Chris Bream | Manager

MANDIANT®

The State of the Hack

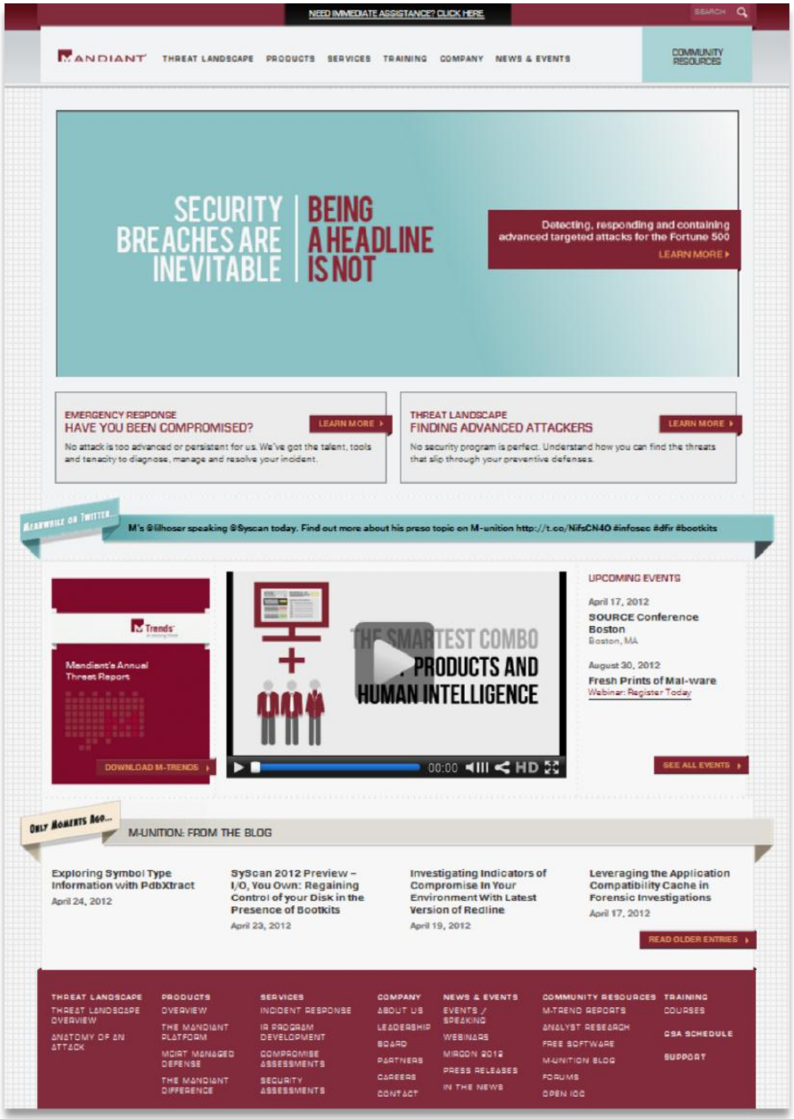
Rocky Mountain Information Security Conference
May 18, 2012

Agenda

- The Threat
- Anatomy of an Attack
- Compromise Case Studies
- Preparing Your Organization Today and Beyond
- Resources

We are Mandiant

- Threat detection, response and containment experts
- Software, professional & managed services, and education
- Application and network security evaluations
- Offices in
  - Washington
  - New York
  - Los Angeles
  - San Francisco



SECURITY BREACHES ARE INEVITABLE | BEING A HEADLINE IS NOT

Detecting, responding and containing advanced targeted attacks for the Fortune 500

EMERGENCY RESPONSE
HAVE YOU BEEN COMPROMISED?

No attack is too advanced or persistent for us. We've got the talent, tools and tenacity to diagnose, manage and resolve your incident.

THREAT LANDSCAPE
FINDING ADVANCED ATTACKERS

No security program is perfect. Understand how you can find the threats that slip through your preventive defenses.

M's @lilhoser speaking @Syscan today. Find out more about his preso topic on M-unition http://t.co/NifsCN40 #infosec #dfir #bootkits

Mandiant's Annual Threat Report

THE SMARTEST COMBO PRODUCTS AND HUMAN INTELLIGENCE

UPCOMING EVENTS

April 17, 2012
SOURCE Conference Boston
Boston, MA

August 30, 2012
Fresh Prints of Mal-ware
Webinar: Register Today

M-UNITION: FROM THE BLOG

Exploring Symbol Type Information with PdbXtract
April 24, 2012

SyScan 2012 Preview – I/O, You Own: Regaining Control of your Disk in the Presence of Bootkits
April 23, 2012

Investigating Indicators of Compromise In Your Environment With Latest Version of Redline
April 19, 2012

Leveraging the Application Compatibility Cache in Forensic Investigations
April 17, 2012

The Threat

All information is derived from MANDIANT observations in non-classified environments

Some information has been sanitized to protect our clients' interests

“APT” Used and Abused

- (Who | what | how) is the APT?

“As hackers have realized that static malicious code is easily thwarted, **new methods, known as advanced persistent threats (APTs) are being employed […] to evade detection**.”

“If an APT cannot connect with its criminal operators, then it cannot transmit any intelligence it may have captured […] This characteristic makes **APTs appear as a sub-category of botnets.”**

“APT is the new way attackers are breaking into systems. **APT is a sophisticated, mercurial way that advanced attackers can break into systems**…”

“While APT malware can remain stealthy at the host level, the network activity associated with remote control is more easily identified. As such, **APT’s are most effectively identified, contained and disrupted at the network level**.”

“Spyware of the early to mid 2000’s was advanced […] **and** persistent […] until anti-spyware defenses came about. So, **advanced persistent threats really aren’t anything new**…”

“**The use of APTs is on the rise** by a growing group of malicious attackers committed to their targets.”

The APT per Bejtlich

- **Advanced**
  - The adversary can operate in the full spectrum of computer intrusion
  - They can use the most pedestrian publicly available exploit against a well-known vulnerability
  - They can elevate their game to research new vulnerabilities and develop custom exploits
  - Depends on the target's posture

The APT per Bejtlich

- **Persistent**
  - The adversary is formally tasked to accomplish a mission
  - They are not opportunistic intruders
  - Like an intelligence unit they receive directives and work to satisfy their masters
  - Persistent does not necessarily mean they need to constantly execute malicious code on victim computers
  - They maintain the level of interaction needed to execute their objectives

The APT per Bejtlich

- **Threat**
  - The adversary is not a piece of mindless code. This point is **crucial**.
  - Some people throw around the term "threat" with reference to malware
  - If malware had no human attached to it, then most malware would be of little worry (as long as it didn't degrade or deny data)
  - The adversary here is a threat because it is organized and funded and motivated
  - Some people speak of multiple "groups" consisting of dedicated "crews" with various missions

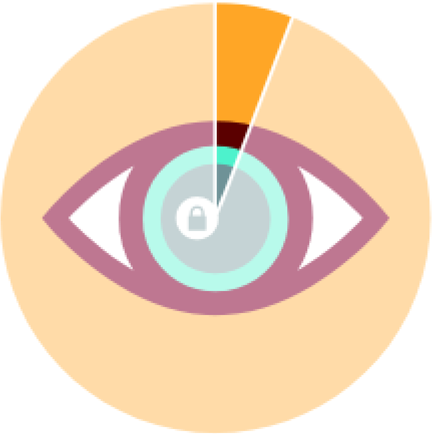
Who are the Victims?

- Any source of data that can provide political, military, or economic advantage
  - Defense contractors
  - Energy and mining companies
  - High-tech companies
  - Multi-national companies
  - Political figures and organizations
  - Law firms
  - Manufacturing companies
  - Pharmaceutical companies
- Typically not interested in PII, credit cards, PHI, etc.

What do they Steal?

- Intelligence for economic trade
- Engineering schematics
- Intellectual property
- Financial information for product manufacturing
- Email related to business strategies
  - Big ticket items place email at risk
- Legal strategies
- Military intelligence
- M&A intelligence

Intrusions by the Numbers



6% Self-Detection

94% External Notification

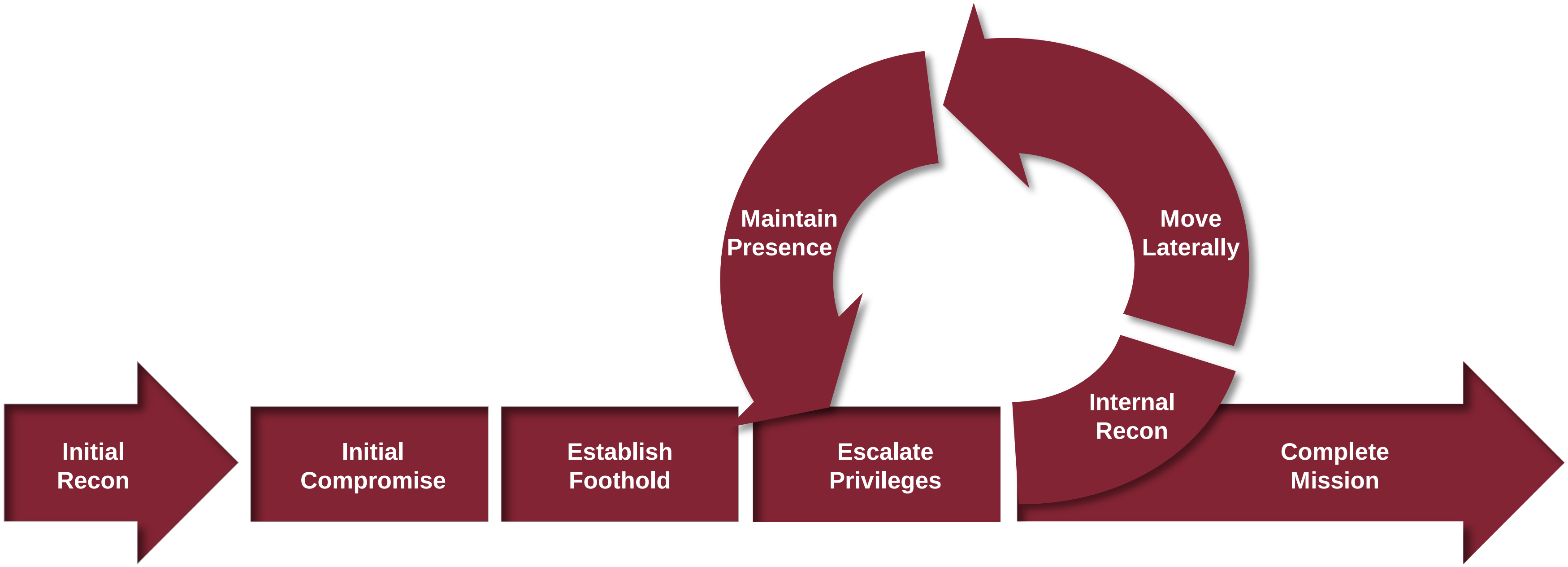
100% Valid Credentials

416 Days Average Length of Compromise

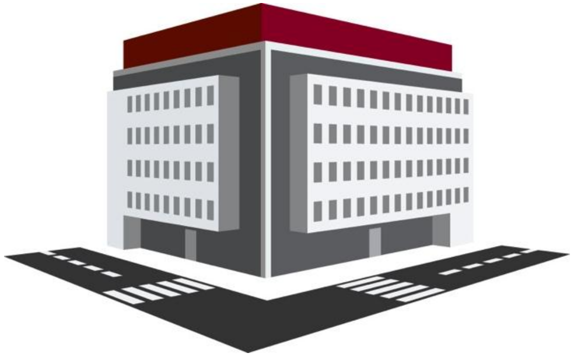
Anatomy of an Attack

The Attack Lifecycle

- Understanding the lifecycle can help your response and defense
- Remember there is intelligence on the other end of the attack so knowing your adversary is critical



APT Attack: Setting the Stage



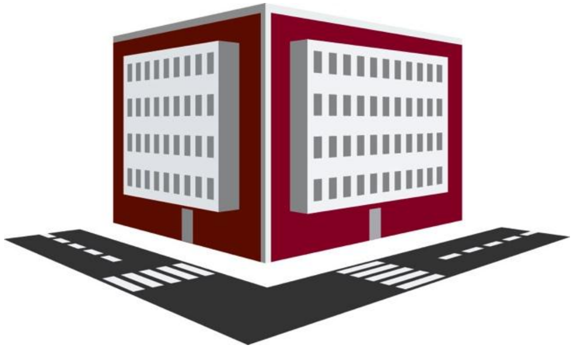
Company A

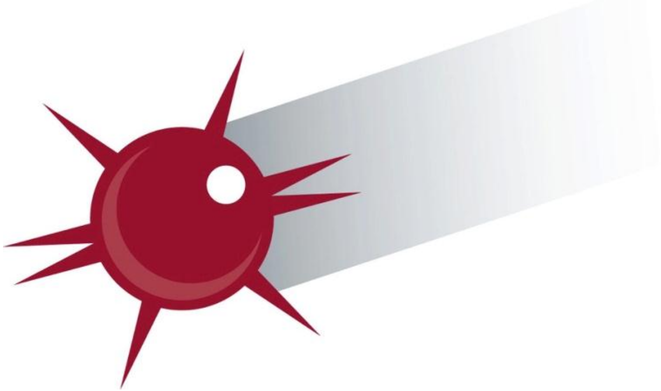
- Manufactures high-tech machinery
- Offices in 49 countries
- 20,000 employees
- 24,000 workstations and laptops, 3,000 servers

Company B

- Manufactures parts for some of Company A’s products

APT Attack: Setting the Stage





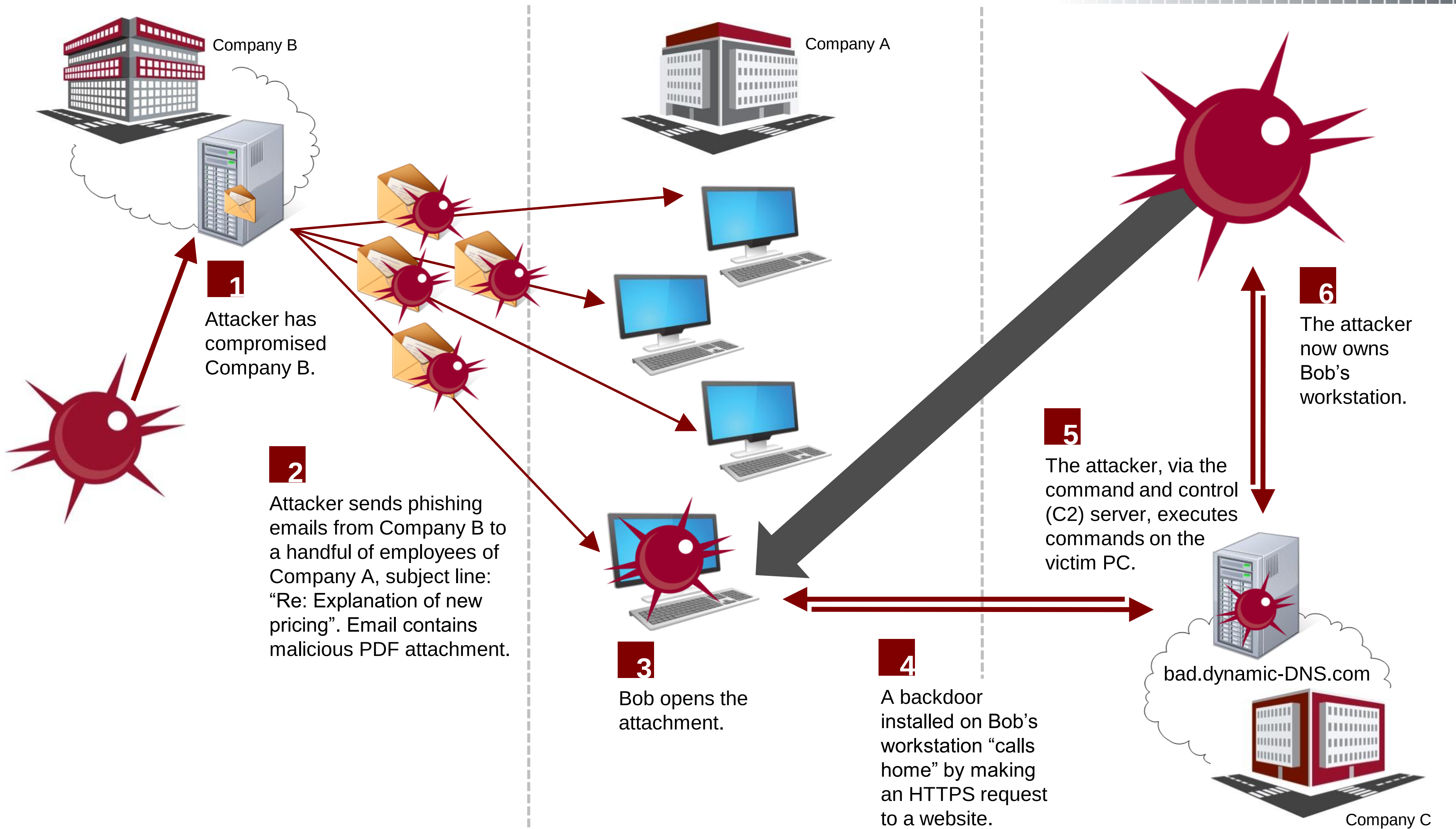
Company C

- Another compromised company, or ISP

The Attacker

- Works on a regular schedule – this is a job
- Receives assignments to obtain certain information
- Uses both custom-built and freely-available tools

APT Attack: Day One



1 Attacker has compromised Company B.

2 Attacker sends phishing emails from Company B to a handful of employees of Company A, subject line: “Re: Explanation of new pricing”. Email contains malicious PDF attachment.

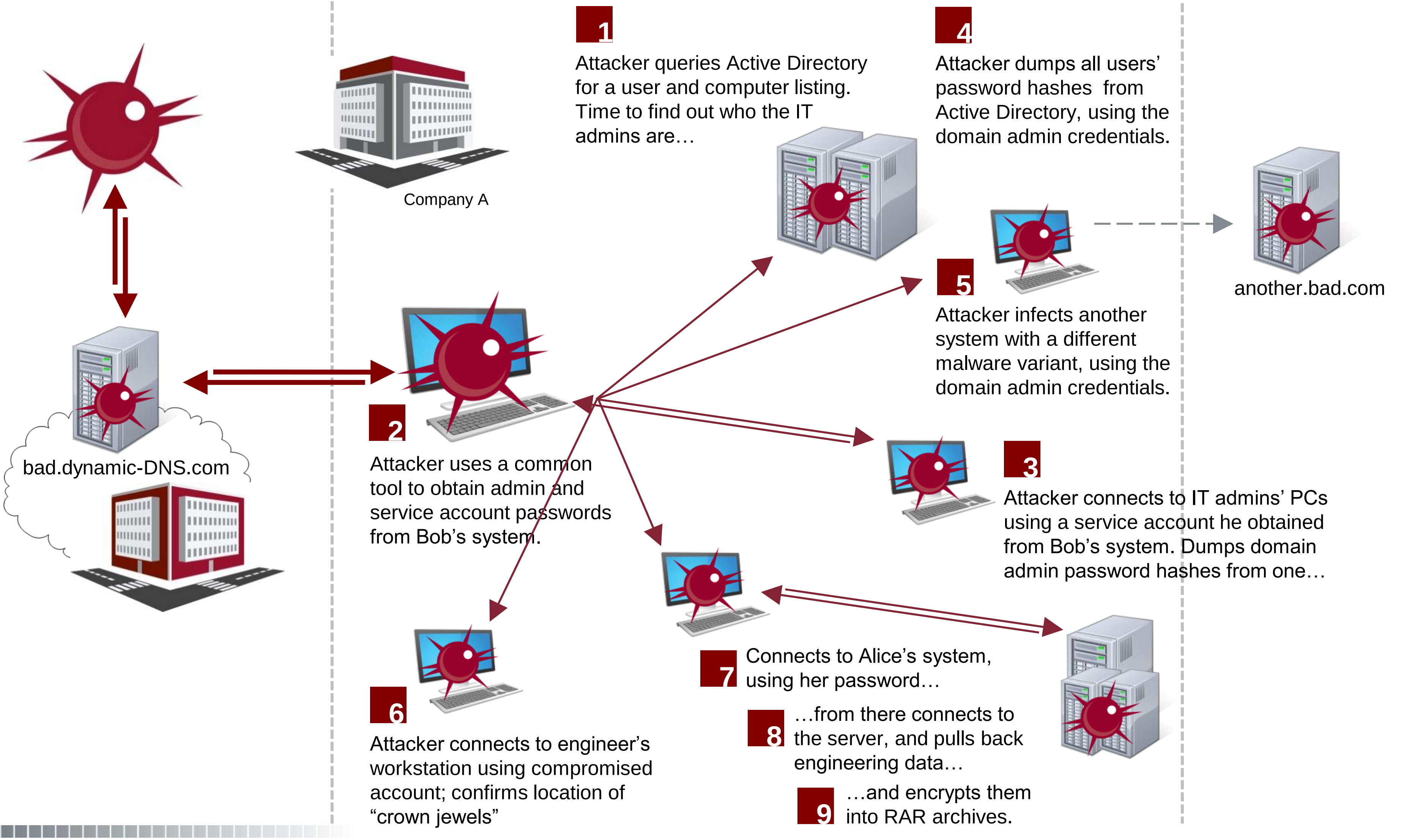
3 Bob opens the attachment.

4 A backdoor installed on Bob’s workstation “calls home” by making an HTTPS request to a website.

5 The attacker, via the command and control (C2) server, executes commands on the victim PC.

6 The attacker now owns Bob’s workstation.

APT Attack: Days Two – Four



1 Attacker queries Active Directory for a user and computer listing. Time to find out who the IT admins are…

2 Attacker uses a common tool to obtain admin and service account passwords from Bob's system.

3 Attacker connects to IT admins' PCs using a service account he obtained from Bob's system. Dumps domain admin password hashes from one…

4 Attacker dumps all users' password hashes from Active Directory, using the domain admin credentials.

5 Attacker infects another system with a different malware variant, using the domain admin credentials.

6 Attacker connects to engineer's workstation using compromised account; confirms location of "crown jewels"

7 Connects to Alice's system, using her password…

8 …from there connects to the server, and pulls back engineering data…

9 …and encrypts them into RAR archives.

Takeaway

- The organization was targeted for a reason

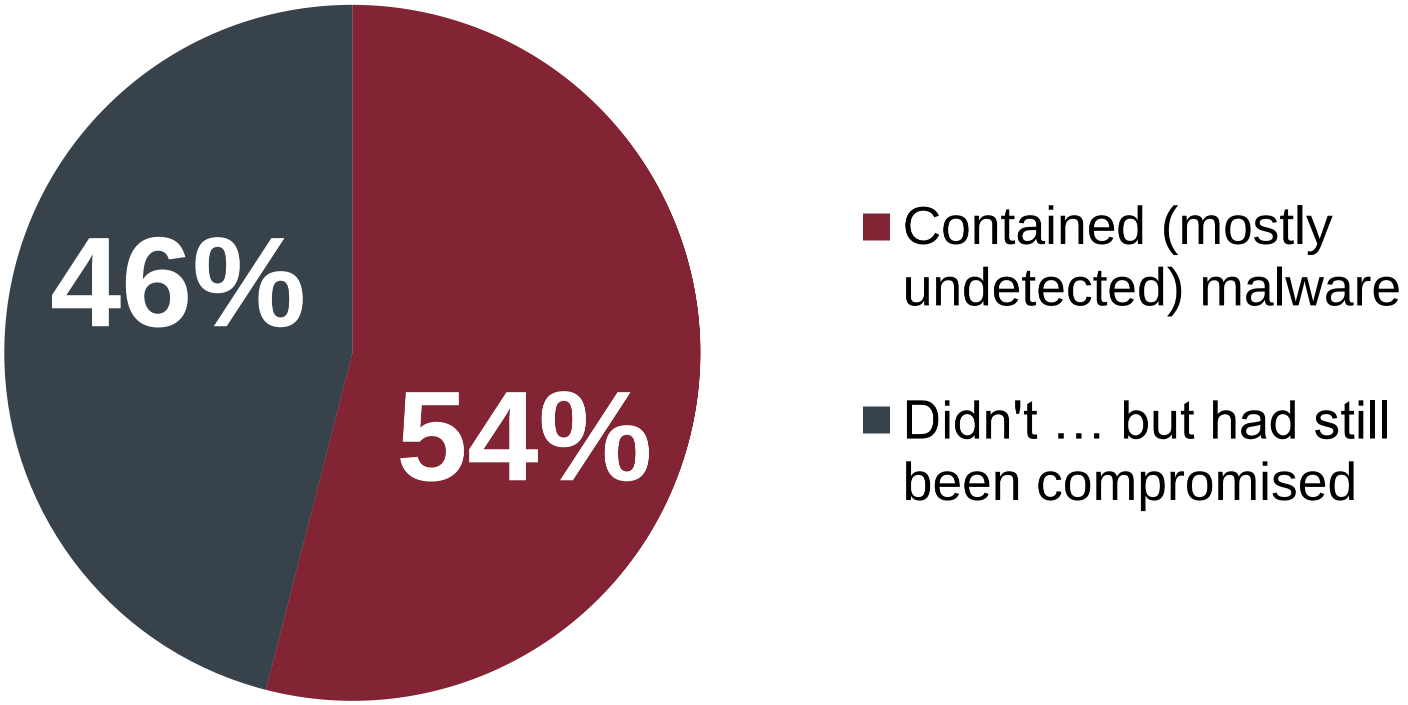
- The attacker had specific goals
  - Accomplish their mission
  - Remain undetected
  - Maintain access to the network

- Defense is not what it used to be
  - The focus is on detecting and responding quickly
  - Goal is to remediate the attack

Compromise Case Studies

How’s that Malware Detection Workin’ for ya?

Of the compromised systems…



It’s All About the Scoping

- Scoping is key to remediation
- Malware detection only tells half the story
- Must look for other indicators of compromise across the entire enterprise
- Investigations must include analysis of many system artifacts

Unaudthorized Use of Valid Accounts

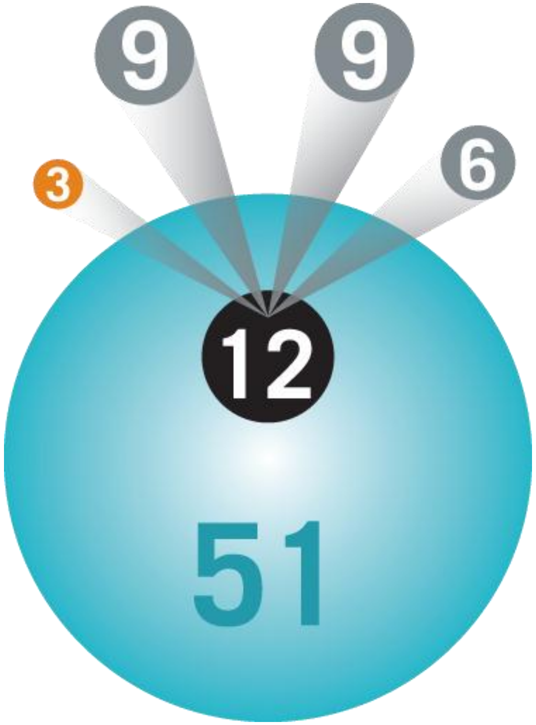
Trace Evidence & Partial Files

Remote System/File Access

Overview of Two Cases

- Indicators generally found in more than one place
- Some systems had more than one malware family on them
- Thus, quantity of malware doesn’t exactly match the number of infected systems

Technology Company



30,000 TOTAL SYSTEMS

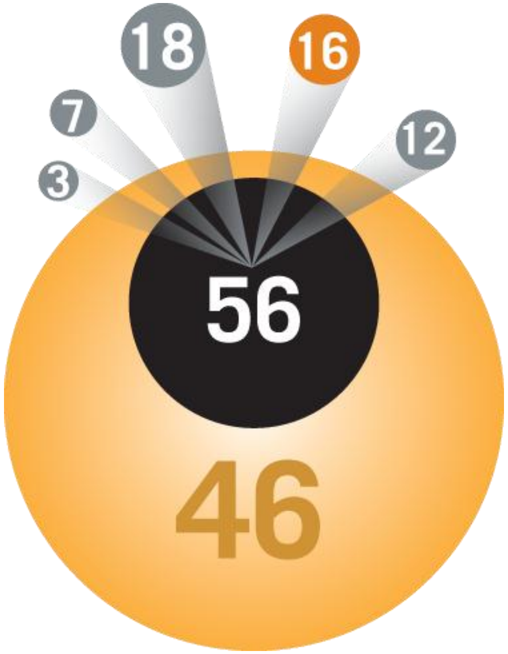
63 COMPROMISED SYSTEMS

12 SYSTEMS CONTAINED MALWARE

51 COMPROMISED SYSTEMS w/o MALWARE

Qty	Type of Malware or Utility
3	Proprietary malware only
9	Poison Ivy Remote Access Trojan
6	Windows Credential Editor
9	PsExec
27	Pieces of Malware or Utilities

High Tech Defense



OVER 6,000 TOTAL SYSTEMS

102 COMPROMISED SYSTEMS

56 SYSTEMS CONTAINED MALWARE

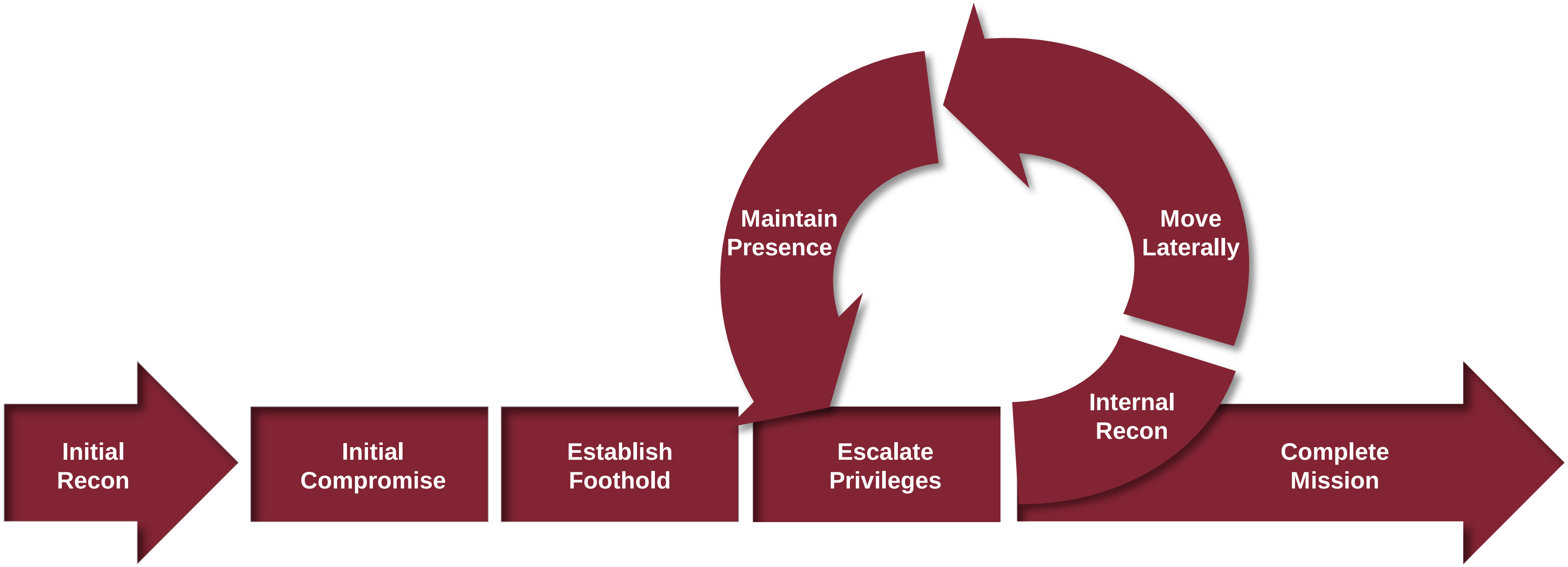
46 COMPROMISED SYSTEMS w/o MALWARE

Qty	Type of Malware or Utility
16	Proprietary malware only
18	Gh0st Remote Access Trojan
3	ASPXSpy
7	GetHashes
12	PsExec
56	Pieces of Malware or Utilities

Preparing Your Organization Today and Beyond

So What do we Do?

- Relax, this happens all the time
- Understand the lifecycle
- Become investigation-ready and then build a more effective defense now and in the future



Become Investigation-Ready

- Inventory sensitive systems and data
- Build or outsource an IR team whose sole job is investigations
- Define an IR plan
- Aggregate log sources into a SIEM tool
- Record and preserve logs for at least one year
- Augment monitoring mechanisms with a threat-based monitoring service
- Conduct tabletop exercises to test the IR plan

Develop Defenses for Initial Recon

Initial Recon

- Posturing
  - Implement education campaign on spear-phishing
  - Test effectiveness of education with social engineering attack simulations
- Strategic
  - Educate users on appropriate use of social media and how targeted threats operate
  - Conduct awareness sessions targeted to IT admins, executives, and other targeted groups

Develop Defenses for Initial Compromise

Initial Compromise

- Posturing
  - Patch third-party end-user applications
  - Tune HIPS/antivirus
  - Implement host-based firewall controls on endpoints
  - Test defenses with social engineering attack simulations
  - Implement email attachment filtering, subject modifications, and warning messages
- Strategic
  - Implement application sandboxing (e.g. browser, PDF reader, Java)
  - Reduce user privileges (Revoke “local administrator” privileges, Privileged Identity Management Tool, UAC)

Develop Defenses for Establishing Foothold

Establish Foothold

- Posturing
  - Deploy application whitelisting to systems performing high volume authentication
  - Deploy application blacklisting to all systems
  - Implement DNS request logging
  - Block dynamic DNS and uncategorized websites
- Strategic
  - Enhance SOC capabilities to drive down the “dwell time”
  - Tune logging and monitoring capabilities to provide SOC effective and timely intel

Develop Defenses for Escalating Privileges

Escalate Privileges

- Posturing:
  - Disable LM hashes (partial mitigation)
  - Deploy application whitelisting to systems performing high volume authentication
  - Deploy application blacklisting to all systems
  - Conduct account inventory, understand application dependencies
  - Tune antivirus/HIPS to block known tools
- Strategic
  - Reduce privileged service accounts' footprint
  - Reduce service account privileges
  - Reduce user privileges (Revoke "local administrator" privileges, Privileged Identity Management Tool, UAC)

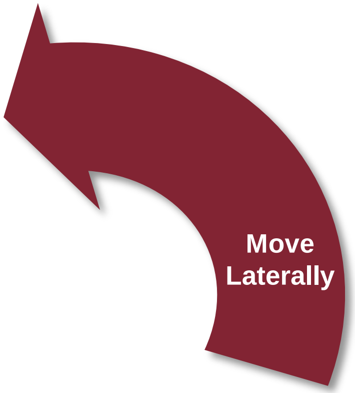
Develop Defenses for Internal Recon

Internal Recon

- Posturing
  - N/A
- Strategic
  - Implement zone-based network segmentation
  - Review and reduce file share and folder permissions
  - Tune SIEM to more effectively detect unusual authentication patterns

Develop Defenses for Lateral Movement

- Posturing
  - Configure appropriate event log settings
  - Aggregate and monitor security event logs
    - Local administrator account logons (local and network)
    - Privileged service account logons
    - Privileged administrator account logons
  - Implement host-based firewall controls on workstations/laptops
  - Disable local administrator or enforce unique passwords
- Strategic
  - Tune SIEM to more effectively detect unusual authentication patterns
  - Implement multi-factor authentication
  - Implement zone-based network segmentation



Develop Defenses for Maintain Presence

- Posturing
  - Deploy application whitelisting to systems performing high volume authentication
  - Deploy application blacklisting to all systems
  - Develop process to expand reach of host- and network-based indicators to identify known malware
  - Review VPN accounts, harden VPN provisioning systems
  - Web-root version control
  - Block dynamic DNS and uncategorized websites
- Strategic
  - Implement multi-factor authentication

Develop Defenses for Complete Mission

Complete Mission

- Posturing
  - Review antivirus logs
  - Regular network monitoring by someone familiar with the normal behavior of the network
  - File integrity monitoring software on web servers
- Strategic
  - Develop damage assessment capabilities to understand the business impact of data theft

Wrap-up

M-Trends 2012

Download the full report
http://www.mandiant.com

Mandiant Webinars

STATE OF THE HACK

- Designed for all technical levels
- Case study format
- Illustrates the latest attacks we are seeing

FRESH PRINTS OF MALWARE

- Designed for the technical user
- Case study format
- Digs deeper into the technical aspects of the incidents we respond to

Interact

Twitter	www.twitter.com/mandiant
LinkedIn	www.linkedin.com/company/mandiant
Facebook	www.facebook.com/mandiantcorp
YouTube	www.youtube.com/mandiantcorp

Free Software

IOCFinder	look for evil on your endpoints
Redline	answers the question: are you compromised?
Web Historian	browser analysis
Memoryze	memory forensics
Highlighter	log analysis
Red Curtain	malware identifier
IOCe	indicator of compromise editor
OpenIOC	common language to describe IOCs
Heap Inspector	detect heap spray in memory
Shim Cache Parser	look for trace evidence of executing evil

Mandiant is Hiring

- Positions in
  - Consulting, federal and managed services
  - Product development
  - Sales
- Locations
  - Alexandria, VA
  - New York
  - Los Angeles
  - San Francisco
  - Reston, VA
- http://www.mandiant.com/careers

Questions?

- Chris Bream
  - chris.bream@mandiant.com

- More MANDIANT info
  - http://www.mandiant.com/
  - http://www.twitter.com/mandiant
  - info@mandiant.com