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

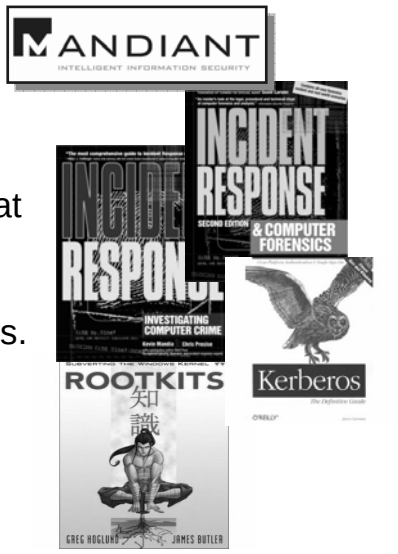
MANDIANT

1

© 2007 by MANDIANT Corporation

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.



MANDIANT

2

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

MANDIANT

3

© 2007 by MANDIANT Corporation

Agenda

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

MANDIANT

4

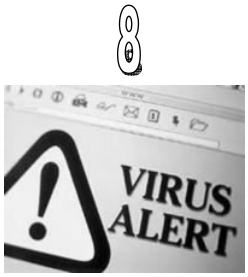
Incident Detection

MANDIANT
INTELLIGENT INFORMATION SECURITY

© 2007 by MANDIANT Corporation

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

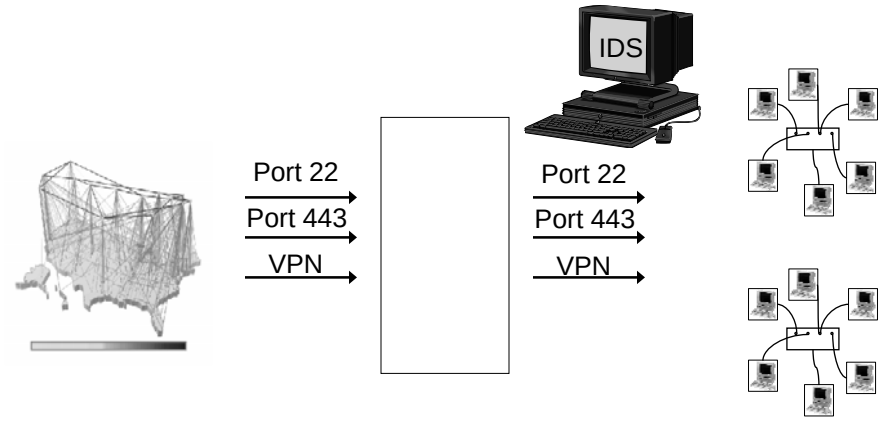


Anti-Virus Merely Alerts an Organization that Something Bad Might have Occurred. No Confirmation. Potential Loss of Critical Data

MANDIANT 6

2. How are Organization's Detecting Incidents?

- IDS Alerts?
  - Rare Detection Mechanism.



MANDIANT 7

© 2007 by MANDIANT Corporation

3. How are Organization's Detecting Incidents?

- Clients (Outside Company)
  - Malicious Software Discovered on Compromised End-User Systems.

MANDIANT 8

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.

MANDIANT 9

© 2007 by MANDIANT Corporation

5. How Are Organization's Detecting Incidents?

- Proactive Audits or Security Scans

1

MANDIANT 10

6. How Are Organization's Detecting Incidents?

- Something Obvious …

5

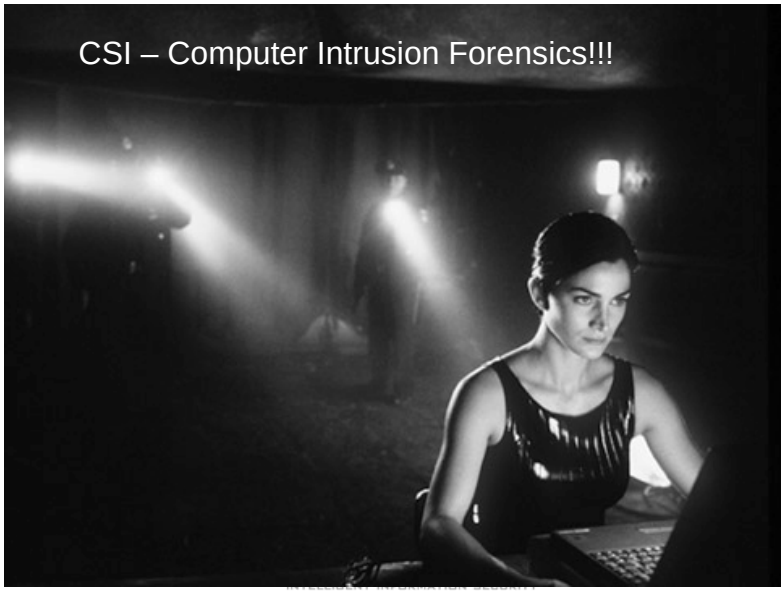
MANDIANT 11

© 2007 by MANDIANT Corporation

7. How are Organizations Detecting Incidents?

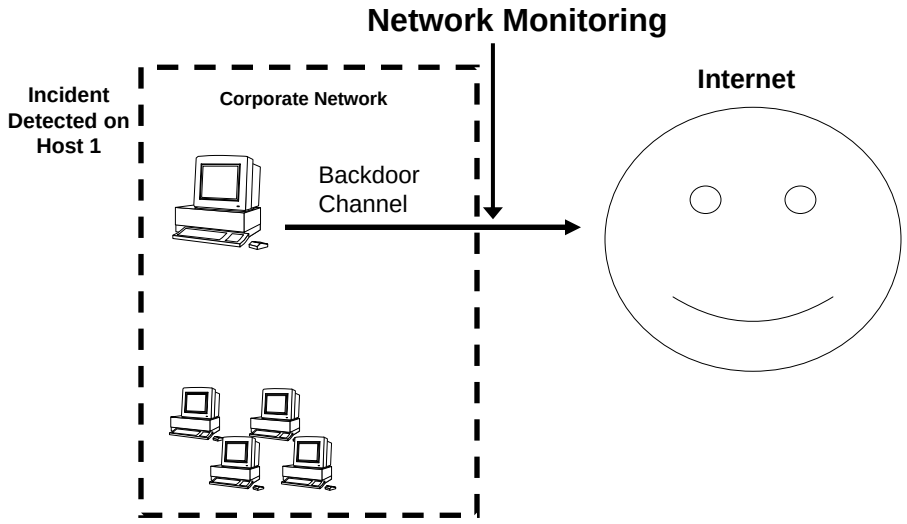
- Notification from other Victims.
- Notification from Government Agencies.

2



© 2007 by MANDIANT Corporation

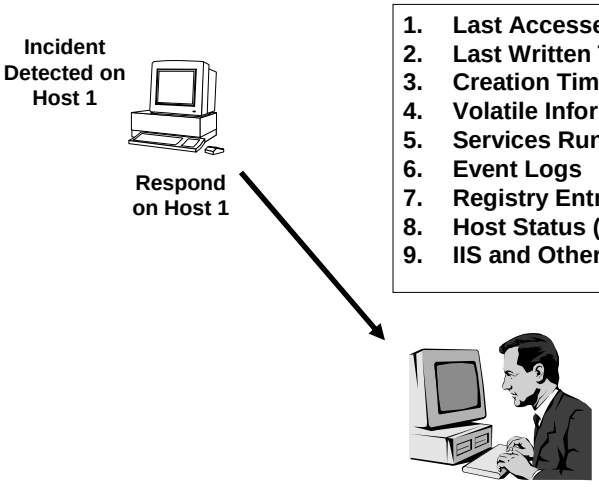
Incident is Detected



MANDIANT

14

Performing Live Response



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

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

MANDIANT

15

© 2007 by MANDIANT Corporation

Review Running Processes …

```
C           4164   8   1   26   1408   0:00:00.015   0:00:00.000  100:32:36.273
As          4492   8   1   30   1324   0:00:00.062   0:00:00.156  100:32:36.242
C           4340   8   1   31   1428   0:00:00.031   0:00:00.000  100:30:02.252
C           4524   8   1   31   1428   0:00:00.031   0:00:00.000  100:27:30.636
CMD         4276   8   1   29   1988   0:00:00.015   0:00:00.015   83:44:11.551
net         4204   8   1   42   2736   0:00:00.015   0:00:00.015   83:44:11.536
CMD         4136   8   1   30   2024   0:00:00.015   0:00:00.015   59:56:59.498
cidaemon    4260   4   4  166    396   0:00:21.781   0:00:10.328   41:15:41.945
cidaemon    4596   4   4  153    384   0:00:21.218   0:00:10.234   41:15:06.022
CMD         4528   8   1   31   1988   0:00:00.031   0:00:00.015   39:47:54.009
net         4256   8   1   44   2736   0:00:00.015   0:00:00.015   39:47:53.993
```


Established Network Connections …

```
TCP    10.231.3.131:1943      10.230.231.39:139      TIME_WAIT
TCP    10.231.3.131:1945      10.230.121.14:445      TIME_WAIT
TCP    10.231.3.131:1947      10.230.131.33:445      TIME_WAIT
TCP    10.231.3.131:1950      10.230.211.65:139      TIME_WAIT
TCP    10.231.3.131:1953      10.230.121.33:139      TIME_WAIT
TCP    10.231.3.131:1955      10.230.121.100:139     TIME_WAIT
TCP    10.231.3.131:1957      10.230.231.23:445      TIME_WAIT
TCP    10.231.3.131:1959      10.230.131.104:445     TIME_WAIT
TCP    10.231.3.131:1961      10.230.211.95:445      TIME_WAIT
TCP    10.231.3.131:1964      10.230.211.83:139      TIME_WAIT
TCP    10.231.3.131:1966      10.230.131.89:445      TIME_WAIT
TCP    10.231.3.131:1969      10.230.231.70:139      TIME_WAIT
TCP    10.231.3.131:1972      10.230.20.117:139      TIME_WAIT
TCP    10.231.3.131:1975      10.230.20.29:139       TIME_WAIT
TCP    10.231.3.131:1978      10.230.131.36:139      TIME_WAIT
TCP    10.231.3.131:1981      10.230.221.36:139      TIME_WAIT
TCP    10.231.3.131:1984      10.231.8.167:139       TIME_WAIT
TCP    10.231.3.131:1986      10.230.121.58:445      TIME_WAIT
TCP    10.231.3.131:1988      10.230.15.62:445       TIME_WAIT
```


© 2007 by MANDIANT Corporation

Review of the Application Event Log

```
6192,Application,Symantec Antivirus, ERROR, HOSTXXX,
  9/21/2006 3:39:31 AM,40,None, Symantec Antivirus
  has determined that the virus definitions are
  missing on this computer. This computer will
  remain unprotected from viruses until virus
  definitions are downloaded to this computer.
```


Review of Listening Ports

```
svchost.exe [2800]
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING
TCP 0.0.0.0:90 0.0.0.0:0 LISTENING
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:21096 0.0.0.0:0 LISTENING
```


© 2007 by MANDIANT Corporation

How Are Attackers Gaining Initial Entry?

MANDIANT
INTELLIGENT INFORMATION SECURITY

How are Attackers Gaining Entry?

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

MANDIANT

21

© 2007 by MANDIANT Corporation

How are Attackers Gaining Entry?

- Web Application Vulnerabilities?

How Are Attackers Gaining Entry?

- End User Attacks

© 2007 by MANDIANT Corporation

How Are Attackers Gaining Entry?

- Never Find Victim 0?
- Valid Credentials

MANDIANT

24

Case Studies

The State of the Hack

MANDIANT
INTELLIGENT INFORMATION SECURITY

© 2007 by MANDIANT Corporation

Case Studies – End User Attacks

MANDIANT
INTELLIGENT INFORMATION SECURITY

The Challenges to Incident Response

MANDIANT
INTELLIGENT INFORMATION SECURITY

© 2007 by MANDIANT Corporation

High-Level Direction

Challenges
Lack of Poignant, High Level Direction.

High Level Direction

- Define the “Win”
- Know the Concerns of ALL Parties.
- Assign/Assume Incident Ownership
- Determine How Good Does the Incident Response Need to Be
  - Priority of IR Role VS. Day Job
  - Business as Usual VS. Business Interruption
- Level of Resources Assigned to the Incident
  - Number of People
  - Level of Escalation
  - Sense of Urgency

© 2007 by MANDIANT Corporation

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?

© 2007 by MANDIANT Corporation

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 32

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 33

© 2007 by MANDIANT Corporation

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

34

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?

MANDIANT

35

© 2007 by MANDIANT Corporation

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?

MANDIANT 36

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?

MANDIANT 37

© 2007 by MANDIANT Corporation

© 2007 by MANDIANT Corporation