black hat USA 2012

Targeted Intrusion Remediation:

Lessons From The Front Lines

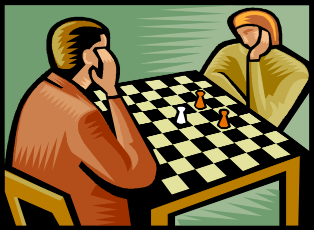
Jim Aldridge

MANDIANT®

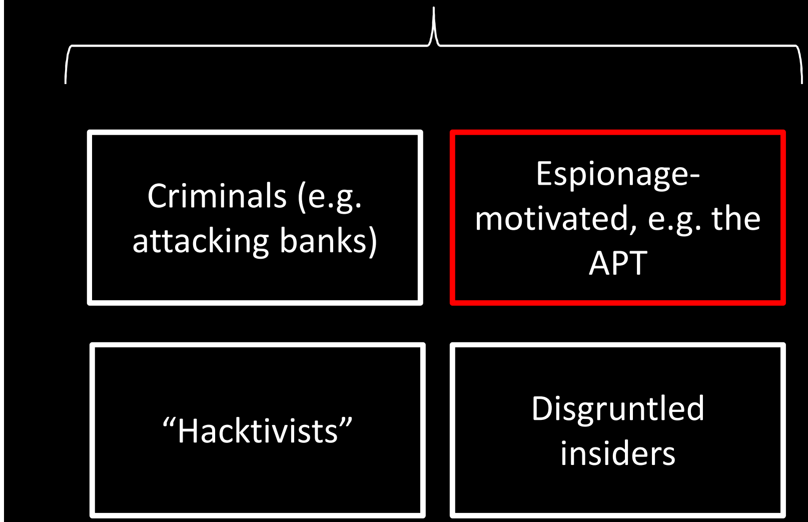
All information is derived from MANDIANT observations in non-classified environments.

Information has been sanitized where necessary to protect our clients' interests.

Remediating intrusions by targeted, persistent adversaries requires a different approach



Targeted



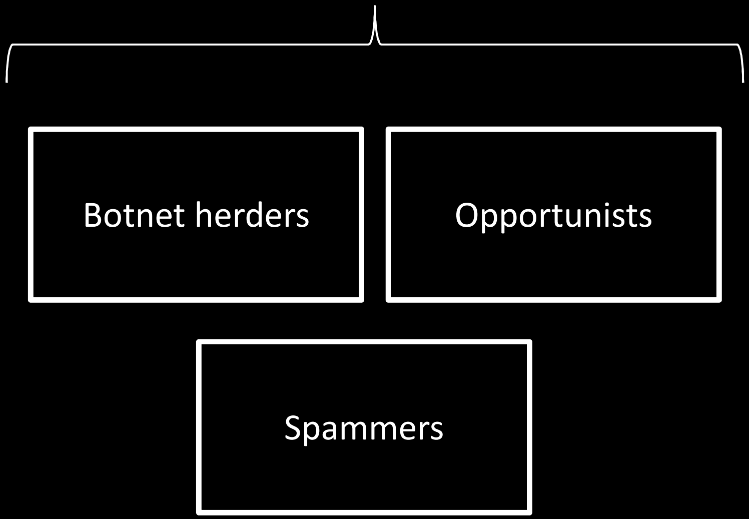
Criminals (e.g. attacking banks)

Espionage-motivated, e.g. the APT

“Hacktivists”

Disgruntled insiders

Non-Targeted



Botnet herders

Opportunists

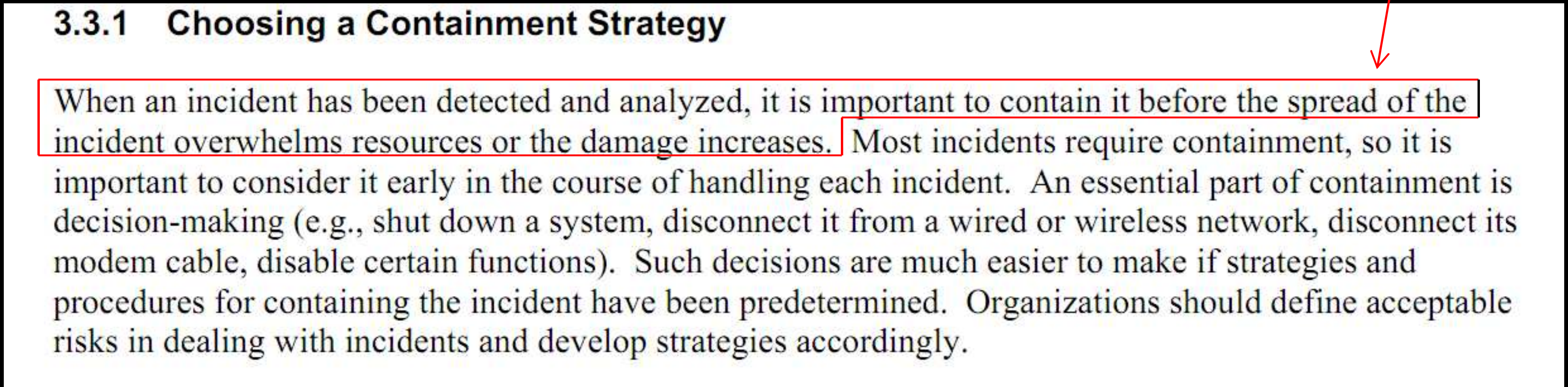
Spammers

- **Targeted**
  - The adversary chose your organization for a reason
  - Today, they want some piece of electronic information
  - …And will likely want more in the future
  - They are not opportunistic intruders

- **Persistent** **(adopted from Richard Bejtlich's definition of APT)**
  - The adversary is formally tasked to accomplish a mission
  - 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

- **Threat** **(adopted from Richard Bejtlich's definition of APT)**
  - 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

Traditional IR Doctrine



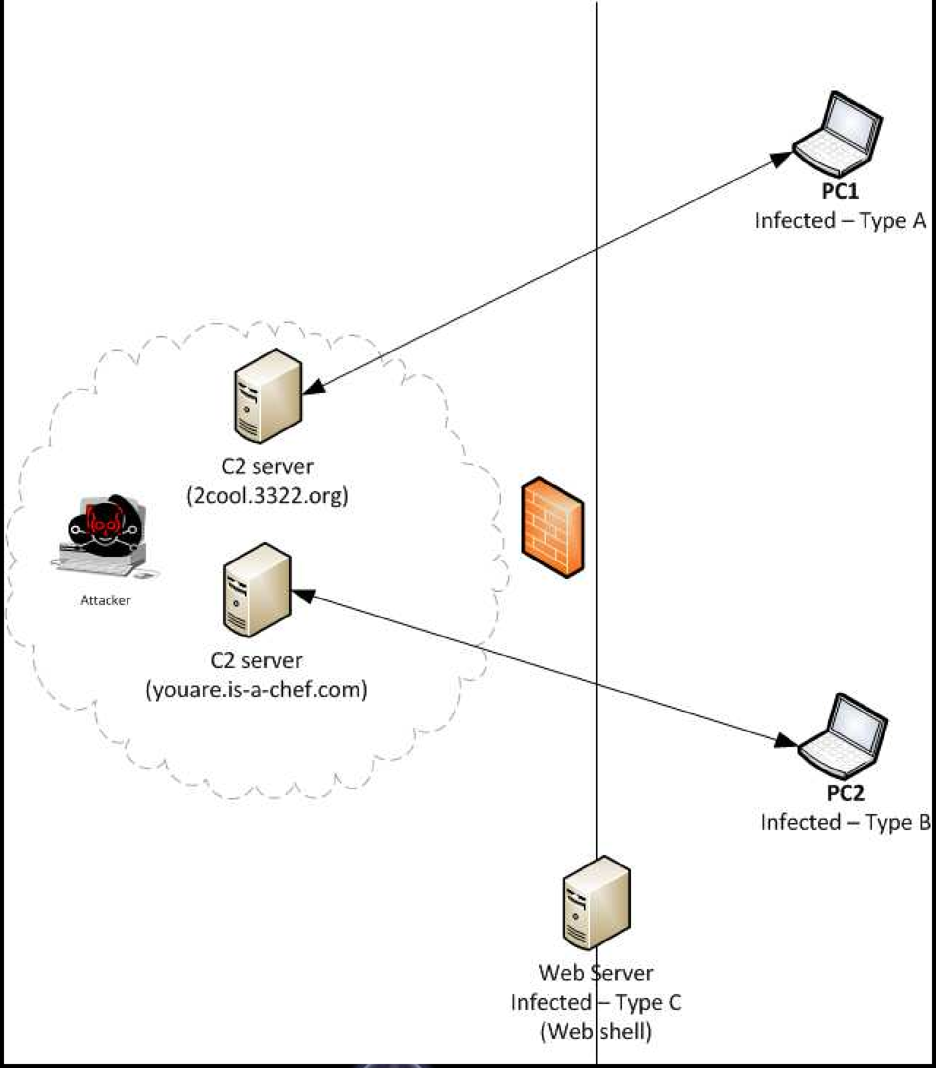
3.3.1 Choosing a Containment Strategy

When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a wired or wireless network, disconnect its modem cable, disable certain functions). Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61 Revision 1

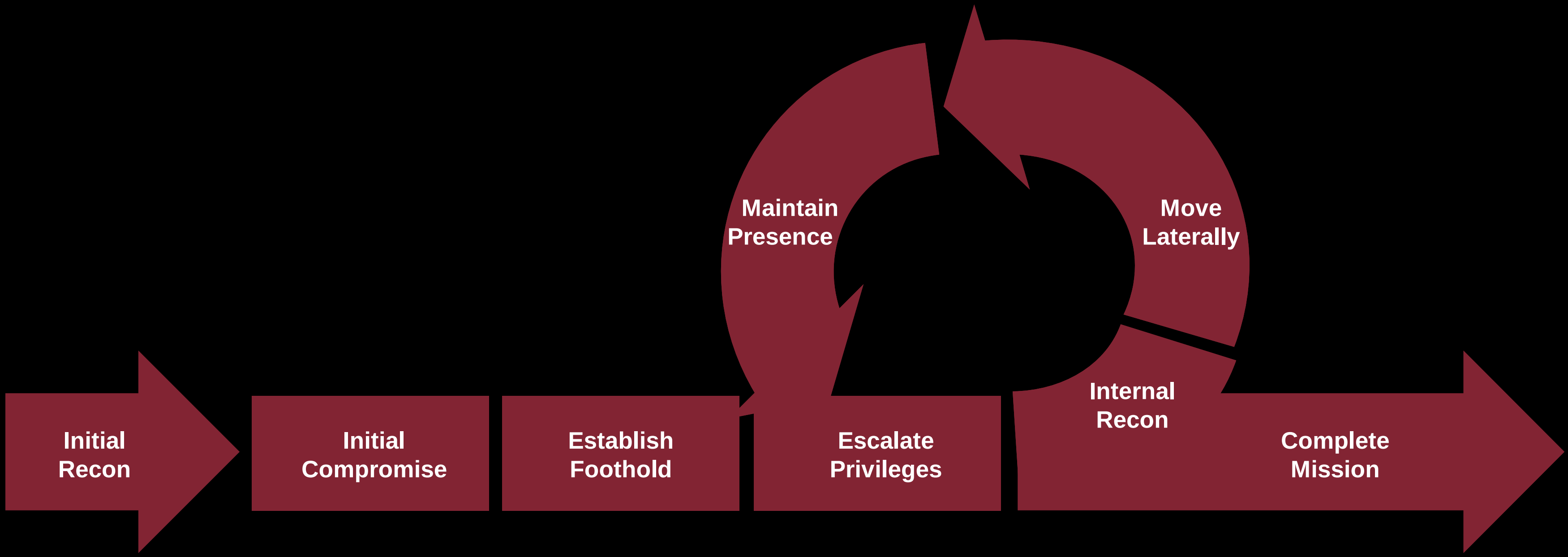
…updated for the modern era



Agenda

- Targeted attack lifecycle
- Recommended approach
  - Background: IR = Investigation + Remediation
  - Prioritizing: The Remediation Planning Matrix
  - The Remediation Event
  - Posturing
  - Strategic Activities

TARGETED ATTACK LIFECYCLE



Initial Recon

Initial Compromise

Establish Foothold

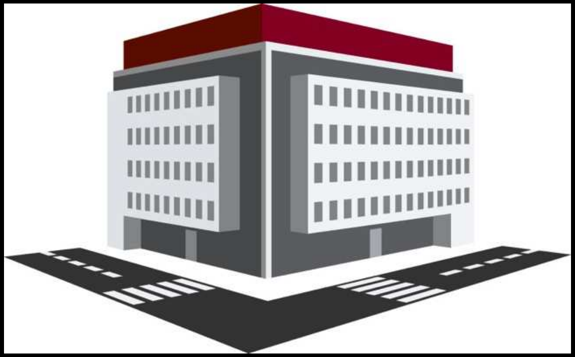
Escalate Privileges

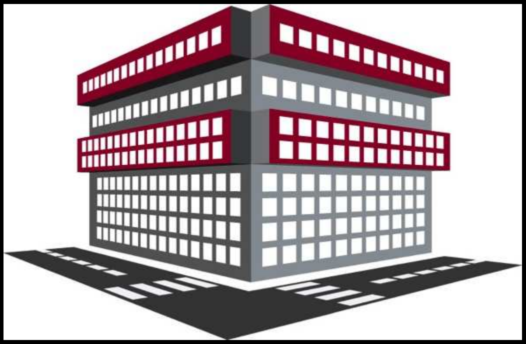
Internal Recon

Move Laterally

Maintain Presence

Complete Mission





Company A

High tech manufacturer

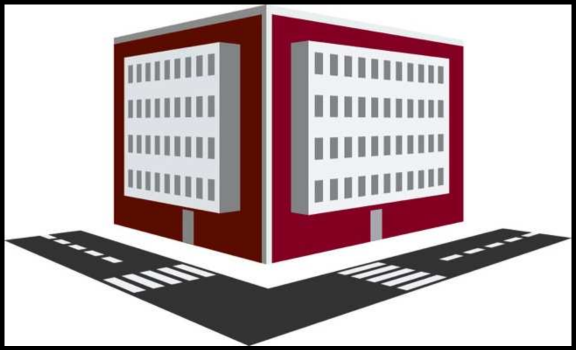
Global presence

20,000 employees

24,000 workstations and laptops, 3,000 servers

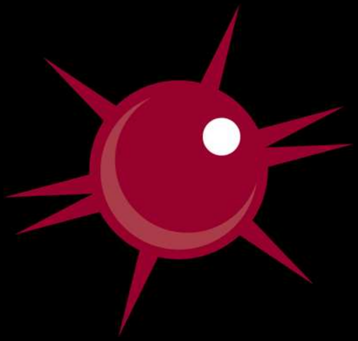
Company B

Supplier to company A



Company C

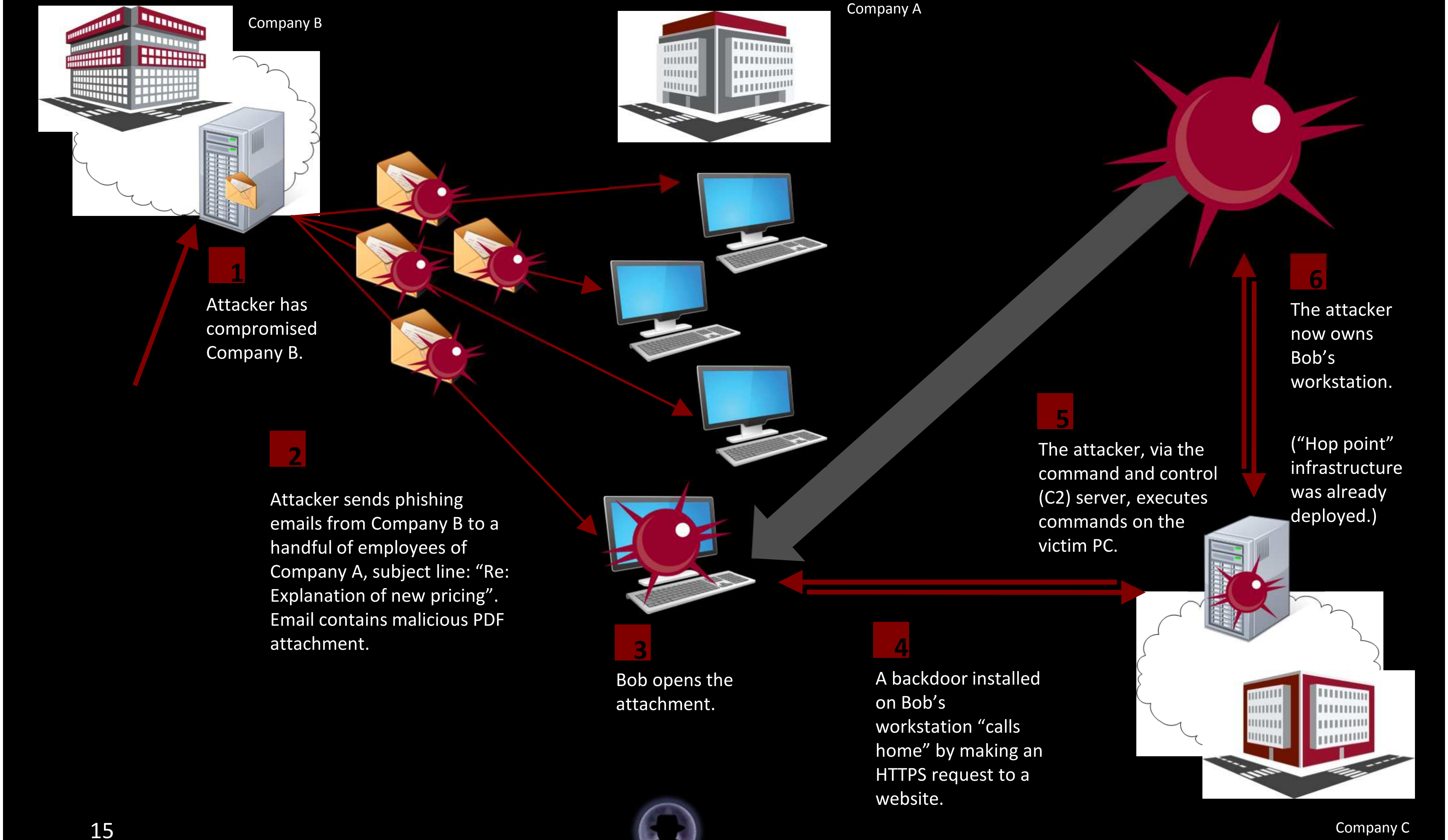
A service provider



Targeted, Persistent Attacker

Works on a regular schedule – this is a job

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

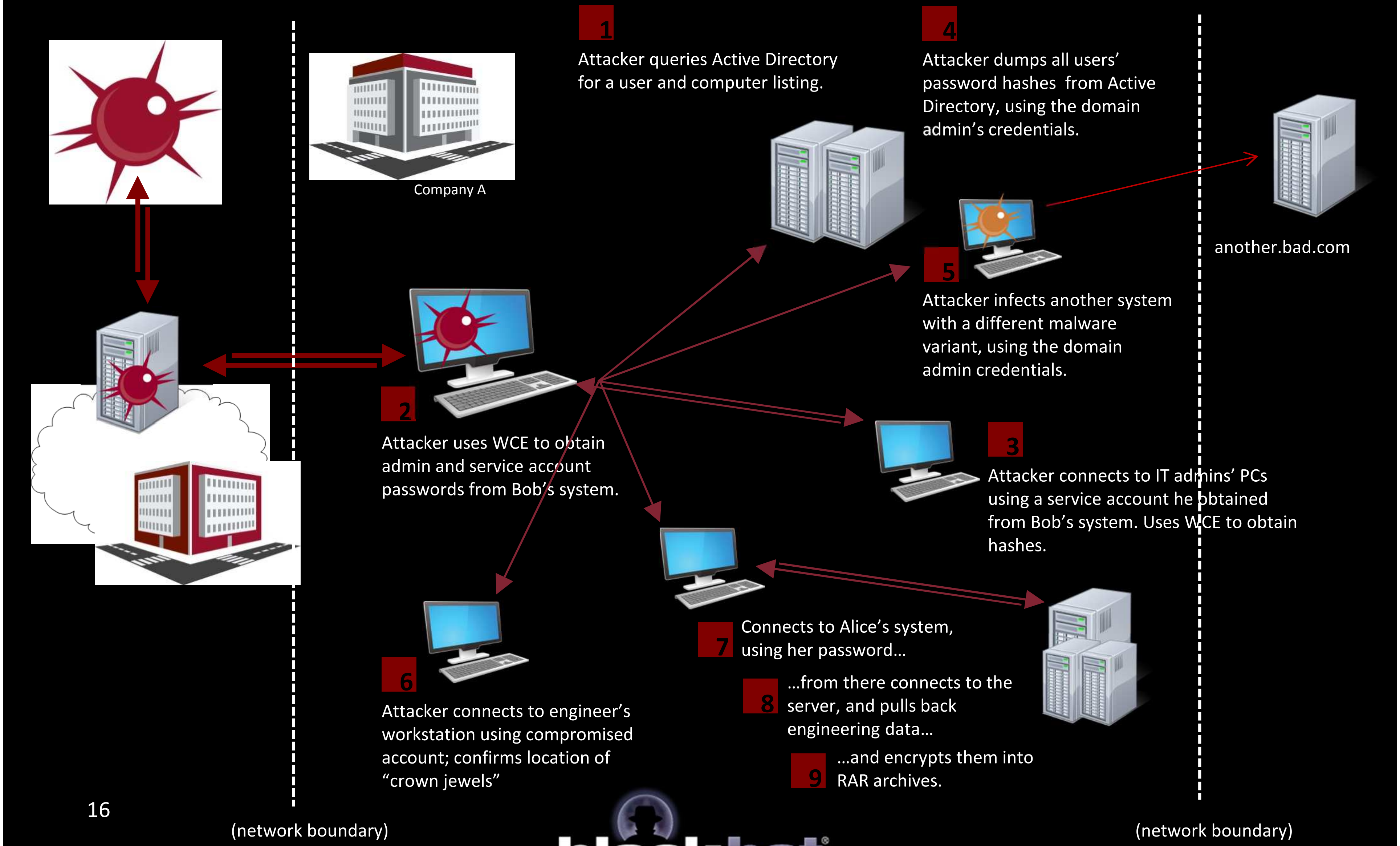
The attacker, via the command and control (C2) server, executes commands on the victim PC.

6

The attacker now owns Bob’s workstation.

(“Hop point” infrastructure was already deployed.)

APT Attack: Days Two – Four



1 Attacker queries Active Directory for a user and computer listing.

2 Attacker uses WCE 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. Uses WCE to obtain hashes.

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

Takeaways:

- The organization was targeted for a reason

- The attacker’s goals
  - Accomplish their mission
  - Remain undetected
  - Maintain access to the network

- Defense is not what it used to be
  - Cannot “prevent” – instead think “inhibit”
  - And, focus on detecting and responding quickly

- Win by:
  - Inhibiting
    - Make the attacker’s job difficult
    - …but realize he will succeed in establishing a foothold
  - Detecting
    - Capability to proactively identify anomalies
    - Ability to quickly answer “investigative” questions
  - Enhancing response capabilities
    - Investigate + remediate in hours, not months/years

RECOMMENDED APPROACH

Response = Investigate + Remediate

- Investigation
  - Scope of compromise
  - Attacker TTPs
  - Data loss
  - Attribution and attacker motivations

- Remediation
  - Mitigate current threat
  - Make it more difficult for future attackers
  - More rapidly detect future activity
  - Analyze lessons learned and strengthen security program

Attacker TTPs drive the approach

Attacker TTPs

- Established a foothold
- Lateral movement capability
- Methods of evading detection
- Specific malware and tools deployed
- Specific command-and-control (C2) networks

Key Remediation Tactics

- Isolate environment during remediation
- Execute contain/eradicate activities over a short time period
- Block C2 and implement rapid alerting mechanism
- Inhibit attacker and improve visibility to detect future attacker activities

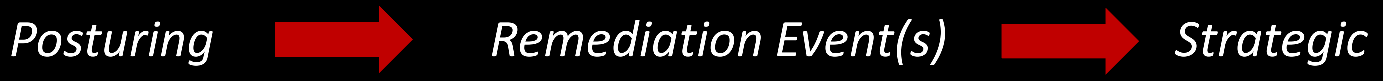
Remediation phases

Remediation encompasses containment, eradication and recovery.

A remediation event as a short, defined period of time during which an organization

Mitigates the current threat

Implements enhancements to directly frustrate attackers’ techniques



Posturing → *Remediation Event(s)* → *Strategic*

The Remediation Event

1. Isolate WAN from the Internet.
2. Block egress traffic to attacker C2 addresses & domains.
3. Replace compromised systems.
4. Reset passwords.
5. Implement technical countermeasures that directly address the attack lifecycle:
   a) Secure Windows ‘local administrator’ accounts
   b) Patch third-party desktop applications
   c) Implement application whitelisting (critical systems)
   d) Block workstation-to-workstation communication
6. Validate effective implementation of tasks
7. Reconnect Internet

*NB: One size does not fit all.

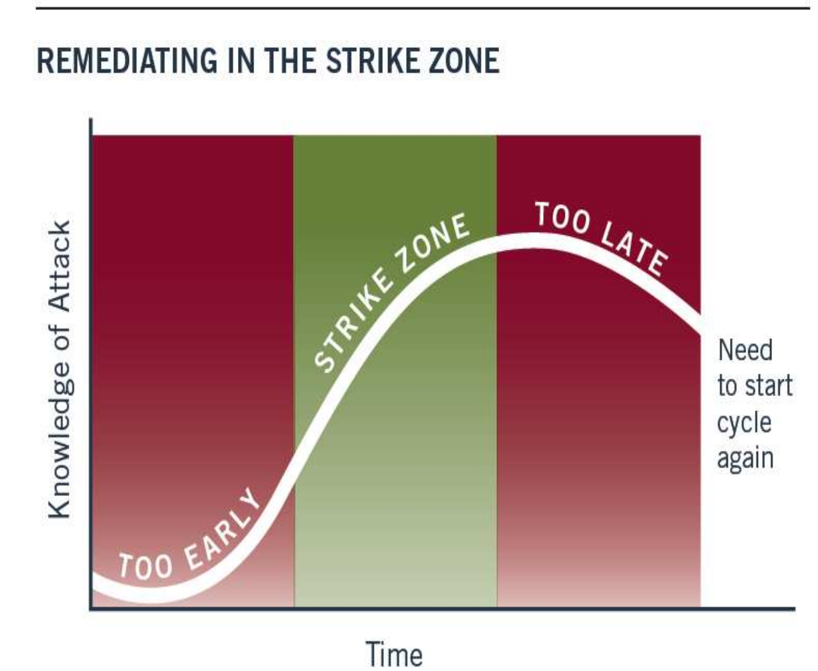
The Remediation Event

Execute event when:

Thorough understanding of the extent of the compromise

Know the attacker’s tactics

Can reliably detect the attackers’ malware and tools



Remediation phases

Remediation is preceded by **posturing**

- Implement triage countermeasures that do not disrupt the investigation
- Plan for the remediation event(s)
- Instrument the environment to make it more “investigation-ready”

Remediation is followed by the implementation of **strategic** initiatives

- Longer-term security improvements that are not tactically necessary for remediation

Posturing → *Remediation Event(s)* → *Strategic*

Caveats

Some situations warrant immediate containment, e.g. when

Attacker knowing that you are remediating

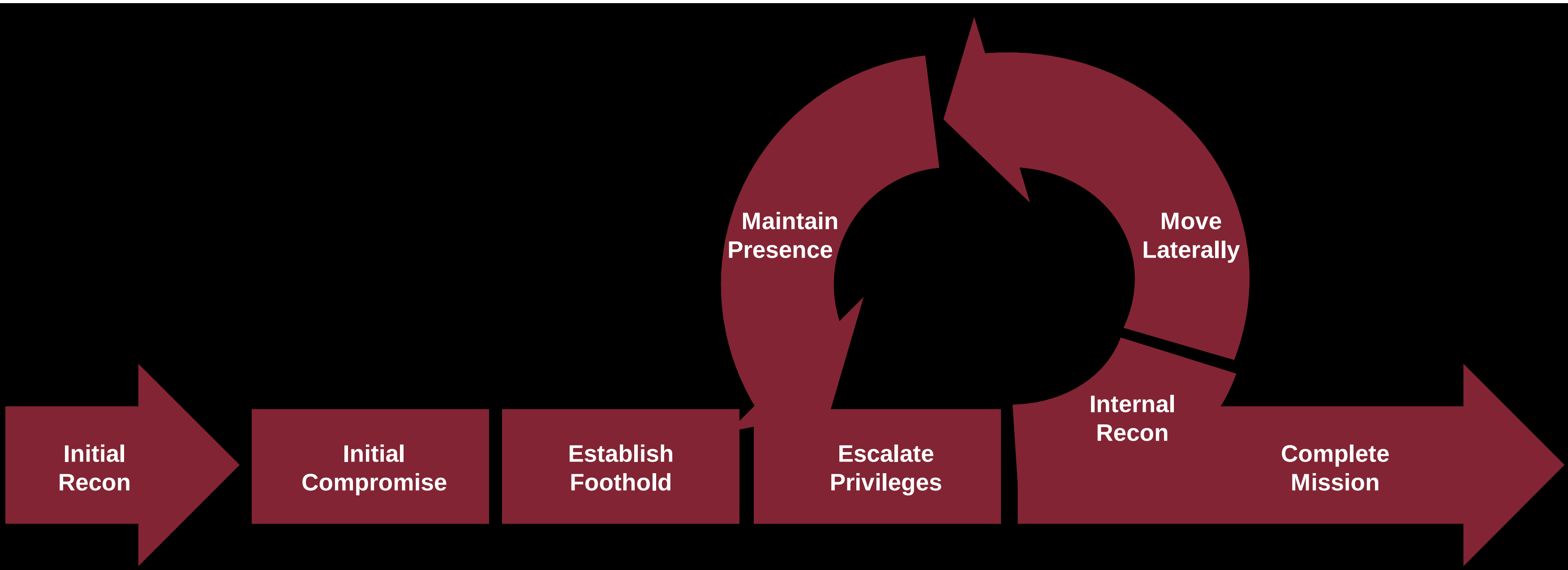
[has less impact than]

Consequences of not containing

Caveats in Action

- Example: financial breach, smash-and-grab
  - Attackers are about to steal millions in cash
  - Attackers are not interested in maintaining access
- Immediate containment is likely justified

Prioritizing initiatives



Initial Recon

Initial Compromise

Establish Foothold

Escalate Privileges

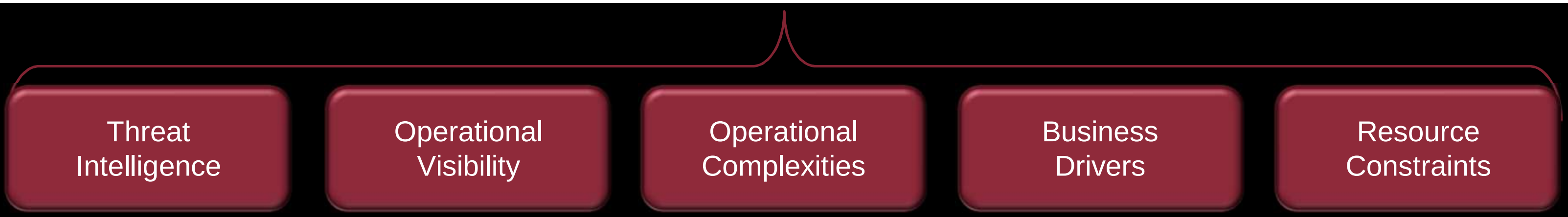
Internal Recon

Move Laterally

Maintain Presence

Complete Mission

	Initial Recon	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Recon	Move Laterally	Maintain Presence	Complete Mission
Inhibit								
Detect								
Respond								



Threat Intelligence

Operational Visibility

Operational Complexities

Business Drivers

Resource Constraints

blackhat®
USA 2012

Posturing

Plan the remediation workstream

Posturing

Enhance logging and monitoring

Posturing

Prepare enterprise-wide password change

Posturing

Focus on the most impactful defensive measures

Strategic

Investing in people

Strategic

Creating an 'investigation-ready' environment

Strategic

Enhancing authentication and authorization

Strategic

Improving the network architecture

Summary

- Targeted, persistent threats require a different approach for remediation success.
- Redefine winning: such attackers will return.
- Plan countermeasures that directly address the attack lifecycle to optimize chances of success.

Contact information

- Jim.Aldridge at Mandiant.com
- 703.224.2963

About MANDIANT:

MANDIANT is the information security industry's leading provider of incident response and computer forensics solutions and services. MANDIANT provides products, professional services and education to Fortune 500 companies, financial institutions, government agencies, domestic and foreign police departments and leading U.S. law firms. To learn more about MANDIANT visit www.mandiant.com, read M-unition, the company blog: http://blog.mandiant.com, or follow on Twitter @MANDIANT.