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>10/18/2001</td>
<td>07:52</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>10/18/2001</td>
<td>07:52</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>04/23/2003</td>
<td>03:17</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>04/23/2003</td>
<td>03:18</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:29</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:30</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/13/2003</td>
<td>12:31</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:51</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:52</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>05/20/2003</td>
<td>10:56</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Respond on Host 1

Signature of Current Attacker Identified!!

Gathering Live Data

Respond on Host 1

Respond on Host 2

Respond on Host 3

Respond on Host 4

Respond on Host X

Search for Signature of Current Attacker on Other Hosts.

digital self defense
Evidence - psloggedon

PsLoggedOn v1.21 - Logon Session Display
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
6/5/2003 2:12:04 PM    NAMERICA\BMcNabb
6/4/2003 9:13:54 AM    NAMERICA\AdminSQL
4/9/2003 10:18:46 AM    NAMERICA\KPI1
5/13/2003 12:26:24 PM    USKP01\Guest

Evidence: Netstat

Review the netstat Output for:
- Unknown/Suspicious IP Addresses Connecting to the Victim System.
- Suspicious Ports Listening for Connections.

digital self defense
Evidence: PSLIST

Review the \texttt{pslist} Output for:
Running Processes with Suspicious Names
- buttsniff
- 1234.exe
- Dsniff

You Normally Identify a Backdoor or Rogue Process by Examining \texttt{fport} or \texttt{netstat} Output.

The \texttt{pslist} output will show you how long the rogue process had been executing.

\texttt{PSLIST} Cannot Distinguish Which Services a SVCHOST.EXE is Listening on Behalf of.
Evidence: Fport

Review the fport Output for:
Open Ports that Should Not be Open.
Any Listening Application that You are Unfamiliar with.

Most Valid Applications that Open Ports are Located in the “Winnt” or the “winnt\system32” Directory.

Does Not Appear to Work With Windows XP

FPORT Cannot Report the Full Path Name for Any Application Installed as a Windows Service.

Digital self defense
Openports

```
C:\>openports

A full text version of the openports data can be found at http://www.digimondo.com/openports/
```

```
77 78
openports
```

digital self defense

```
tasklist /SVC

C:\>tasklist /svc

<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>System</td>
<td>520</td>
<td>N/A</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>884</td>
<td>N/A</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>8188</td>
<td>N/A, PolicyAgent, ProtectedStorage, Sams</td>
</tr>
<tr>
<td>lsass.exe</td>
<td>1042</td>
<td>IISManager, TermService</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1152</td>
<td>N/A, Audiosrv, Browser, CryptSvc, Dnp, dsnserver,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet, print, FastUserSwitchingCompatibility, helpsvc,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HelpZ, lanmanserver, lanmanworkstation, Metz, Nis, Ntp, Snmp, Schedule, sslsoap,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D3D9, SharedMmoire, ShellNtNotification,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>spservice, syslog, Themes, tcpmks, W32Time,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>winms, wncac, wns, win32ehci, vcsync</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1256</td>
<td>N/A</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1362</td>
<td>N/A, RemoteRegistry, SMBFS, WebClient</td>
</tr>
<tr>
<td>BSNP CoD:</td>
<td>1720</td>
<td>N/A, Print Service</td>
</tr>
<tr>
<td>EXE:</td>
<td>1792</td>
<td>N/A</td>
</tr>
</tbody>
</table>
```
Evidence - Regdump

Review the MRU Files
- Last Opened Files
- Last Searches
- Last Commands Executed (Start-> Run)

Review the Startup Registry Keys

Review the Full Path of Applications Executed when A Windows Service is Initiated

evidence - psservice

SERVICE_NAME: mediadriver
DISPLAY_NAME: Microsoft Windows Mediaplayer
(null)

  TYPE : 10 WIN32_OWN_PROCESS
  STATE : 1 STOPPED

  (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

  WIN32_EXIT_CODE  : 0 (0x0)
  SERVICE_EXIT_CODE : 0 (0x0)
  CHECKPOINT  : 0x0
  WAIT_HINT : 0x0
Evidence - RegDump

mediadriver
Type = REG_DWORD 0x00000010
Start = REG_DWORD 0x00000002
ErrorControl = REG_DWORD 0x00000000
ImagePath = REG_EXPAND_SZ
C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll\svrany.exe
DisplayName = Microsoft Windows Mediaplayer
ObjectName = LocalSystem
Parameters
  Application = C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll\ioFTPD.exe
  AppDirectory = C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll
  Security [17 1]

Evidence - psservice

SERVICE_NAME: ZGBPool
DISPLAY_NAME: ZGBPool
 (null)
  TYPE : 10 WIN32_OWN_PROCESS
  STATE : 1 STOPPED

  (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
  WIN32_EXIT_CODE : 1077 (0x435)
  SERVICE_EXIT_CODE : 0 (0x0)
  CHECKPOINT : 0x0
  WAIT_HINT : 0x0
Evidence - regdump

ZGBPool

Type = REG_DWORD 0x00000010
Start = REG_DWORD 0x00000004
ErrorControl = REG_DWORD 0x00000001
ImagePath = REG_EXPAND_SZ X:\WINNT\srvany.exe
DisplayName = ZGBPool
ObjectName = LocalSystem
Parameters
  Application = x:\winnt\system32\drivers\disdn\temp2\zgbbot\mirc.exe
  AppParameters =
  AppDirectory = x:\winnt\system32\drivers\disdn\temp2\zgbbot
Security [17 1]
  Security = REG_BINARY 0x00000B8 0x80140001
  0x000000a0 0x0000000c 0x00000014 0x00000030 0x001c0002 0x00000014 0x00148002
  0x000f01ff 0x00000101 0x01000000 0x00000000 0x00700002
  0x00000004 0x00180000 0x000201fd 0x00000101 0x00500000 0x00000012

Obtaining the Event Logs

psloglist –s –x security
psloglist –s –x application
psloglist –s –x system

digital self defense
Evidence: The Event Logs

Application Log
- Anti-Virus Records.
- SQL Server Records.

System Log
- Starting and Stopping (Crashing) of the Web Server.

Security Log
- Brute Force Netbios Connections.
- Access to Files (when auditing file access).
- Policy Changes.
- Logins and Logouts.

Detection – Application Log

005, Application, Norton AntiVirus, ERROR, XXX-XX, Mon Feb 21 18:15:44 2005, 5, None, Virus Found! Virus name: Trojan Horse in File: C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\com1\bon gthom\service2.bat by: Realtime Protection scan. Action: Clean failed: Quarantine failed: Access denied

003, Application, Norton AntiVirus, ERROR, XXX-XX, Mon Feb 21 18:04:47 2005, 5, None, Virus Found! Virus name: Trojan Horse in File: C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll\ioselbst .bat by: Realtime Protection scan. Action: Clean failed: Quarantine succeeded: Access denied
Detection – Application Log

202, Application, DNTUS26, INFORMATION, T
SERVER, Thu May 01 00:32:53
2003, 0, None, DameWare NT Utilities
2.6 Last Error: 0 The following
user has connected via remote
console. User: Dentadmin From:
NET-UK03

evidence – security event log

5/25/03 4:58:51 PM 8 7 632 ...
5/25/03 4:58:51 PM 8 7 624 ...
5/25/03 4:58:51 PM 8 7 636 ...
5/25/03 4:58:51 PM 8 7 642 ...
5/25/03 4:58:51 PM 8 7 642 ...
5/25/03 4:58:51 PM 8 7 642 ...
5/25/03 4:58:51 PM 8 7 632 ...
5/25/03 4:58:51 PM 8 7 624 ...
5/25/03 4:58:51 PM 8 7 642 ...
5/25/03 4:58:51 PM 8 7 642 ...
5/25/03 4:58:51 PM 8 7 636 ...
5/25/03 4:58:51 PM 8 7 642 ...

digital self defense
Reviewing the Security Event Log

Review the Security Log for the Following
- User accounts being used during anomalous hours.
- User accounts logging in from improper systems.
- User accounts logging onto a system that the account should not require access to.
- A large number of failed logons, implying brute force logon attacks.
- Suspicious password changes.

Determine if Process Tracking is Turned on.

Specifically, review the following event types for review:
- Event ID 528 – Successful Logons
- Event ID 529 – Failed Logons
- Event ID 538 – Successful Logoffs
- Event ID 540 – Successful Network Logons
- Event ID 592 – Process Started
- Event ID 627 – Password Changes
- Event ID 681 – Failed Remote Logons

Reviewing the Application Event Log

Review the Anti Virus alerts:
- Type 2 – Records When Scans were Executed.
- Type 5 – Virus Found Record.
- Type 6 – Permission Failures during AV Scans
- Type 7 – New Virus Definition Loaded
- Type 16 – Virus Definitions are Current

Review all Dr Watson Creations
Review all Winlogon Errors.
Detection - pwdump

Administrator:500:******************************************************************************
Guest:501:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB90262B43:Built-in account for guest access to the computer/domain:
DERINGER$:1000:48F8334424A899986B212F1369F32900:730BB14FD775BE4C67B6EDAC7F03B4:
IUSB_DERINGER:1001:1319783F0C685626D4791CFCB8AB4707:APCFCE010F830AAE265E3A10A345BAD:
bob:1004:4318B176C3D8E3DEAAD3B435B51404EE:B7C899154197E8A2A33121D76A240AB5:Bob::
spiderman:1005:98CC13F72447D06CAAD3B435B51404EE:ACC5E857C583A07E40A7AE83792CC45:Peter Parker::
MAUSER1$:1008:D22507430A62B283AAD3B435B51404EE:4167BCD8F39697A3ABC76617094F396F:
HelpDesk:1009:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB90262B43:
HelpAssistant:1010:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB90262B43::

Detection - pwdump

Administrator:500:NO PASSWORD******************************************************************************:
Guest:501:21E4A6AFB7A1F4891AFD45894F5366B5:62B58FCADA68058B6D725F257834D241:
TsInternetUser:1000:21E4A6AFB7A1F4891AFD45894F5366B5:62B58FCADA68058B6D725F257834D241::

digital self defense
A Flurry of Recent Attacks Demonstrates that Attackers are Turning Off Windows Audit Policies and Deleting the Security Event Log.

Intent / Purpose / Goals

Host-Based Evidence is Usually Severely Limited.
- Dr. Watson Logs
- PageFile
- Unallocated Space

Often Network Security Monitoring is Needed to Assist in Determining Intent, Purpose, and Goals.
**Dr Watson Log**

**ABC.exe = sniffer from xfocus.org (Chinese site). “Sniffing TCP PASSWORD”**

01ece77c 0d 0a 43 3a 5c 57 49 4e - 73 74 65 69 6e 67 20 74 6f 20 3c 67 6f 72 20 77 69 6e 32 - 30 30 0d 0d 0a 43 6f 64 65 20 62 79 20 67 6c 61 63 69 65 72 40 78 66 6f 63 75 73 2e 6f 72 67 0d 0d 0a 0d 0d 0a 53 6e 69 66 69 6e 67 20 54 43 50 20 50 41 53 53 70 44 20 2e 2e 2e 0d 0d 0a 3c 43 74 72 6c 2d 43 3e 20 74 6f 20 71 75 69 74 0d 0d 0a 0d 0a 49 6f 63 74 6c 20 45 72 72 6f 72 3a 20 31 30

**SQL Commands used to execute:**

**Xp_cmdshell dir**

530def44 70 3d 89 00 01 01 00 44 - 00 00 01 00 45 00 58 00 p=....D....E.X.
530def54 45 00 43 00 20 00 6d 00 - 61 00 73 00 74 00 65 00 E.C..m.a.s.t.e.
530def64 72 00 00 2e 00 0e 00 78 00 - 70 00 5f 00 63 00 6d 00 r....x.p....c.m.
530def74 64 00 73 00 68 00 65 00 - 6c 00 6c 00 20 00 22 00 d.sh.e.l.l.
530def84 64 00 69 00 72 00 22 00 - 92 00 04 00 09 00 d.i.r.********
dr watson log

sql commands used to execute:
xp_cmdshell echo bye >> c:\winnt\system32\ftp3.txt

97

digital self defense
The Future is Now

Responding to SpreadSploit Malbotworms

Challenges to Current Response Methods

Even When an Organization has Pre-Made Toolkits and a Plan:
Live Response Can Be Very Time Consuming
Responder Usually is Challenged to Recognize Anomalies
Response Tools are Most Often User Space
   Attack Tools are Migrating to Kernel Space
What Windows Rootkits Do

- Hide Files and Directories
- Hide Processes
- Hide Registry Entries
- Prevent Deletion of Files
- Prevent Anti-Virus from Executing
List Goes On …

Vanquish

digital self defense
digital self defense
Vanquish

AFX

digital self defense
digital self defense
RootKit Revealers to the Rescue

www.sysinternals.com
Interprets File System Discrepancies
Interprets Registry Discrepancies
Command Line as well as GUI Tool
Can be Executed Remotely Using PSEXEC
RootKit or Other Emerging Revealers Must be Incorporated into your Response Toolkits
Contact Information

Kevin Mandia
President

1285 Avenue of the Americas - 35th Floor
New York, NY 10019
www.red-cliff.com

Kevin.Mandia@red-cliff.com