

How the Federal Government can apply lessons learned from the private sector

By Kevin Mandia

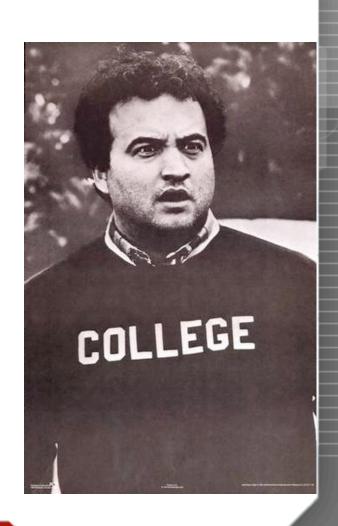
## Why Are We Here?

- Every Major Organization has been Exploited by Attackers.
- All Outsourced Software is Being Made with Backdoors.
- Every Developed Nation is Creating
   Cyber-Warfare Capabilities.
- Firewalls, IDS, and Antivirus are not Abolishing the Security Problem.
- There are Hundreds of Non-Publicly Available Exploits in use Right Now.



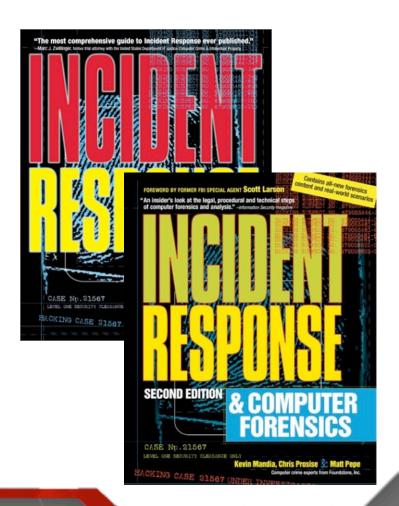
# Agenda

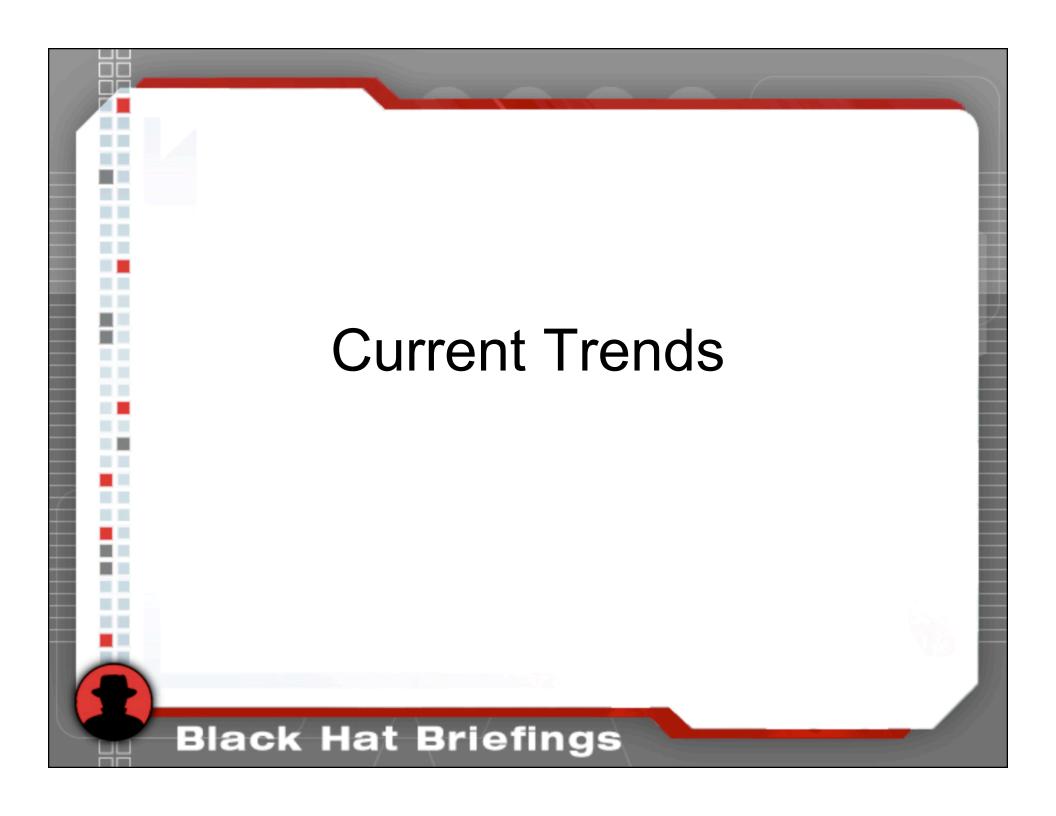
- Current Incident Response Trends
- Incident Detection
- Case Studies / Attack
   Trends
- The Future of Incident Response



#### Who Are We?







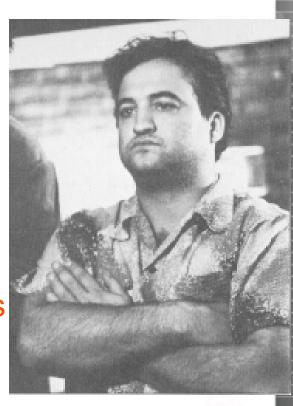
#### Who We Are

- Last 3 Years
  - Responded to over 215 Potentially Compromised Systems.
- What Are Some Things I Learned About the Current Attack Trends?



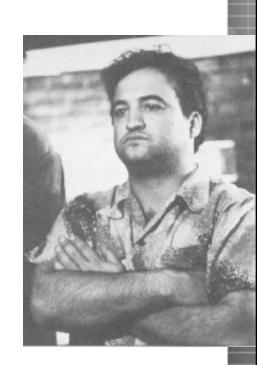
#### Conclusions

- Verified that 103 were Compromised.
- 2. Determined Known Mode of Entry for Approx 32 Systems.
  - Too Much Time Elapsed.
  - Poor Host-Based Accounting
  - No Network Device Records of Merit
- 3. Concern for Reporting Requirements
- 4. Managers Desire Diligence = Process



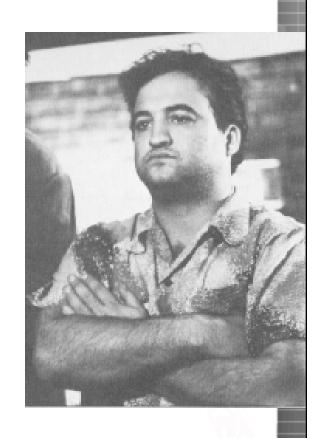
### Conclusions

- 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
- 7. End Users are More at Risk.
  - Shift in Focus from Server Attacks to People and Client-Side Attacks.
- 8. Attacks are Originating from Overseas.



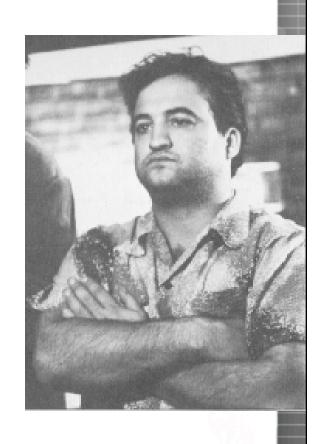
### Conclusions

- Wide Gap Between the Sophistication of Attack Tools vs. the Tools Used to Respond.
- 10. Attribution for Attacks is Getting More Difficult:
  - Fire and ForgetMalspreadbotwormkits
- 11. The Detection Mechanism that Triggers Incident Response Seems to be More Diverse ...



#### **Tech Conclusions**

- 12. Need to Acquire Physical RAM is Increasing
- Attacker's Toolkit is Commonly Armored in Some Capacity
- 14. The Need to Perform Adequate Malware Analysis is Growing
  - Needed for Host-Based and Network Based Indicators of Attack
- 15. Network Monitoring is Still a Critical Method for Determining the Scope of Compromise



#### Attacks Trends

- Attacks Against End Users Remain the Dominant Attack Against the Financial Services
  - Motivation: \$\$\$
  - Spear-Phishing
  - Browser Vulnerabilities
- Most Attacks Still Rely on User Interaction

#### Parsers are Under Attack...

- Many Recent Vulnerabilities are Against Parsers for Binary Files
  - A JPG that can root your box?
  - PNG, JPEG, GIF, Icons
  - Microsoft has standard libraries for parsing these formats, any program that uses those libraries is vulnerable
- File Format "fuzzers" are Available and Will be Popular Amongst Attackers until these Bugs are Exhausted

### The Kernel is Being Assaulted...

- Several years ago discussions involving hacking and the kernel was focused on LKMs
- Researchers are becoming more sophisticated in their ability to find and exploit kernel flaws
- Every driver on your system is a potential entry point for malicious code
- Consider a USB stick that can root any box it is inserted into by exploiting some vulnerability in the USB driver

#### Rootkits are the New Hotness

- New Rootkit detection/protection products from:
  - F-secure, Microsoft, SysInternals
- Brilliant Hacker Defender Forever is \$1100
- Sony (XCP) vs. Mark Russinovich
- Hoglund and Butler's book makes Windows rootkits more accessible

# Everything Runs over Http(s)

- Configuring Firewalls is Hard
- Especially in NAT'ed Environments
- More and More Technologies are Simply Tunneling
  - RPC over HTTP(S)
  - Sprint PCS business connection
  - Microsoft Remote Help
  - Deep Inspection is Increasingly Important

## **Exploitation Frameworks**

- Exploitation frameworks (free and commercial) are constantly improving
- Point → Click → Root
- Sophistication of Payloads is Increasing butKnowledge Required is Decreasing
- Memory-only exploitation has raised the bar for effective forensic response
- CORE Impact, Metasploit, CANVAS

# Rooting Routers

- Mike Lynn caused a big splash at BlackHat
- Consider the implications of a stealthy attacker owning your border
- A router is a computer
- In fact, a switch is a computer

# The SANS Top 20 for 2005 (Windows)

- 1. Windows Services (11 critical updates)
- 2. Internet Explorer (10 updates)
- 3. Windows Libraries (11 critical updates)
- 4. Microsoft Office (3 critical updates)
- 5. Windows Configuration
  - ❖ Policy problems... sa/blank, etc...

# Case Study 1 Need to Acquire Physical Memory **Black Hat Briefings**

#### **Initial Detection**

- Victim Organization the Target of a Persistent,
   Ongoing Attack
- Victim Forwards Signature of Attacks to Anti-Virus Vendor.
- In August Anti-Virus triggers on Unique Signature.
- Administrator Responds and Notices the Following File:
  - c:\XXX\XXX\X.EXE
- Administrator Leaves System On but Takes it off the Network.



- We Dumped Memory Space for Rogue Processes.
- We Dumped Entire 1 GB of Ram.

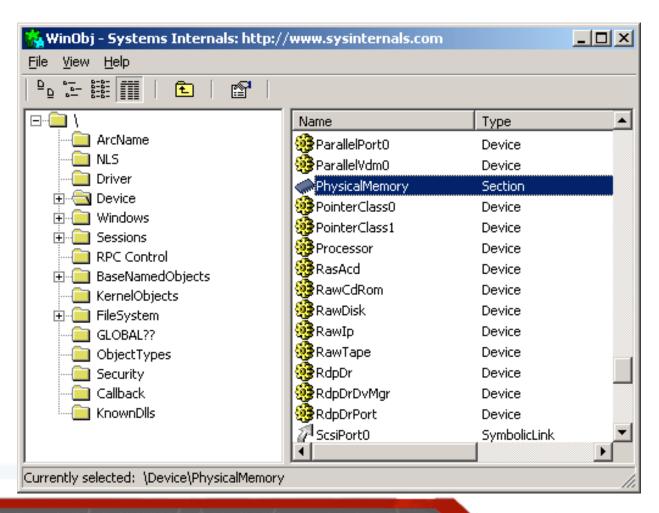
# **Obtaining Ram**

- Mr. George M. Garner, Jr. modified dd, along with several other useful utilities, specifically for forensic investigation on Windows.
- Enhancements include correction of several Windows compatibility issues, built-in md5sum, compression and logging abilities, to name a few.
- http://users.erols.com/gmgarner/forensics.
- Some of Mr. Garner's utilities are based on the UnxUtils distribution, available at http://unxutils.sourceforge.net.

# /Device/PhysicalMemory

- By using the /dev/mem file on Unix systems, we can obtain the contents of physical memory from a live Unix operating system.
- Unfortunately, Windows operating systems do not provide such a file object, but they do (since NT) have a /Device/PhysicalMemory section object.

# /Device/PhysicalMemory

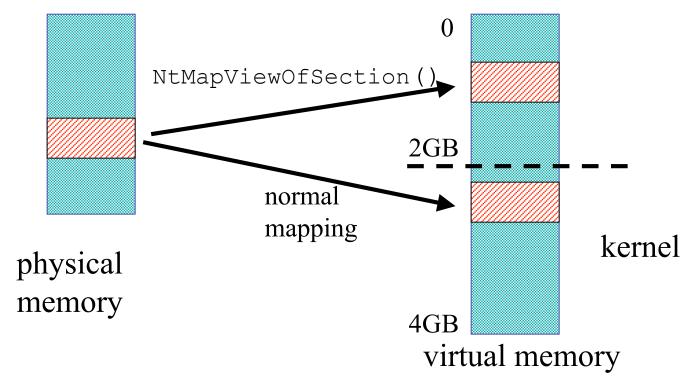


# /Device/PhysicalMemory

- A section object, also called a file-mapping object, represents a block of memory that two or more processes can share.
- Section objects can be mapped to a page file or other on-disk file.
- The first use of this section object for viewing physical memory, that we are aware of, was by Mark Russinovich when he created the Physical Memory Viewer, physmem. (<a href="http://www.sysinternals.com/ntw2k/info/tips.shtml#KMem">http://www.sysinternals.com/ntw2k/info/tips.shtml#KMem</a>
   m)
- By mapping the /Device/PhysicalMemory section object to virtual address space, Mr. Garner's version of dd can save this data out to generate dump representing physical memory.



- NtOpenSection() gives us a handle
  - NtMapViewOfSection() maps a section of physical memory into the current process





#### E:\>dd.exe if=\\.\physicalmemory of=z:\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=z:\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

# Forensic Acquisition of Process Memory

- Besides the pagefile and complete system memory contents, the third type of memory you can collect is memory from individual processes
- Especially useful in responding to intrusion incidents where one or more processes are still running
- Process memory has often proved to be a quick way to determine what is happening

# Why Obtain Process Memory?

- By obtaining a memory dump of the suspect application, we can confirm
  - What the application really is,
  - The command line used to launch the application,
  - View the application's data stored in memory, and
  - Potentially commands executed or spawned

## userdump

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, including capture of multiple processes on a single command line and displaying running processes.
- E:\>userdump 744 Z:\svchost\_PID744.dmp
  - **User Mode Process Dumper (Version 3.0)**
- Copyright (c) 1999 Microsoft Corp. All rights reserved.
- Dumping process 744 (svchost .exe) to
- Z:\svchost PID744.dmp...
- The process was dumped successfully.

# Examining the dumpfile

 Now that we have the dump file, we can examine it with dumpchk.exe, a utility provided as part of the Debugging Tools for Windows package available at

http://www.microsoft.com/whdc/devtools/debugging/default.mspx .

- Dumpchk is intended to validate a dump file, but it also gives us some useful information like the original COMMAND LINE.
- The most common tool used for examining dump files is Windbg, part of the Debugging Tools for Windows package.
- Several of the utilities distributed as part of this package will require the symbols from the Windows operating system that was the source of the memory dump.
- These symbols, and information on their use, are available at <a href="http://www.microsoft.com/ddk/debugging/symbols.asp">http://www.microsoft.com/ddk/debugging/symbols.asp</a>.

### Significant Findings

Scope of Compromise

HOSTNAME	IP Address	Status	Comments
XXX	XXX	Compromised	Found Malware on the System.
XXX	XXX	Compromised	Directory Listing of D:\Lotus\Domino\Data
XXX	XXX	Compromised	Directory Listing of the Documents and Settings Folder.
XXX	XXX	Compromised	Directory Listing on XXX.
XXX	XXX	Compromised	Created Files on System from XXXX.
XXX	XXX	Potentially Compromised	Attempted Net Use to IPC\$



# Demonstration – Ram Dump and Review

# Case Study 2 The Need for Malware Analysis **Black Hat Briefings**

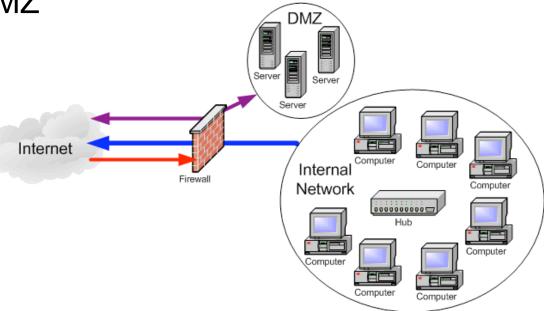
# Demonstration - Malware Analysis **Black Hat Briefings**

# Case Study 3 Our Most Recent Client-Side Attacks **Black Hat Briefings**

# Current Trends in Incident Detection



- Security Assessment validates strong external controls
- Necessary traffic allowed to the DMZ



Black Hat brienings

#### Regional Bank – Internet het links become Issues

- Internet links become saturated too much traffic
- Further investigation reveals....





#### Regional Bank – File Sharing

 Bank's most successful online venture ever – thousands of anonymous FTP users worldwide!

#### What happened??

- Ineffective security audit?
- New vulnerability?
- Misguided business plan?

#### Captain Edward A. Murphy



#### Regional Bank - Investigation

- Firewall ruleset dropped by knowledge-challenged sys admin 1 week after security audit completed
- File transfers commenced almost immediately, continued for over 1 month til detection (not by IDS!)
- Anonymous FTP home directory also IIS web root
- .ASP files uploaded, executed via webserver
- FTP server also code repository for online banking applications
- No logging of activity



# 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?

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

<del>biack nat briefings</del>

#### Findings – Ongoing Intrusion

- The Review of 54 Malicious Executable Files Yielded 21 Snort Signatures.
- 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 Detected by AV
  - 10 / 54 Files Reviewed were Packed via 4
     Different Methods
- Size of Toolkits is Large.
  - 85 Unique Tools.

#### Holy\_Father

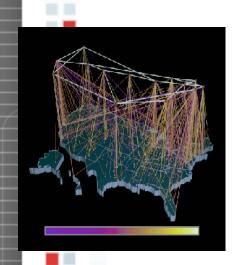
We're offering anti-detection service for any type of windows modules. There are many ways how to make your module undetected hence you can see below quite complicated price table with examples. To order this service write a mail with full description of what you need to holy\_father@phreaker.net. Feel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

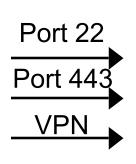
feature	Morphine	Häcker detender	Hacker defender driver	Other (no driver or libraries)	Libraries	Drivers
basic fee	€ 30.00	€ 20.00 <sup>0</sup>		€ 15.00	€ 15.00	€ 15.00
morphined <sup>1</sup>	x	+ € 02.50	x	+ € 02.50	+ € 02.50	x
morphined - unique <sup>2</sup>	x	+ € 25.00	x	+ € 20.00	+ € 20.00	x
per AV <sup>3</sup>	+ € 10.00	+ € 05.00	+ € 05.00	+ € 08.00	+ € 09.00	+ € 10.00
all AV <sup>3</sup>	x	+ € 25.00	+ € 30.00	+€30.00	+€35.00	+ € 40.00
unique version <sup>4</sup>	+ € 20.00	+ € 25.00	+ € 20.00	x	x	x
source code	+ € 20.00	+€30.00	+ € 15.00	-€ 10.00 <sup>5</sup>	-€ 10.00 <sup>5</sup>	-€ 10.00 <sup>5</sup>
no driver	x	+ € 10.00 <sup>8</sup>	x	x	x	x
special	х	special <sup>7</sup>	x	x	x	x

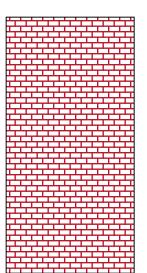
# How are Organization's Detecting Incidents?

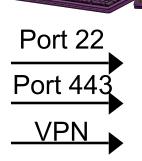
IDS Alerts?

Rare Detection Mechanism.

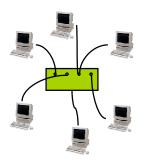


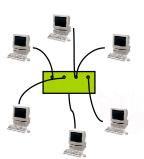






**IDS** 



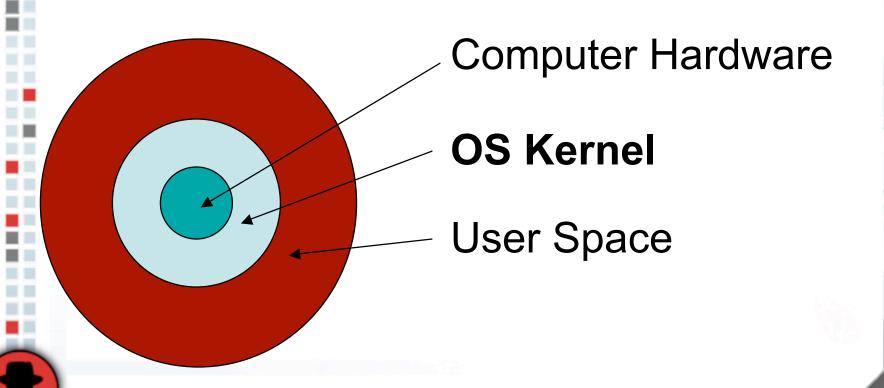


#### How are Organization's Detecting Incidents? Clients (Outside Company)

- - More Often than Pro-Active Countermeasures.
- Sensors Detecting Unusually High Levels of Network Activity.
- End Users (Internal)
  - Emerging as a Common Detection Mechanism.



System Crashes.



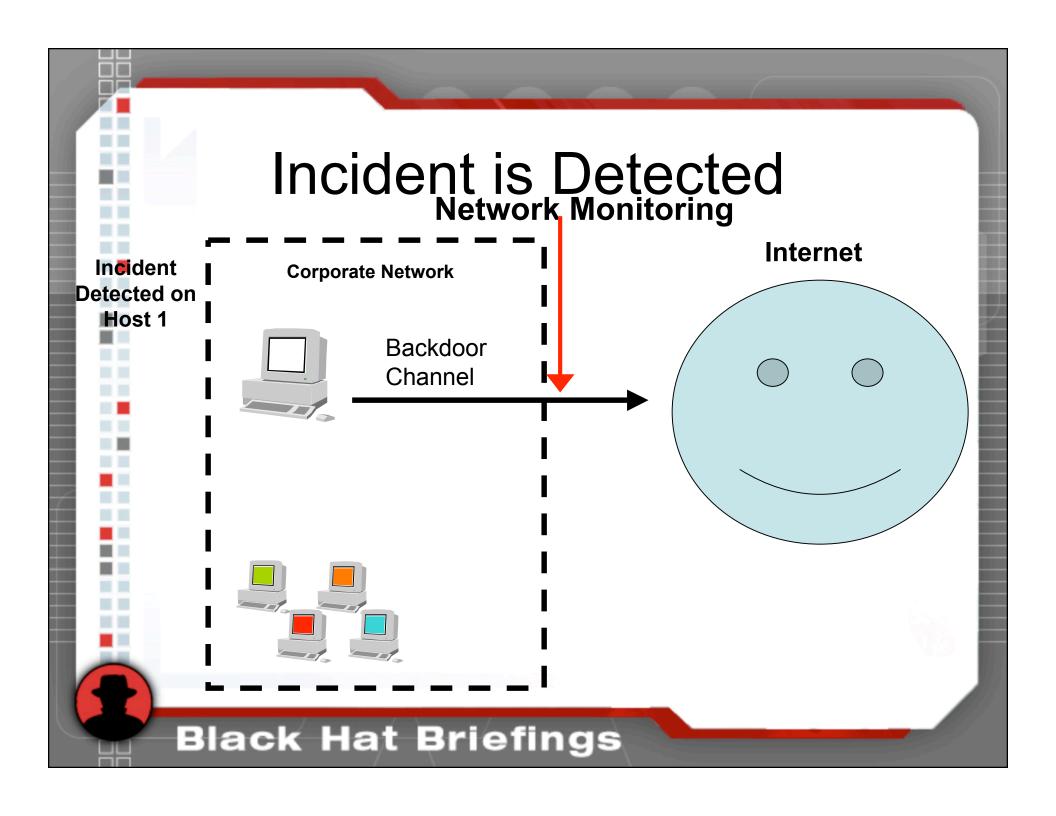
# How are End User's Detecting Incidents?

- 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?

- The Registry Editor (regedit) Closes Immediately When it is Invoked.
- The Inability to Connect to <a href="www.nai.com">www.nai.com</a>, www.nai.com
   www.mcafee.com
   or other Anti-Virus
   Web Sites. You are Redirected to Other Web Sites like <a href="www.google.com">www.google.com</a> When you Attempt to Visit Antivirus Web Sites.

# Current Incident Response Methods



#### Compromise Suspected

- Reporting Channels Often Vague
- Skills and Experience Lacking
- Processes are Shelf-ware or Non-Existant
- Instead of Precision Blitzkrieg, Response Sometimes becomes an Infantry March



#### 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!!!!

#### 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

Incident
Detected on
Host 1



- 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"



### What Are Some Indicators of Attack?

- Potential Indicators of Attack Revealed in Live Response:
  - Suspicious IP Addresses Connected to the Victim System
  - Suspicious Processes Running
  - Suspicious Logons, Failed Logons
  - Suspicious Windows Services
  - Registry Alteration
  - Filenames of Known Malicious Programs
  - Anti-Virus Logs (Application Log)



#### Review Live Response Data

Incident
Detected on
Host 1



Respond on Host 1

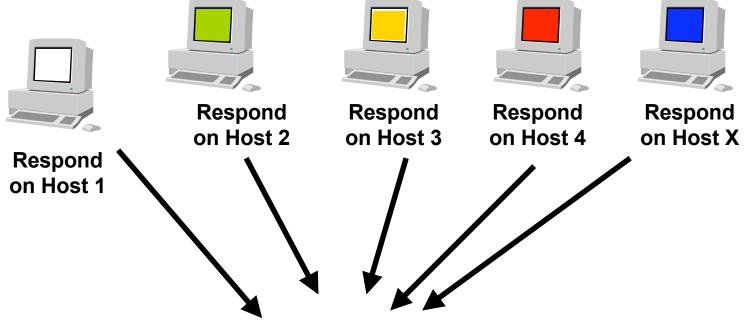
Directory of c:\WINNT\system32\drivers\disdn

10/18/2001	07:52a	<dir></dir>		• •
10/18/2001	07:52a	<dir></dir>		•
04/23/2003	03:17p		778,701	zgbtrca1.exe
04/23/2003	03:18p	<dir></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></dir>		AROD2W



Signature of Current Attacker Identified!!







Search for Signature of Current Attacker on Other Hosts.

# Demonstration Black Hat Briefings

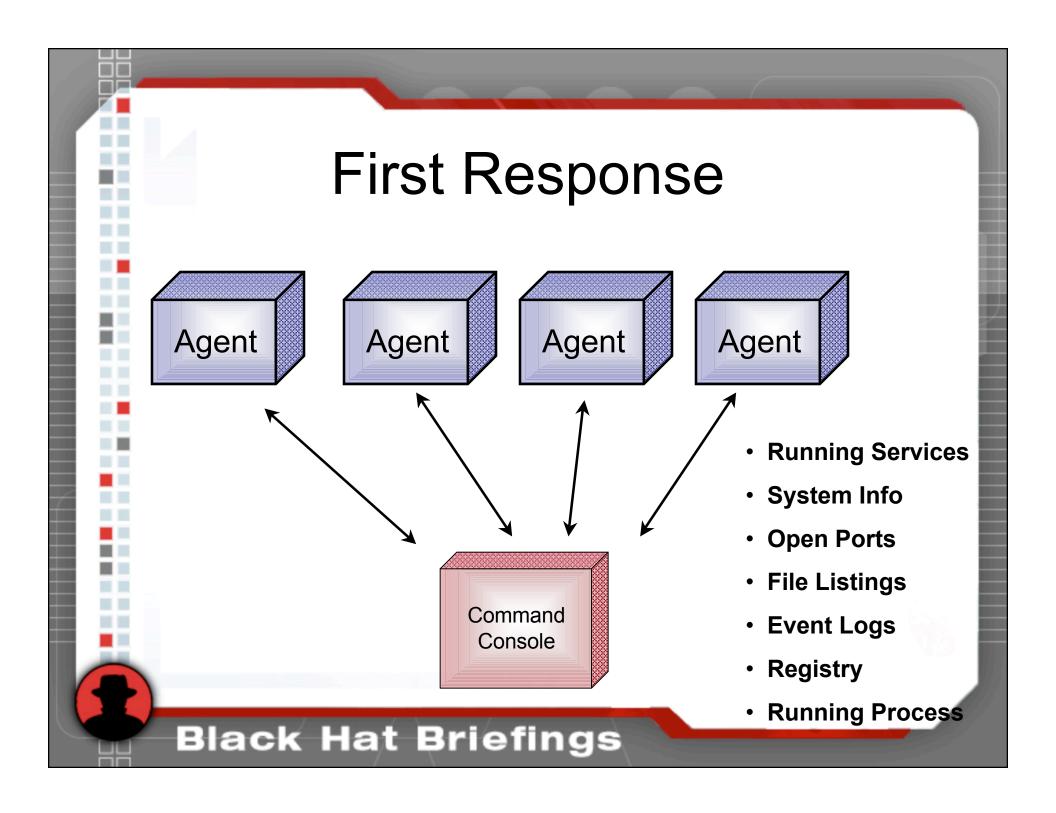
# Live Response Tools Newer, Faster Ways **Black Hat Briefings**

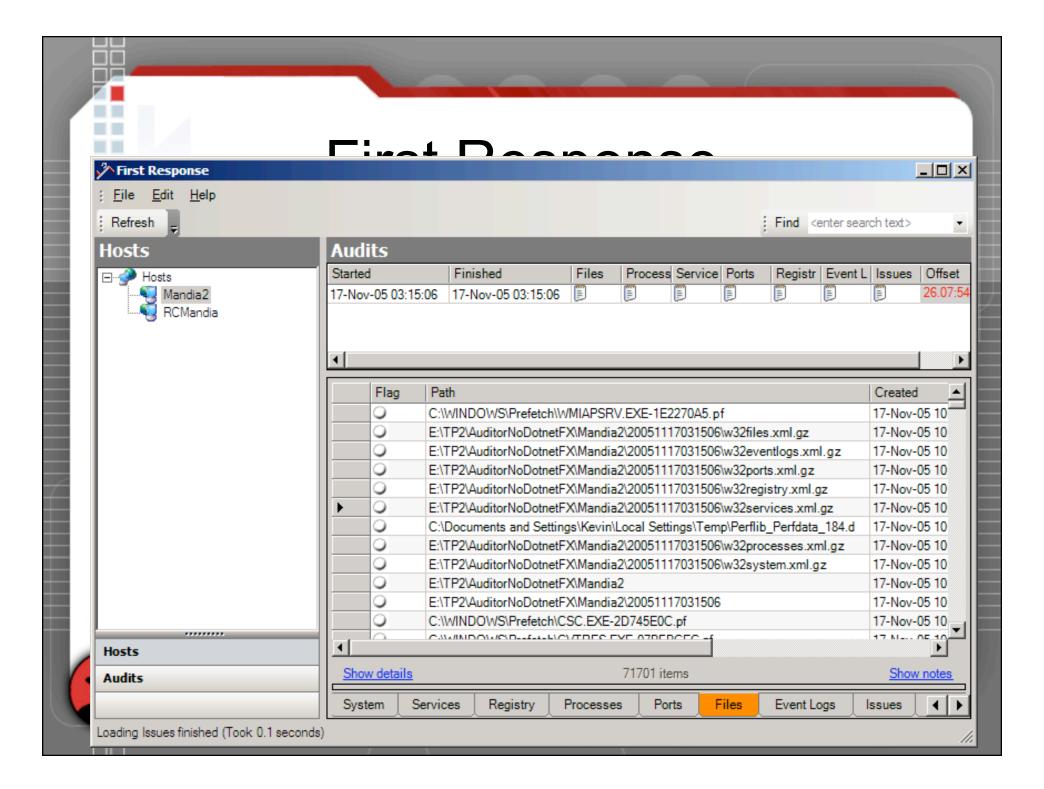
# Problems with Current Live Response Techniques

- Cumbersome
- Requires Several Iterations of Data Cultivating
  - Perl Scripts to Parse Large Output
  - Analysis Platform is Wordpad
- One to One Communications Channel
- Cannot "Pull" Data

#### First Response Demo

- A Tool is Needed to Blend all the Live Response Data Together for Faster Analysis!
- First Response is a FREE tool being released by Red Cliff in January.
  - Implements the Live Response Process of Data Collection.
  - Supports rapid analysis for confirmation of an incident.





# Live Demonstration of New Response Tool

# Emerging Trends in Incident Response

A Look Into the Future of Incident Response

# Emerging Trends in Incident Response

- Increased Forensic Skills Required for Successful / Rapid Remediation
- Compliance Concerns (Regulations/Standards)

#### More Dangerous Malware

What's the worst that could happen?

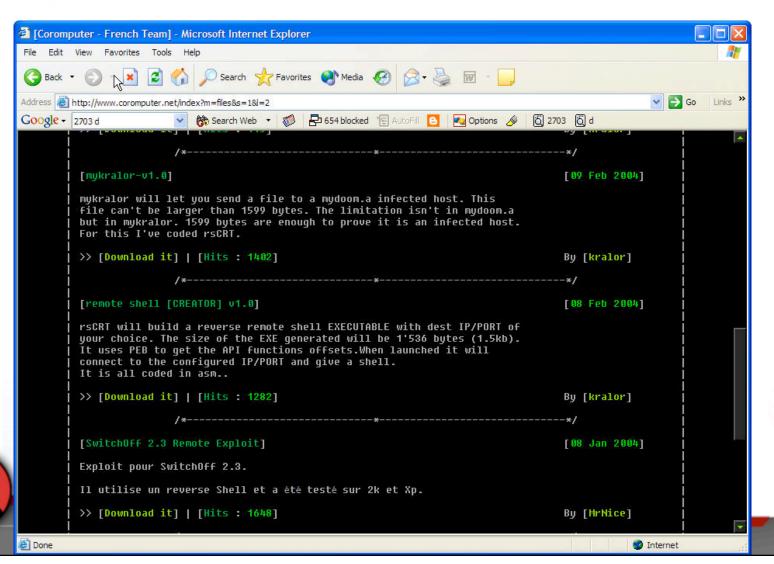
#### Complex Exploits

- Today a successful exploit requires multiple vulnerabilities
- A successful exploit must circumvent AV/FW
- Successful exploits combine a subset of:
  - More Dangerous Malware
  - User Initiated Propagation Methods
  - Web application insecurity
  - New vulnerabilities in new technologies (VOIP, mobile connectivity)
  - Untrusted networks

#### Malware Capabilities

- Remote Control capabilities to circumvent FW
- Sniffing / keystroke logging to circumvent encryption
- Disabling security software to circumvent AV / anti-spyware / FW
- Prolific code "templates" available
- Morphed malware

### Viruses/Worms Easy to Develop with Templates



#### Viruses can Circumvent AV?

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	Häcker detender	Hacker defender driver	Other (no driver or libraries)	Libraries	Drivers
basic fee	€ 30.00	€ 20.00 <sup>0</sup>		€ 15.00	€ 15.00	€ 15.00
morphined <sup>1</sup>	x	+ € 02.50	x	+ € 02.50	+ € 02.50	х
morphined - unique <sup>2</sup>	x	+ € 25.00	x	+ € 20.00	+ € 20.00	х
per AV <sup>3</sup>	+€ 10.00	+ € 05.00	+€ 05.00	+ € 08.00	+€09.00	+ € 10.00
all AV <sup>3</sup>	x	+ € 25.00	+€30.00	+ € 30.00	+ € 35.00	+ € 40.00
unique version <sup>4</sup>	+ € 20.00	+ € 25.00	+ € 20.00	x	x	x
source code	+ € 20.00	+ € 30.00	+€ 15.00	- € 10.00 <sup>5</sup>	-€ 10.00 <sup>5</sup>	-€ 10.00 <sup>5</sup>
no driver	х	+ € 10.00 <sup>8</sup>	х	х	x	x
special	X.	special <sup>7</sup>	x	x	X	x



#### Programmers Tools [Protools.owns.it]

#### Packers/Crypters/Protectors

#### Freeware packers

UPack by Dwing. 08.IV.2005.

Upack 0.25.

Upack is a packer that can compress Windows EXE file, which can be run without decompressing manually. It packs exe-files with best compression ratio. So it's only for compression, not for protection.

Mew by Northfox. 22.IX.2004.

Mew 11 SE 1.2.

Mew is an exe-packer program, based on LZMA and ApPack methods, written in MASM 32 and Visual C++ by Northfox. Originally it was designed for small files (4k,64k intros), but it supports bigger files too. With one of the best compression ratio.

UPX by Laszlo & Markus. 03.VII.2004. UPX 1.25.

#### News:

- watcom/le: don't crash on files without relocations
- win32/pe: stricter checks of some PE values
- source code: much improved portability using ACC, the Automatic Compiler Configuration
- source code: compile fixes for strict ISO C++ compilers
- source code: compile fixes for Win64
- excellent compression ratio.

- very fast decompression: about 10 MB/sec on a P133.
- no memory overhead for your compressed executables
- safe: you can list, test and unpack your executables.
- universal: supports dos/exe, dos/sys, dos/com, djgpp2/coff, watcom/le (DOS4G, PMODE/W, DOS32a and CauseWay), win32/pe, rtm32/pe, tmt/adam.

#### **Packers**

- UPack by Dwing. 08.IV.2005.
- Mew by <u>Northfox</u>. 22.IX.2004.
- UPX by Laszlo & Markus. 03.VII.2004.
- Packman by <u>bubba</u>. 27.II.2005.
- EZIP by <u>Jonathan Clark</u>.
   21.VII.2001.
- PE-PaCK by ANAKIN. 12.I.1999.
- FSG by bart. 24.V.2004.
- Dropper by Gem. 13.III.2005.
- CExe by <u>Scott</u>. 20.III.2003.
- PE Diminisher by tERAPHY.
   11.IX.1999.
- PECRYPT32 by <u>random</u>, <u>killa</u> 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 <u>Jonathan Clark</u>.
   29.III.2005
- PEBundle by Jeremy Collake. 12.III.2004.
- PECompact by <u>DevelTek</u>. 06.IV.2005.
- AS-Pack (shareware) by <u>Solodovnikov Alexey</u>. 07.I.2002.
- NeoLite (shareware) by <u>NeoWorx</u> Inc. 04.IV.1999.
- WWPack 32 by Piotr Warezak. 07.VII.2000.
- ARM Protector by SMoKE.
   22.IX.2004.

#### **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

#### Malware is now pervasive

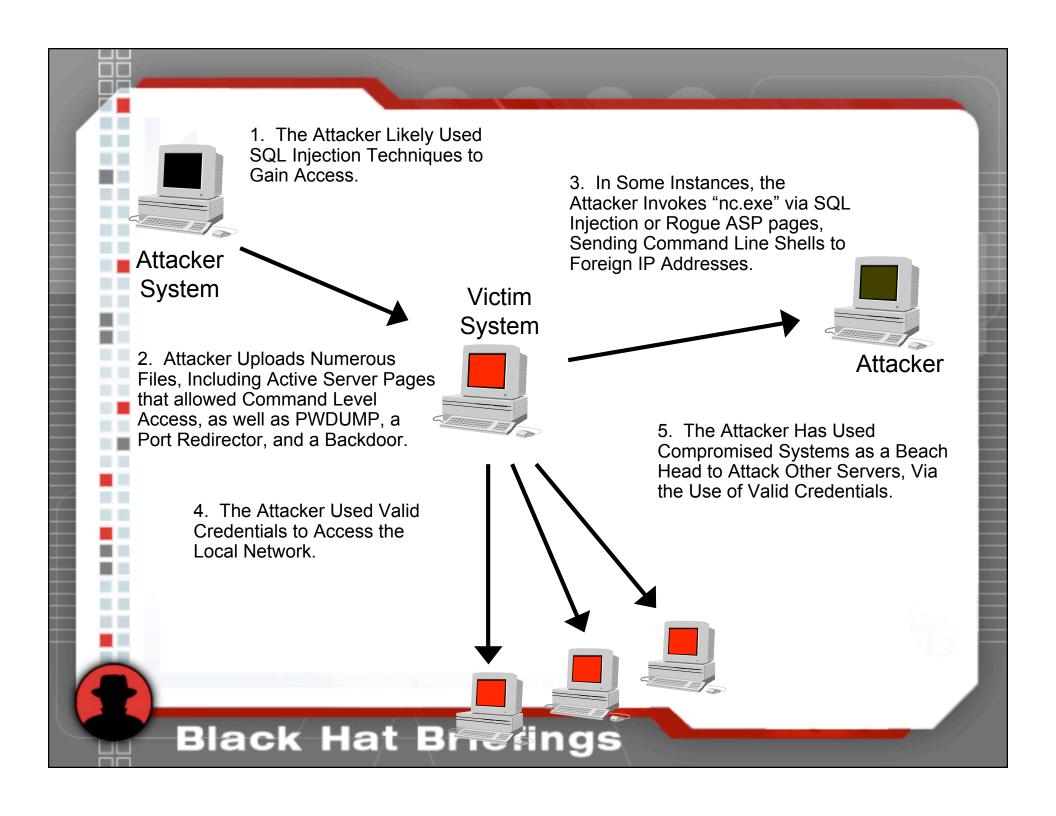
- 7% of enterprise systems infected with MONITORING software
- Each infected system averages 1.2 instances of malicious spyware
- Exposure is not limited to enterprise systems –
   remote access means consumer/home exposures to spyware may also compromise the enterprise

# Compliance Issues Black Hat Briefings

## Some CISO Challenges Frequency **Government Regulations** Complexity Black Hat Briefings

#### Compliance

- California SB 1386
- Cal. Civ. Code §1798.82(a)
- Federal Law Closing In S.1408
- Federal Law Closing In S.1332
- SEC Rule 17a-4(b)(4)
- 15 U.S. states to-date
- Japan & Canada



#### Client's #1 Concern

# Has Glent Data Compromised?

#### Damage Assessment

- Were Important Files Taken?
- Forensic Review of Important Systems is Required:
  - Time/Date stamps critical.
  - Log files critical.
  - Immediate / timely response critical.
- Network-based Logging Key Ingredient
  - Netflow Logs
  - Firewall Logs

### How do Companies Meet Reporting Requirements

- Processes
- Dry Runs
- Tools
- Proper Resources and Training

#### Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security

Agency Alleges Security Flaws Placed Consumers' Credit Card Numbers at Risk to Hackers

- On June 18, 2003 Guess, Incorporated agreed to settle charges that it exposed consumers' personal information, including credit card numbers, to commonly known attacks by hackers.
  - According to the FTC press release, the settlement requires Guess to establish and maintain a comprehensive information security program that must be certified by an independent professional within a year, and every other year thereafter.

#### Eli Lilly Settles FTC Charges Concerning Security Breach

Company Disclosed E-mail Addresses of 669 Subscribers to its Prozac Reminder Service

- On January 18, 2002 Federal Trade Commission (FTC) settled with Eli Lilly regarding the unauthorized disclosure of sensitive personal information through Eli Lilly's Prozac.com website.
- Eli Lilly agreed to establish and maintain a **four-stage information security program** designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect consumers' personal information against any reasonably anticipated threats or hazards to its security, confidentiality, or integrity, and to protect such information against unauthorized access, use, or disclosure.



### Likelihood of Compromised Client Data The attack was a scripted attack, requiring no human

- The attack was a scripted attack, requiring no human intervention.
- The attacker's backdoor ftp server did not appear to be used to upload or download any files.
- The directory structure and the tools installed on the victim server "XXX-XX" are consistent with the attacker setting up a WAREZ site a site for pirated software, music, and video distribution.
- The attacker's toolkit did not include programs that would increase the attacker's access into the network.
- The attacker's methodology was easily detected.

# Contact Info Kevin Mandia Kevin.mandia@red-cliff.com

# Questions and the second secon

**Black Hat Briefings** 

뻐