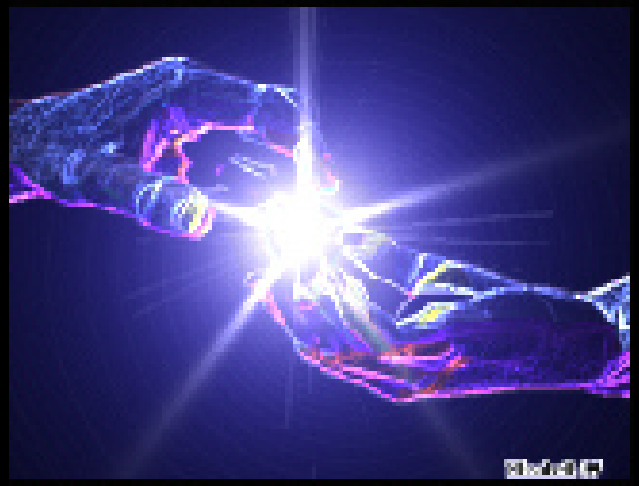
The State of the Hack



Kevin Mandia
MANDIANT

MANDIANT
INTELLIGENT INFORMATION SECURITY

Who Am I?

- Adjunct Professor
  - Carnegie Mellon University
    - 95-856 Incident Response
    - Master of Information System Management
  - The George Washington University
    - Computer Forensics III
    - Masters in Forensic Science
- Author for McGraw-Hill
- Honeynet Project

MANDIANT
INTELLIGENT INFORMATION SECURITY

The Honeynet project

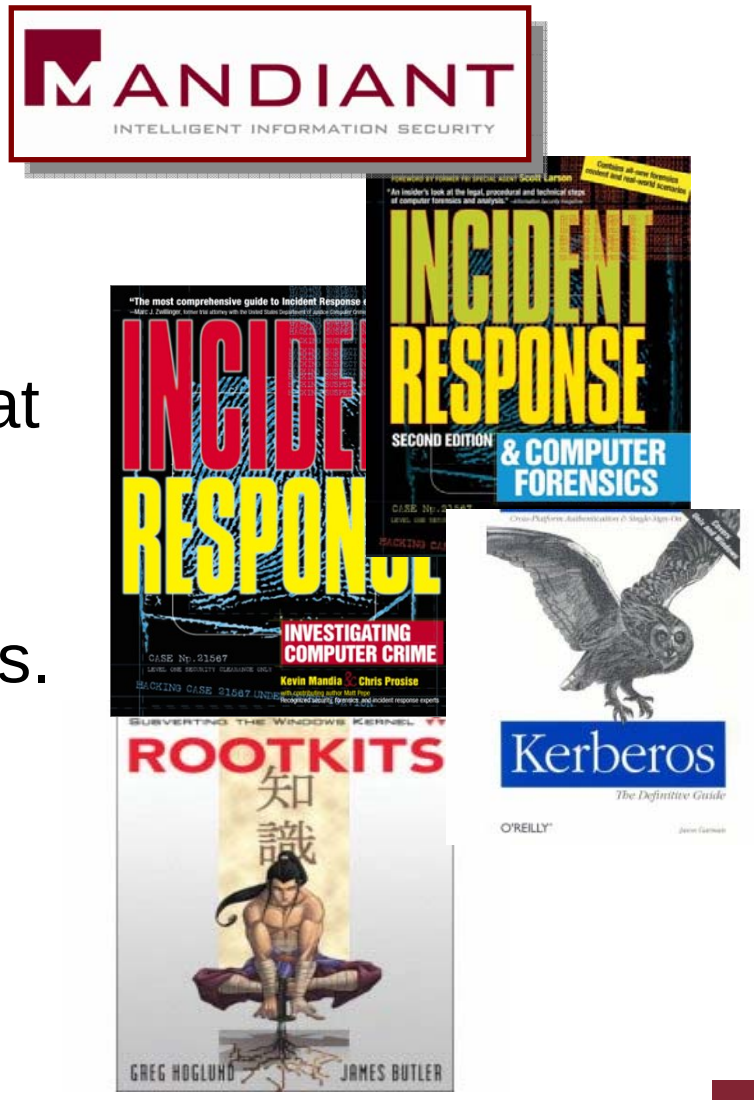
Carnegie Mellon

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

MANDIANT

Who Am I?

- Last 5 Years
  - Responded to over 300 Potentially Compromised Systems.
  - Responded to Intrusions at Over 40 Organizations.
  - Created IR Programs at Several Fortune 500 Firms.



Evolution of IT Attacks

-- 1998

- Technical Problem
- Unix Systems
- Servers
- Attacks were a Nuisance

1998 -- 2002

- Technical/Business Problem
- Windows Systems
- Servers
- Attacks Were About Money

2002 -- Now

- Technical/Business/Legal Problem
- Windows Systems
- Client Systems / End Users
- Attacks Are About Money

Agenda

- Incident Detection
- Case Studies
- Challenges When Responding to Security Incidents

Incident Detection

How Organizations are Detecting Incidents?

MANDIANT
INTELLIGENT INFORMATION SECURITY

1. How are Organization's Detecting Incidents?

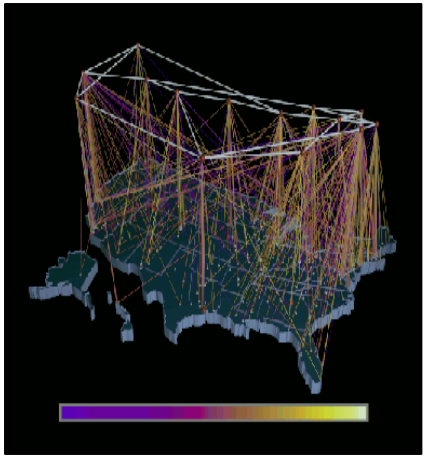
- Antivirus Alerts?
  - Perhaps, but do not Count on It…
  - Alerts are Often Ignored – and Perhaps Value-less Without an In-Depth Review of the System.
  - Quarantined Files Often Remain a Mystery

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

File Name	Size	MD5SUM	Packer	Initial Comments
AgentSlave.exe	14,848	9c1b827d4960779b 55e2fd330a3b4212	UPX 1.24 *(Unpacked)*	Redirect Utility. Source code located and comparative analysis performed.
C.EXE	103,424	093d637578d7a531 a7aca468e823f898	UPX 1.2 **(Armored)**	Command Shell Interpreter (cmd.exe)
ESmb.exe	11,776	e4e317524176c184 41d0f38109f6ac9c	UPX 1.24 *(Unpacked)*	eSMB v1.0, by Eric (A&D Team)
Net.exe	21,504	a8da00e86561eb96 66e668f101c2864a	UPX 1.20 **(Armored)**	Windows net command
Net1.exe	58,368	13244f36d89c8e44 2aaadaaa0fa9a6bc	UPX 1.20 **(Armored)**	Strace shows net1.exe called when net.exe executed
Netdom.exe	31,744	cdf2682374a2c472 3693482ccbbf0ef4	UPX 1.20 **(Armored)**	Windows Support Tool. Allows you to work with Windows domains and trusts, allowing you to add and remove computer accounts from a domain, reset computer account passwords, move servers among domains, and establish one- and two-way trusts between Windows domains.
MT.exe	99,328	b55b1bda620306a8 3af346694b6ea35b	ASProtect 1.23 RC1	Same functionality as previous mt.exe
PWDUMP4.EXE	16,384	605E2D28BC58E0 146C0AE3DFC6D 04F26	UPX 1.22 *(Unpacked)*	Password Hash dump utility
PWDump4.dll	4,608	90482aa6838d5440 1c8f21139a6c7e2d	UPX 1.22 *(Unpacked)*	Dynamic Link Library used by pwdump
Ps.exe	35,840	adb3927dc329889a 31279cb3ec76f7a5	UPX 1.20 **(Armored)**	Sysinternals PSEXEC
Sl.exe	20,480	5D7F8A1F9D4BB 168ED24CADDBE 7D031A	UPX 1.22 **(Armored)**	Foundstone ScanLine.exe. Command line port scanner.
Winfo.exe	53,248	5f043c1b282d2fc27 dc044465cdc6c3c	NOT PACKED	http://www.ntsecurity.nu/toolbox/winfo/ Winfo uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. It also identifies the built-in Administrator and Guest accounts, even if their names have been changed.

2. How are Organization's Detecting Incidents?

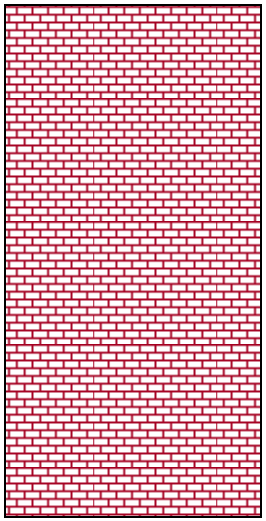
- IDS Alerts?
  - Rare Detection Mechanism.

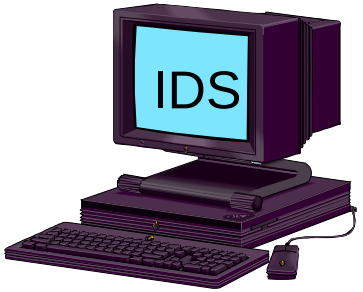


Port 22

Port 443

VPN

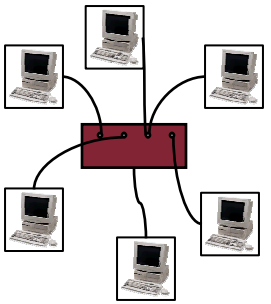


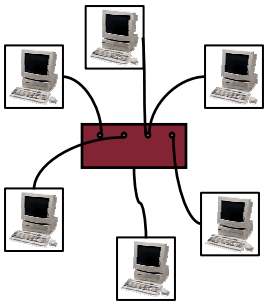


Port 22

Port 443

VPN





3. How are Organization's Detecting Incidents?

- Clients (Outside Company)
  - Malicious Software Discovered on Compromised End-User Systems.
  - Account Manipulation (Online Trading).

4. How are Organization's Detecting Incidents?

- End Users (Internal)
  - System Crashes (Blue Screens of Death)
  - Continual Termination of Antivirus Software.
  - Installing New Applications Simply Does Not Work.
  - Commonly Used Applications Do Not Run.
  - You Cannot "Save As".
  - Task Manager Closes Immediately When You Execute It.

5. How Are Organization's Detecting Incidents?

- Proactive Audits or Security Scans

6. How Are Organization's Detecting Incidents?

- Something Obvious …

Rogue ASP Pages

服务器名	target=_blank>
IP:端口 时间	:
CPU数量 OS	个 []
局域网址:	
运算速度	毫秒(256M 2.4G为156.3毫秒)
客户端IP→端口 [无代理]	→ []
本文件	>
绝对路径: <%=Server.MapPath(	size=84>
文件1 Browse...	空=><=格口 设定 上传 1 文件 上传 重置

"> 执行 服务器变量 退出 重置

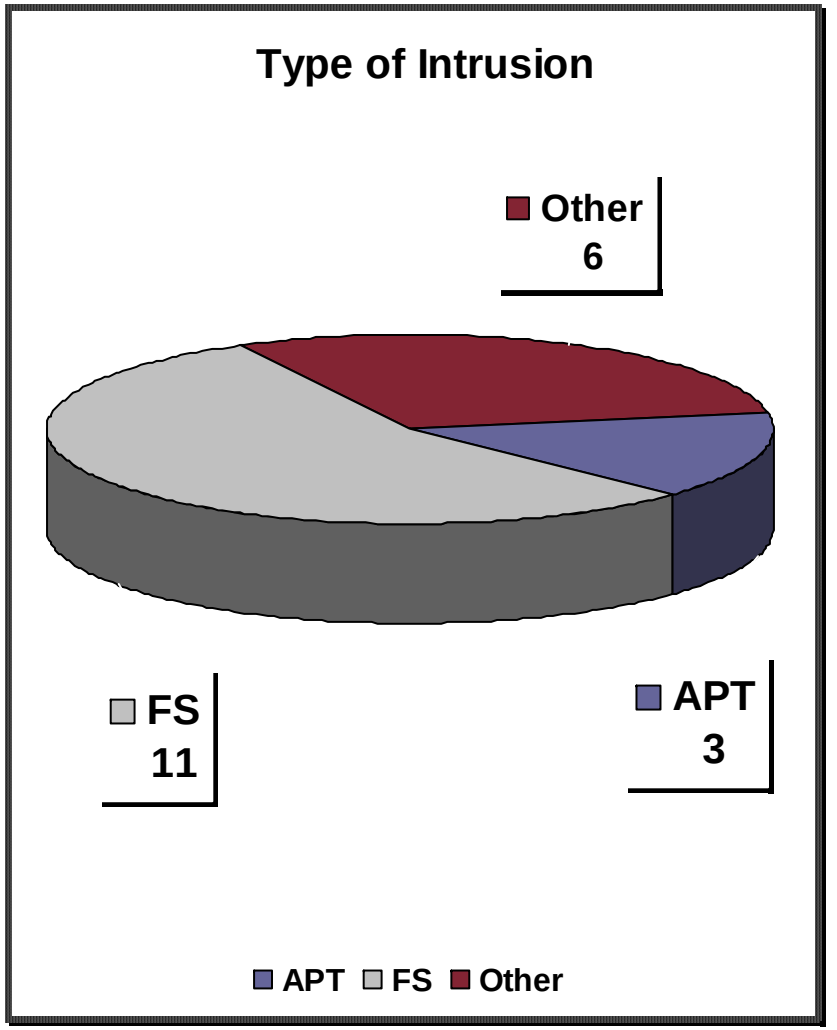
复制:		目的路径:	
移动:		目的路径:	
程序:		附加参数:	
浏览:		DOS 命令:	%COMSPEC% /c
下载:		论坛登陆	冰点极限&海洋顶端

7. How are Organizations Detecting Incidents?

- Notification from other Victims.
- Notification from Government Agencies.

Types of Intrusions - 2008

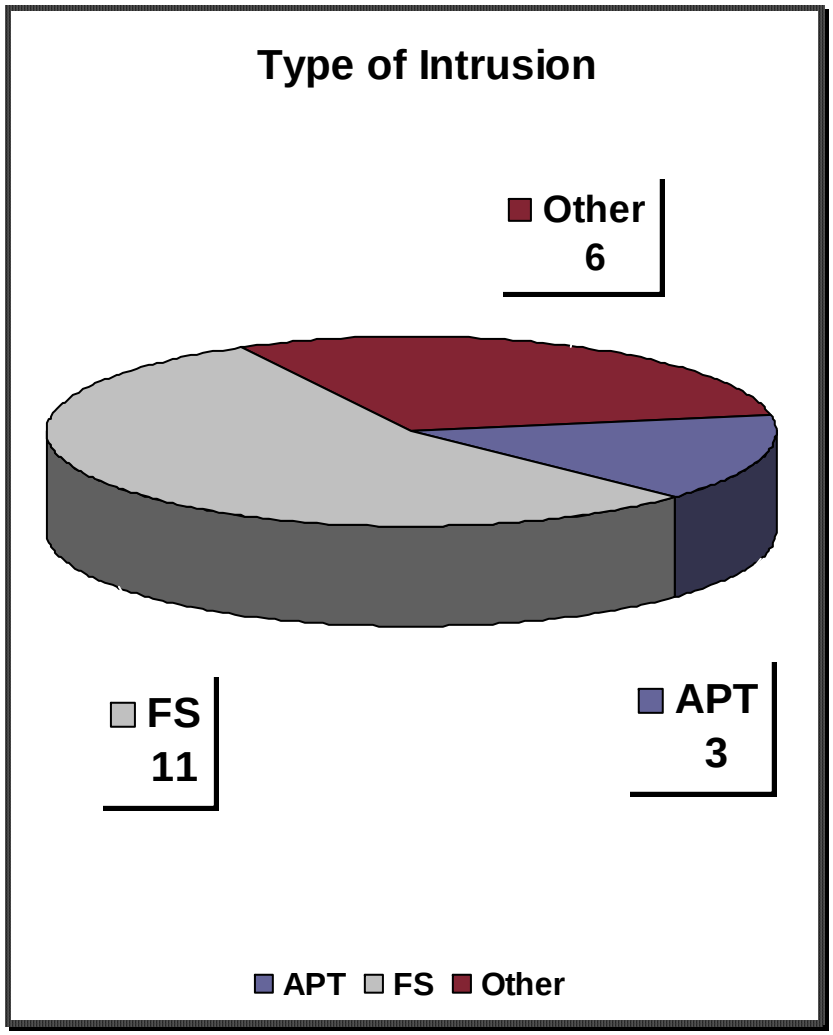
- Last 20 Computer Intrusions in 2008:
  - 10 Financial Services
  - 5 Retailers
  - 2 Government
  - 2 EDU
  - 1 Insurance



MANDIANT

Detection – Last 20 Incidents

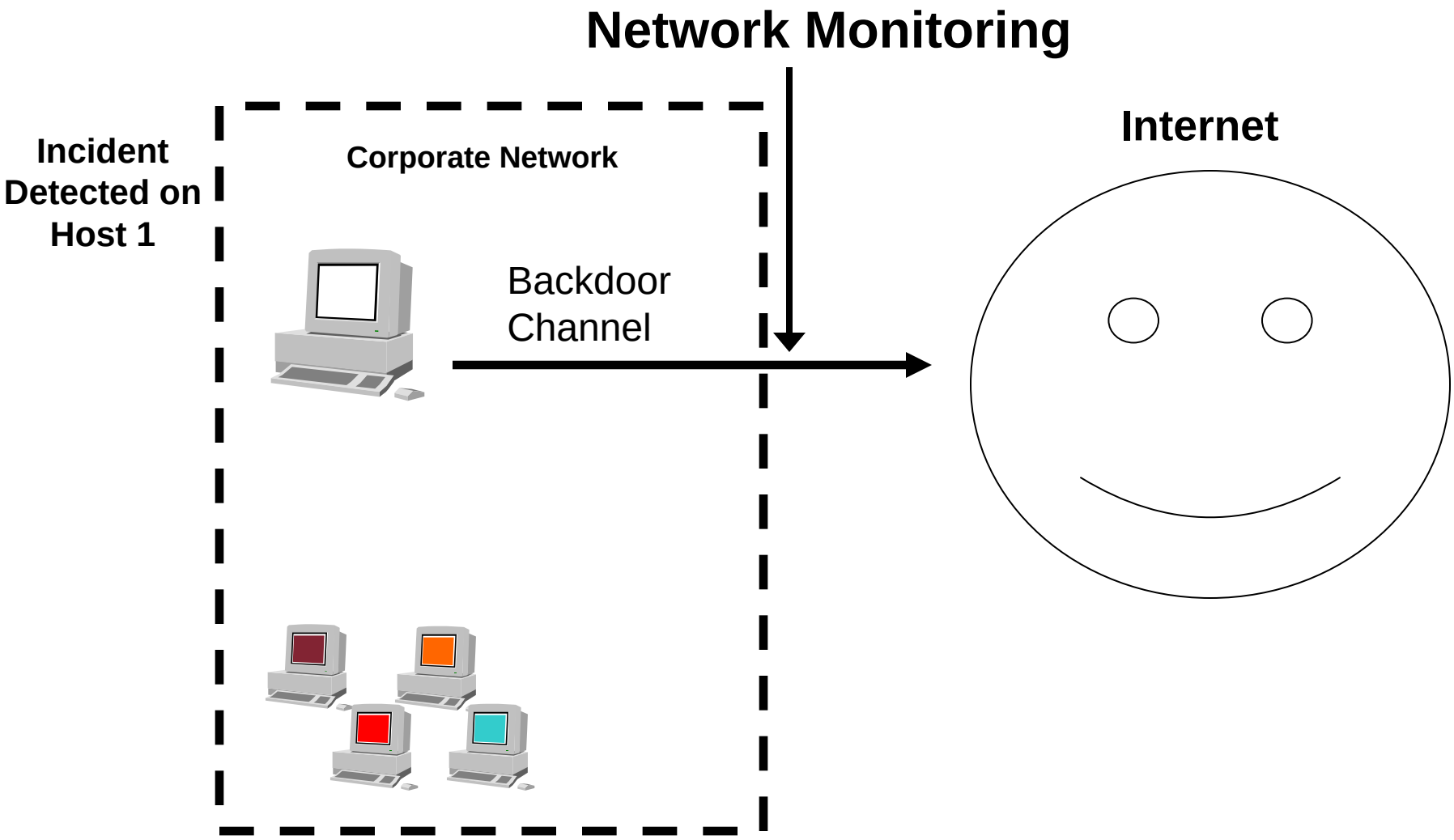
- Antivirus .5
- IDS .5
- Clients/External 1
- End Users 6
  - IT
- Audits 0
- Obvious 0
- External 12



MANDIANT

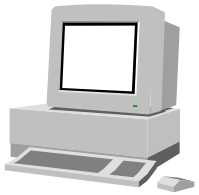
CSI – Computer Intrusion Forensics!!!

Incident is Detected



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**

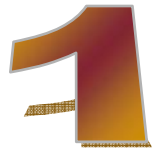
Live Data Collection Performed to Verify Incident and Determine Indicators / Signature of the Attack

MANDIANT

How Are Attackers Gaining Initial Entry?

How are Attackers Gaining Entry?

- Vulnerable Services?
- Not Nearly as Common as 1998-2003.



How are Attackers Gaining Entry?

- Web Application Vulnerabilities?
  - SQL Injection

How Are Attackers Gaining Entry?

- End User Attacks

How Are Attackers Gaining Entry?

- Never Find Victim 0?
- Valid Credentials

What Attackers are Doing Now

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

Case Studies

The State of the Hack

MANDIANT
INTELLIGENT INFORMATION SECURITY

Case Studies – Attacks for Information

MANDIANT
INTELLIGENT INFORMATION SECURITY

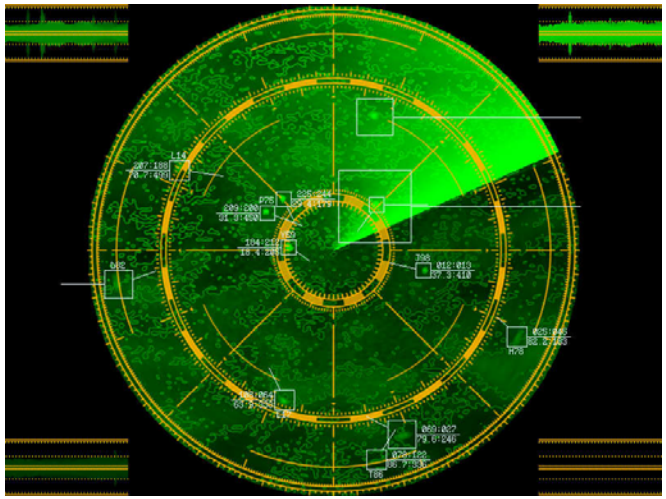
Case Studies – Attacks for Money

MANDIANT

INTELLIGENT INFORMATION SECURITY

Challenge

- Knowing the Constituencies you are Investigating the Breach for:
  - Executive Management
  - Technical Management
  - Legal Counsel
  - Insurance
  - Clients/Customers



- There are Conflicts Amongst these Constituencies

Evolution of Incident Response

- Executive Concerns
- Legal Concerns
- Technical Concerns

Technical

Business

Compliance

Management Concerns (Board and CEO)

- What is the Incident's Impact on Business?
- Do We have to Notify our Clients?
- Do We have to Notify our Regulators?
- Do We have to Notify our Stock Holders?
- What is Everyone Else Doing about this Sort of thing?

Legal Counsel Concerns

- Are we required to notify our clients, consumers, or employees about the security breach?
- What constitutes a "reasonable belief" that protected information was compromised – the standard used in many states to determine whether notification is required?

MANDIANT

Legal Counsel Concerns

- What are the applicable regulations or statutes that impact our organization's response to the security breach?
- Which state laws are applicable? Which might be in the future?
- Are there any contractual obligations that impact our incident response strategy?

MANDIANT

Legal Counsel Concerns

- How might public knowledge of the compromise impact the organization?
- What is our liability if PII was compromised?
- What is our liability if the compromised network hosted copyrighted content (pirated movies, music, software…)
- Does notifying our customers increase the likelihood of a lawsuit?

MANDIANT

Legal Counsel Concerns

- Is it permissible to monitor/intercept the intruder's activities?
- How far can/should we go to identify the intruder?
- Who knows about the incident?
- Should the organization notify our regulators? Law enforcement?

Technical Management (CIO)

- How long were we exposed?
- How many systems were affected?
- What data, if any, was compromised (i.e., viewed, downloaded, or copied)?
- Was any Personal Identifiable Information (PII) compromised?
- What countermeasures are we taking?

Technical Management (CIO)

- What are the chances that our countermeasures will succeed?
- Who else knows about the security breach?
- Is the incident ongoing? Preventable?
- Is there a risk of insider involvement?

Questions?