

MANDIANT


When prevention fails
The tough respond

Michael J. Graven
michael.graven@mandiant.com

Introductions **MANDIANT**

MICHAEL J. GRAVEN

- Director
- Reformed Cisco IOS jockey
- Recovering UNIX admin
- Native Californian
- Adopted Minnesotan
- Snowboarder



2 © Copyright 2011

Who is MANDIANT

- Targeted threat experts
- Offices in DC, NY, LA, SF
- About 170 employees
 - Many with U.S. DoD Top Secret clearances
- Lots of customers
 - 23 of Fortune 100
 - 69 of Fortune 500
 - 8 of 10 largest defense contractors
 - 3 of the largest banks



3 © Copyright 2011

Why we see interesting things **MANDIANT**

MANDIANT is among the best organizations detecting and responding to advanced, targeted threats.*

* We just never get to talk about it

4 © Copyright 2011

Caveat **MANDIANT**


All information is derived from Mandiant observations in non-classified environments.

Some information has been sanitized to protect our clients' interests.

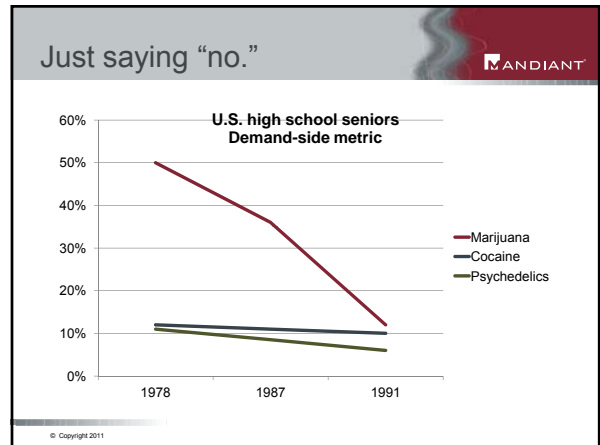
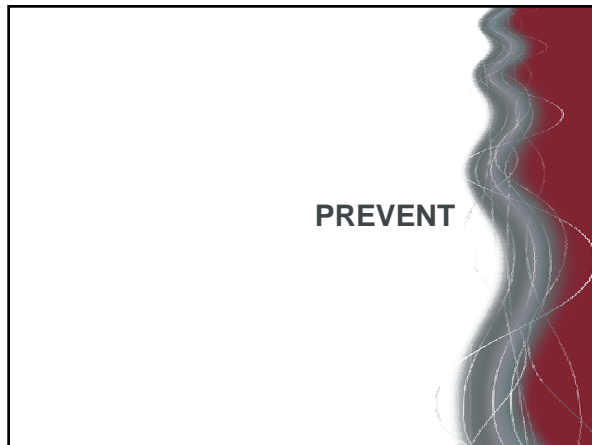
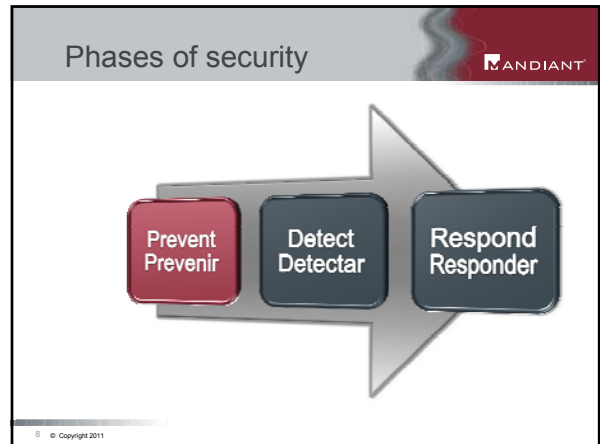
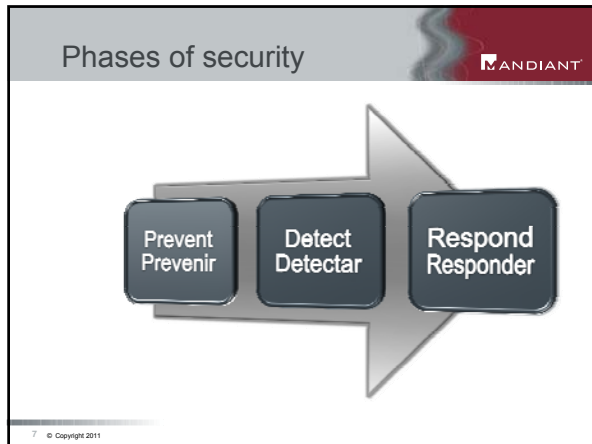
© Copyright 2011

Overview **MANDIANT**

- Phases of security
- What is prevention
- Why does it fail
- Targeted attackers
- Case studies
- What actually works




6 © Copyright 2011



- ### How much "no" do you need?
- 100% NO
 - End users must never make a single mistake
 - Never click on evil links
 - Never open evil attachments
 - Wear a clear plastic hood to work every day
- © Copyright 2011

- ### When prevention works
- | | |
|--|---|
| <p>YES</p> <ul style="list-style-type: none"> ▪ Commodity problems ▪ Compliance requirements ▪ Operational efficiency ▪ The known bad | <p>NO</p> <ul style="list-style-type: none"> ▪ Targeted threats ▪ Ad hoc environments ▪ Unknown bad |
|--|---|
- © Copyright 2011

Good prevention measures 

- Increase security operations efficiency
 - Host anti-virus
 - Web/mail proxies
 - Patch / software deployment
- Defend against known threats
 - Worms, bots, viruses
 - Other industry-specific problems
- GOAL: let computers handle all the "stupid, but important" things.

© Copyright 2011

BUT



But 


**Prevention
eventually
fails.**


© Copyright 2011

Not all threats respect 


- Targeted threats don't care if you're compliant
- They care if you're vulnerable
- Are you compromised?
- Let's take the APT


© Copyright 2011

Botnets: Not the APT 



© Copyright 2011

Exploits: Not the APT 



© Copyright 2011

“Hacktivists”: Not the APT

© Copyright 2011

So who are they?

- The APT is a specific set of threat actors
- The APT is a “who”, not a “how”
- Not all targeted attacks are APT-related
- Motivation is very different
- Similar techniques used by
 - APT
 - Other targeted attackers
 - Mass malware

© Copyright 2011

APT Objectives

- Political
- Economic
- Technical
- Military

© Copyright 2011

APT Objectives

- Political
 - Maintaining internal stability
- Economic
- Technical
- Military

© Copyright 2011

APT Objectives

- Political
- Economic
 - Steal intellectual property (IP) from victims
 - Duplicate and sell IP
 - Study IP and under-bid in competitive dealings.
 - Combine with local research, produce new products and services faster and cheaper than the victims can.
- Technical
- Military


© Copyright 2011

APT Objectives

- Political
- Economic
- Technical
 - Further their ability to accomplish their mission.
 - Gain access to source code for further exploit development
 - Learn how defenses work in order to better evade or disrupt them.
- Military

© Copyright 2011


APT Objectives



- Political
- Economic
- Technical
- Military
 - Help inferior forces defeat superior forces.

© Copyright 2011


Takeaway




The targeted attacker cannot be discouraged from attacking his target.

© Copyright 2011

The APT strategy is different



- The usual attacker
 - Accesses and steals information
 - Uses it for competitive advantage
- The APT conducts that attack
- But it also
 - Maintains a much lower profile
 - Remains undetected
 - Establishes a way to return later
 - *And steal more.*



27 © Copyright 2011

Targets and Tactics



Targets




EVOLUTION OF TARGETS BY INDUSTRY

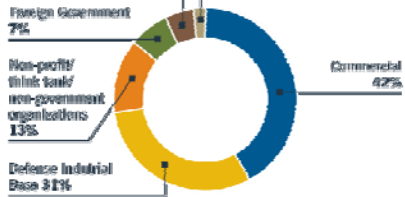


© Copyright 2011

2010 Investigations

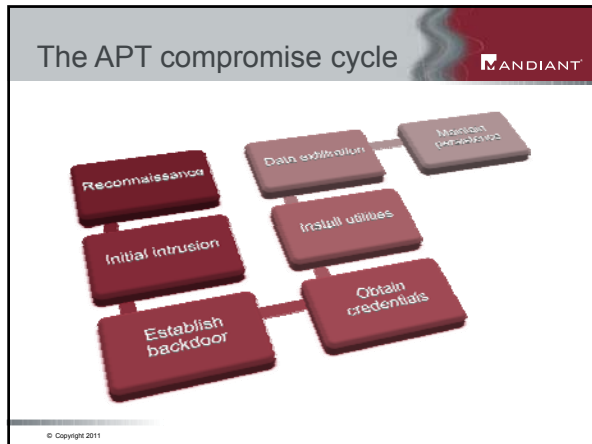


PERCENT OF OVERALL VICTIMS BY SECTOR



Sector	Percentage
Commercial	42%
Defense Industrial Base	31%
Non-profit/Think tank/non-government organizations	13%
Foreign Government	7%
U.S. Government	5%
Military	2%

© Copyright 2011



Persistence – basic

- Stability over stealth
 - Windows services
 - Autorun techniques
 - Users' Startup folder

USING WINDOWS SERVICES AS A PERSISTENCE MECHANISM

Generating Interesting 20%

Registry Run Keys 22%

Windows Services 78%

WINDOWS SERVICE REPLACEMENTS

- Attackers use services disabled by default
- Side Effect: Service no longer able to be used by system
- Popular Services used:
 - Windows Zero Configuration Service (wscntcfg)
 - RIP Listener Service (IPRIP)
 - Background Intelligent Transfer Service (BITS)

Persistence – advanced

- Advanced Techniques
 - Less reliable
 - More platform dependencies
 - "Something Interesting"
 - DLL search order hijacking
 - Group Policy Objects
 - COM objects
 - System binary modification

USING WINDOWS SERVICES AS A PERSISTENCE MECHANISM

Generating Interesting 20%

Registry Run Keys 22%

Windows Services 78%

Command and Control (C2)

- Old tricks
 - C2 in encrypted or obfuscated HTML comments
 - Data theft utilities using multipart RAR with free e-mail
- ¡Hola, nuevo social!
 - First stage malware downloader using Facebook
 - Backdoors using MSN and Google Chat
- Legitimize it
 - Stolen SSL credentials from victim used to encrypt C2

Lateral movement

- Once they're in...
- Credential theft:
 - Password hash dumping
 - Pass-the-hash
 - Keystroke logging
- Obtain domain admin
- Checkmate

LATERAL MOVEMENT TECHNIQUES

1. Attacker uploads malware to remote computer file share
2. Sends "all" job to execute malware


Types of Activities Accomplished:

- list tasks
- obtain directory listings
- download passwords
- install backdoors

What are they stealing?

- Everything
- Email
 - Sensitive data
 - Targeting information
 - Negotiation positions
 - Business plans
- Files
 - Research and development
 - New technology
 - Resource exploration



Data exfiltration




- Easy
 - FTP/SSH/HTTP POST files out the front door
 - Use public file-transfer facilities
- Medium
 - Use backdoors' file transfer functions
 - Hijack SSL credentials
- Hard
 - Establish their own layer 3 VPN
 - Ask @iiaimit for tips

© Copyright 2011

Case Study: Escalation


The situation



- Small enterprise of about 3,000 hosts
- Victim notified by law enforcement
- Attack activity attributed to one APT group
- Over 150 compromised hosts
- Period of compromise more than 2 years

39 © Copyright 2011


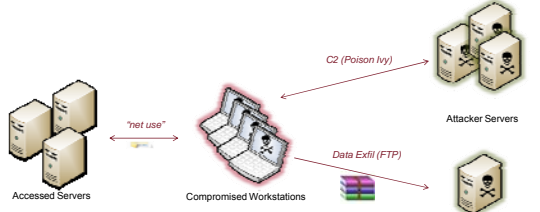
The attack



- Attacker used variants of common malware:
 - Poison Ivy backdoor: ~65 systems
 - ZXShell backdoor: ~10 systems
 - Hookmsgina login hook: ~25 systems
- Lateral movement using psexec
- Anti-virus detection during period of compromise: 0%

40 © Copyright 2011


The attack

- 150 compromised systems – mainly workstations
- 38 malware variants incl. 10 Poison Ivy variants
- ~20 C2 DNS and IP endpoints
- Exfil via 2GB multi-part RAR files staged on workstations and uploaded via FTP

41 © Copyright 2011

Attacker footprint



- Attacker used fewer than 10 of the backdoored hosts during the entire duration of compromise
- Proactively updated existing but unused backdoors across environment
- So why bother infecting so many hosts?

42 © Copyright 2011

The responder's challenge

- Many compromised hosts means...
 - Higher chance of detection, **BUT**
 - Higher chance of incomplete remediation effort
- One missed system can be an avenue for re-compromise...
- ...especially if its backdoor variant uses a C2 domain you don't know about

Poison Ivy IOC


- Developed specific and methodology Indicators of Compromise (IOCs) based on characteristics in memory, disk, and registry
- Examined each host in the environment for these indicators

```

OR
  File ADS Name contains exe
  AND
    Registry Text contains not ieuadint.exe
    Registry Text contains not Pund132.exe
    Registry Text contains not regsvr32.exe
    Registry Text contains not ietvsnat.exe
    Registry Text contains not unregmp2.exe
    Registry Text contains not shell32
    Registry Text contains not shaprate.exe
    Registry Text contains not unpopcm.exe
    Registry Text contains not OCInstallUserCon
    Registry Text contains not updr1.exe
    Registry Text contains not asissec.exe
  OR
    Registry Text contains C:\WINDOWS\system
    Registry Text contains C:\WINNT\system32
  AND
    Registry Path contains StubPath
    Registry Path contains not {4595913F-449
    Registry Path contains not {smartView930
  AND
    File Path contains Prefetch
    File Name is SYSTEM32
    
```

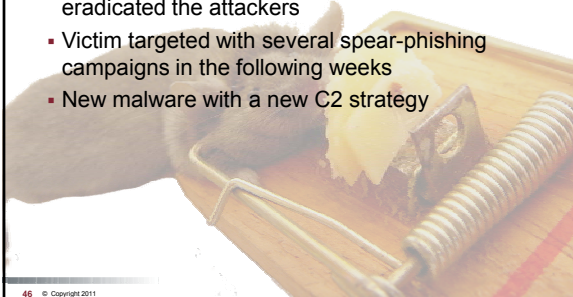
Resolution

- Defeating "shotgun" approach required enterprise-wide analysis
 - Host-based forensic artifacts
 - Network traffic
- Larger sample of attacker malware variants made it easier to develop indicators

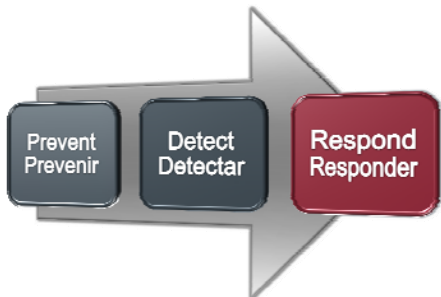


Thorough Remediation

- Significant enterprise-wide remediation effort eradicated the attackers
- Victim targeted with several spear-phishing campaigns in the following weeks
- New malware with a new C2 strategy



Phases of security



Prevent
Prevenir

Detect
Detector


Respond
Responder

Takeaway

Redefine what it means to win.

Winning incident response

- Winning means identifying, predicting and detecting
- NOT PREVENTING THE ATTACK
- NOT BEING SURPRISED
- Create, maintain, use threat intelligence
- Make the attacker work harder



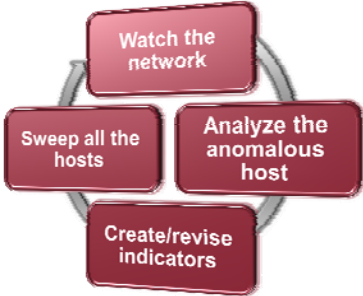
© Copyright 2011

Win: detecting incidents

- On the network
 - Look at network traffic in near real time
 - Correlate network traffic from different entities
 - Trace it back to the end host
 - Interpret the data stream contents
- On the host
 - Look at persistence
 - Look at installed software
 - Correlate attacker activity across hosts
 - Look at all the hosts you can

© Copyright 2011

Host/network feedback loop



© Copyright 2011

Differences

NETWORK	HOST
<ul style="list-style-type: none"> ▪ Network tells you <ul style="list-style-type: none"> - What is communicating now - What data is being moved now - Time patterns ▪ Network does not say <ul style="list-style-type: none"> - What happened while you weren't watching 	<ul style="list-style-type: none"> ▪ Host tells you <ul style="list-style-type: none"> - What is latent - Different variants of the same family - What data was moved previously ▪ Host does not tell you <ul style="list-style-type: none"> - What is happening right now


© Copyright 2011

Win: responding

- Avoid premature remediation
 - Know the true scope of the incident
 - Don't turn and burn hosts
- Keep the team small
- Integrated operations
 - Host and network at the same time
 - Big bang approach, no rolling remediation
 - ... at first

© Copyright 2011

Winning on the host



© Copyright 2011

Sources of host-based data

MEMORY ANALYSIS

- Driver enumeration
- Handles and sections
- Per-process memory space acquisition
- Kernel hook enumeration
- Injection detection
- Network connections

OTHER USEFUL STUFF

- Web history
 - URLs, cookies, forms, files
- Prefetch file parsing
- Raw or API access to disk, memory, registry
- ARP, DNS cache, route table
- Stealth

55 © Copyright 2011

Things for super-geniuses

PE & DRIVER ANALYSIS

- Imports, exports
- Entropy calculations
- Anomaly detection
 - JMP detours
 - Past-EOF data
 - PE checksums
 - Compiler/packer signatures
- Signature validation
- Resources, strings

SCALED IR OPERATIONS

- Indicators of Compromise
 - Enable large-scale ops
 - Reduce false positives*

56 © Copyright 2011

Stuxnet (Signature)

© Copyright 2011

Stuxnet (Data Reduction)

© Copyright 2011

Whitelisting within IOCs

IOC for "WINDOWSHELP" staging area

```

OR
AND
- File Name is not hhupd.exe
- File Name is not bntps.dll
- File Name is not tour.exe
- File Name is not sniffpol.dll
- File Name is not sstub.dll
- File Name is not tshoot.dll
- File Name is not cobewrap.exe
- File Name is not splshrep.exe
- File Name is not d2hlink32.dll
- File Name is not d2hnav32.exe
- File Name is not d2htl32.dll
- File Name is not hhoolreq.dat
OR
- File Path contains \windows\help
- File Path contains \winnt\help
OR
- File Extension is dll
- File Extension is exe
- FileItem/PEInfo/Type is Executable
- File Extension is rar
- File Extension is bat
    
```

Whitelist valid OS files in this path

Define path

Look for bad stuff

© Copyright 2011

Methodology IOCs

```

UK
AND
- File Name is index.dat
- File Strings contains System Volume Information
AND
- File Name contains hh.dat
- File Strings contains 2011 Salary.chm
- URL History URL contains www.innocuous-site.org
- EventLog user contains ADOMAIN\User12
- File Owner is ADOMAIN\User12
    
```

Activity-based:

- Files opened
- CHM file opened
- Website visited

Username-based:

- Events generated by user
- Files owned by user

These IOCs are powerful methods to track down the activity of an attacker.

© Copyright 2011

MANDIANT

**Look for what the attacker does,
don't just look for his tools.**

© Copyright 2011

MANDIANT

Premature remediation

- Removing compromised systems immediately
 - Only alerts the attacker that you know how to find him
 - Starts the chase
 - Do you know the story about the bear in the woods?
- Blocking IP addresses / DNS lookups
 - Same deal, unless you know *all* of them
- Changing some passwords
 - Tells the attacker which accounts he can't use anymore

© Copyright 2011

MANDIANT

Why not just use anti-virus?

- Submitting curious malware to A/V or VirusTotal
 - Gives your A/V company control of your incident
 - Alerts a whole bunch of Russian reversers
- Gives you low-quality signatures
 - A/V vendors are metriced on speed, not quality
 - See the *Take Back Netcat* paper (a great read)



© Copyright 2011

MANDIANT

Increase the difficulty

Increase Visibility	Harden the Target
<ul style="list-style-type: none"> • Host-based visibility • Network-based visibility • Logging • DNS • DHCP • VPN • Windows Security Events 	<ul style="list-style-type: none"> • Admin reduction • Password complexity • Credential cache • Disable LANMAN • Patch management • End user training

© Copyright 2011

MANDIANT

Remember to define the win

- The target *is* usually compromised again
- Their win:
 - Faster identification
 - Smaller remediation effort
 - Normal operations vs. surge response
 - Ongoing managed cost vs. uncontrolled emergency expense

© Copyright 2011

MANDIANT

Takeaway

You are winning when you:
Make it harder for the attacker
Make detection faster and repeatable
Make response easier

© Copyright 2011

Takeaway

**You are winning when:
YOU GET TO GO HOME FOR DINNER**



© Copyright 2011

Resources

The bad guys have them, do you?




68 © Copyright 2011

Free resources

- Free tools
 - Redline
 - IOCe
 - Memoryze
 - Audit Viewer
 - Highlighter
 - Red Curtain
 - Web Historian
 - First Response
- Resources
 - M-trends
 - M-union
 - blog.mandiant.com
- Education
 - Black Hat classes
 - Custom classes
- Webinar series
- OpenIOC initiative

69 © Copyright 2011

MANDIANT Redline




- Guided memory analysis
- Aimed at less-experienced responders
- Malware investigations
 - Process user match
 - Injection detection
 - Digital signature validation
 - DLL scoring
- Word report generation
- New version on 30 Nov

NUEVO

70 © Copyright 2011

Malware analysis class


- Like our Black Hat course, only colder
- Learn
 - How to investigate unknown malware
 - Static and dynamic analysis
 - IDA, Olly, assembly
- Alexandria, Virginia US
- Dec 12 – 16, 2011
- \$4,900



71 © Copyright 2011

Live incident response

- Remotely
 - Collect data (e.g. web history, file listings, registry)
 - Perform forensic tasks on live systems
 - Obtain binaries of interest
 - Translate intelligence into IOC format



72 © Copyright 2011

MCIRT

The diagram illustrates the MCIRT architecture. At the top, 'Internet' connects to a 'Network Sensor'. The sensor feeds into the 'MCIRT Portal', which is linked to a 'MIR Controller'. The controller then feeds into 'Endpoint Threat Detection'. Below this, 'Threat Intelligence' is shown as a central hub, with 'Customers' on either side. The entire system is managed by the 'MANDIANT Security Operations Center (SOC)'.

- 24 x 7 monitoring by Mandiant's team of expert threat analysts
- Sweeps all endpoints to detect advanced targeted attacks
- Watch network traffic to detect ongoing attacks
- Correlates indicators of attack against the most recent tactics

73 © Copyright 2011

Education services

- We train the U.S. FBI and U.S. Secret Service
- We have taught other governments as well (shhh)
- We support active criminal investigations
- We are PCI Forensic Investigators

© Copyright 2011

Professional Services

- Incident Response
- Proactive Security Assessments
- Computer Forensics & Litigation Support
- Research & Development
- Cyber Security

© Copyright 2011

Discussion

Michael J. Graven
 @mjg5772
 michael.graven@mandiant.com
 Tel. +1 650 740 2304

© Copyright 2011