Targeted Intrusion Remediation:

Lessons From The Front Lines

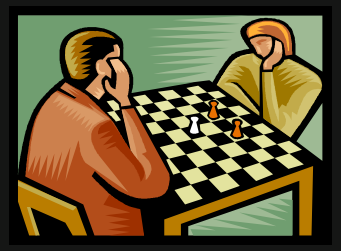
Jim Aldridge

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)
- Spies (e.g. foreign intel service, corp. spies)
- "Hacktivists"
- Disgruntled insiders

Non-Targeted

- Botnet herders
- Opportunists
- Spammers

- **Targeted**
  - The adversary chose your organization for a reason
  - Professionals that seek particular information
  - Will perform reconnaissance to understand
    - Your business
    - Your personnel
    - Operating locations

- **Persistent (adopted from Richard Bejtlich's definition of APT)**
  - The adversary is formally tasked to accomplish a mission
    - Often includes "maintain long-term access"
  - 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

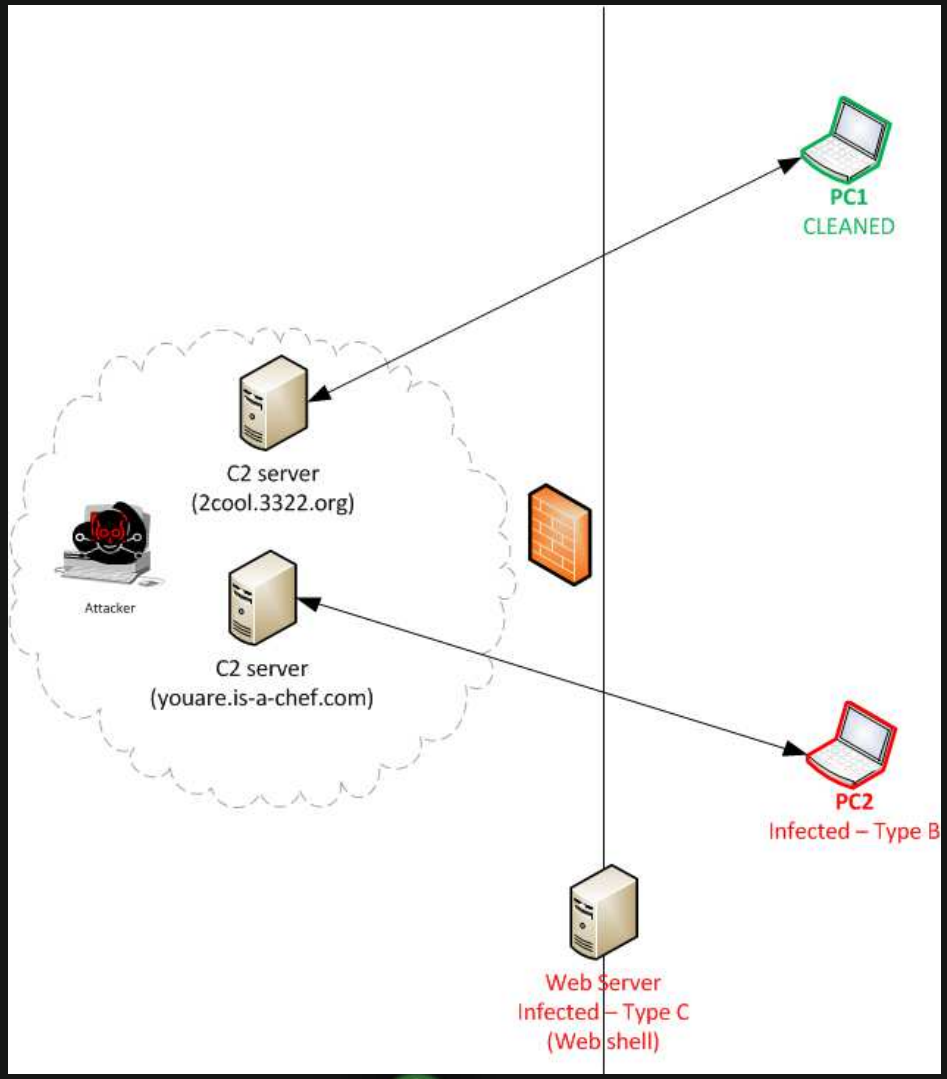
3.3.1 Choosing a Containment Strategy

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

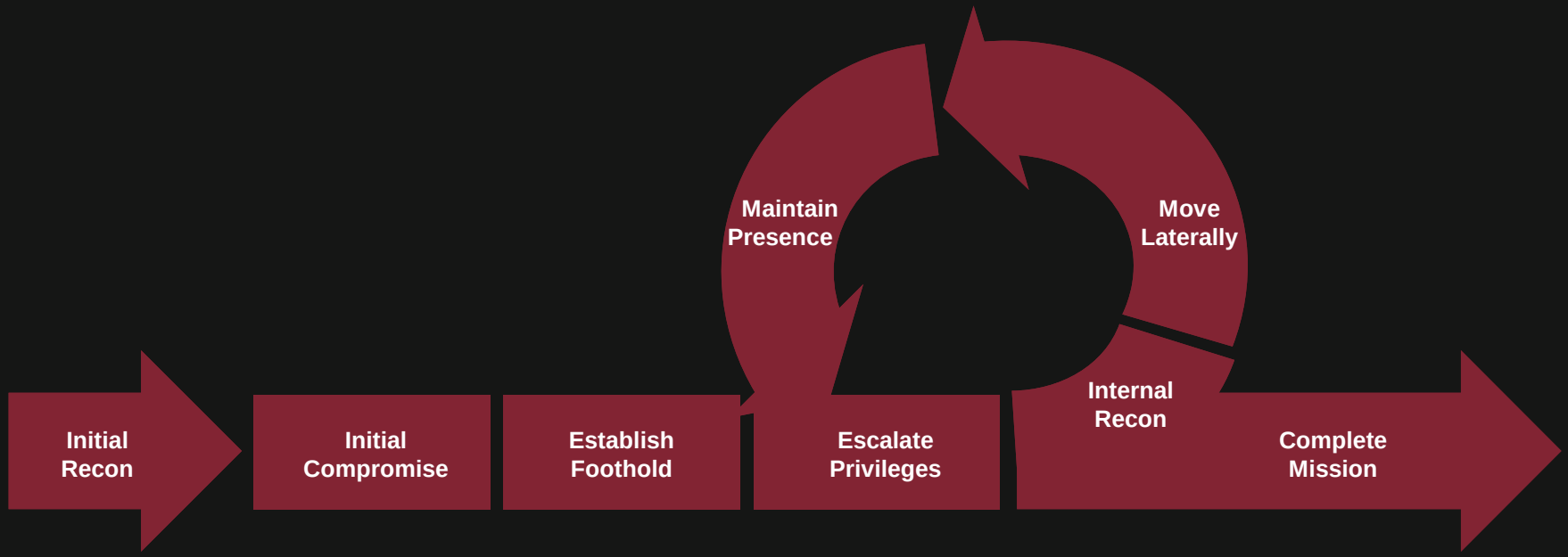
…updated for the modern era

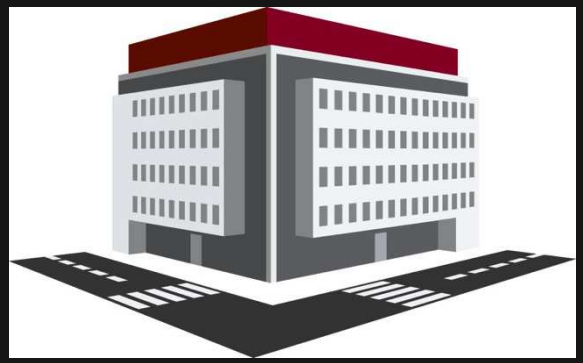


Agenda

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

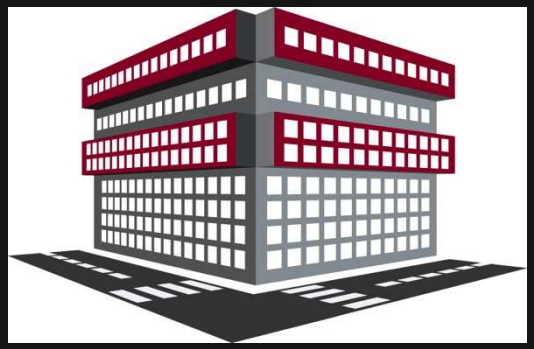
Targeted Attack Lifecycle


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



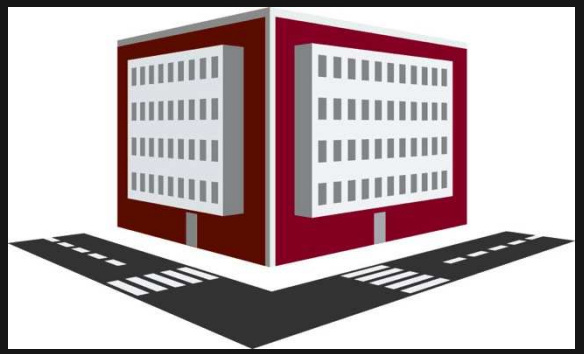
Company A

- High tech manufacturer
- Global presence
- 20,000 employees
- 24,000 workstations and laptops, 3,000 servers



Company B

- Supplier to company A



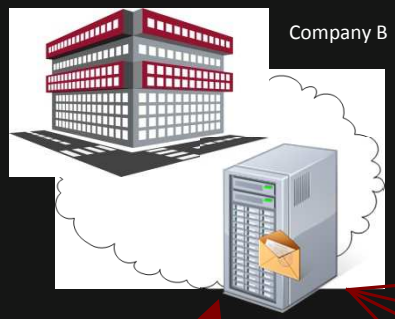
Company C

- A service provider

Targeted, Persistent Attacker

- A professional associated with a state-run
- intelligence service

APT Attack: Day One



Company B

Company A

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.

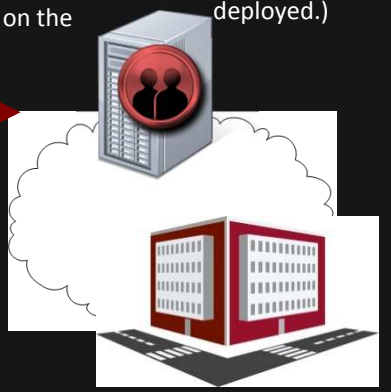
5

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

6

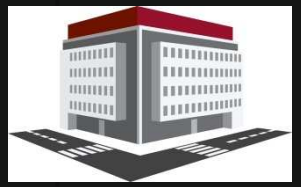
The attacker now owns Bob’s workstation.

(“Hop point” infrastructure was already deployed.)



Company C

APT Attack: Days Two – Four



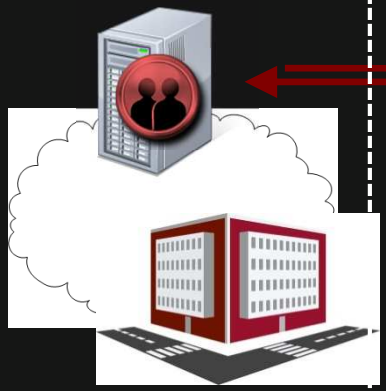
Company A

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

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

another.bad.com

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



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

3 Attacker connects to IT admins' PCs using the local admin password he obtained from Bob's system. Uses WCE to obtain hashes.

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…

Crown Jewels

9 …and encrypts them into RAR archives.

(network boundary - Internet)

(network ACL, access only from certain workstations)

(network boundary - Internet)

- The organization was targeted for a reason
- 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

Attacker tactics drive the approach

Attacker tactics

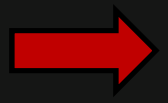
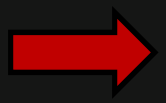
- Established a foothold
- Lateral movement capability
- Methods of evading detection
- Specific malware and tools deployed
- Specific command-and-control (C2) networks
- Will keep trying to re-compromise your environment

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
- Conduct investigation to fully scope compromise

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*

Typical Remediation Event

1. Isolate WAN from the Internet to prevent egress traffic (temporary)
2. Block egress traffic to attacker C2 addresses & domains (permanent)
3. Replace compromised systems
4. Reset passwords
5. Implement technical countermeasures that directly address the attack lifecycle
6. Validate effective implementation of tasks
7. Reconnect Internet.

Remediation phases

- Remediation is preceded by **posturing**
  - Implement triage countermeasures that do not disrupt the attacker
  - 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

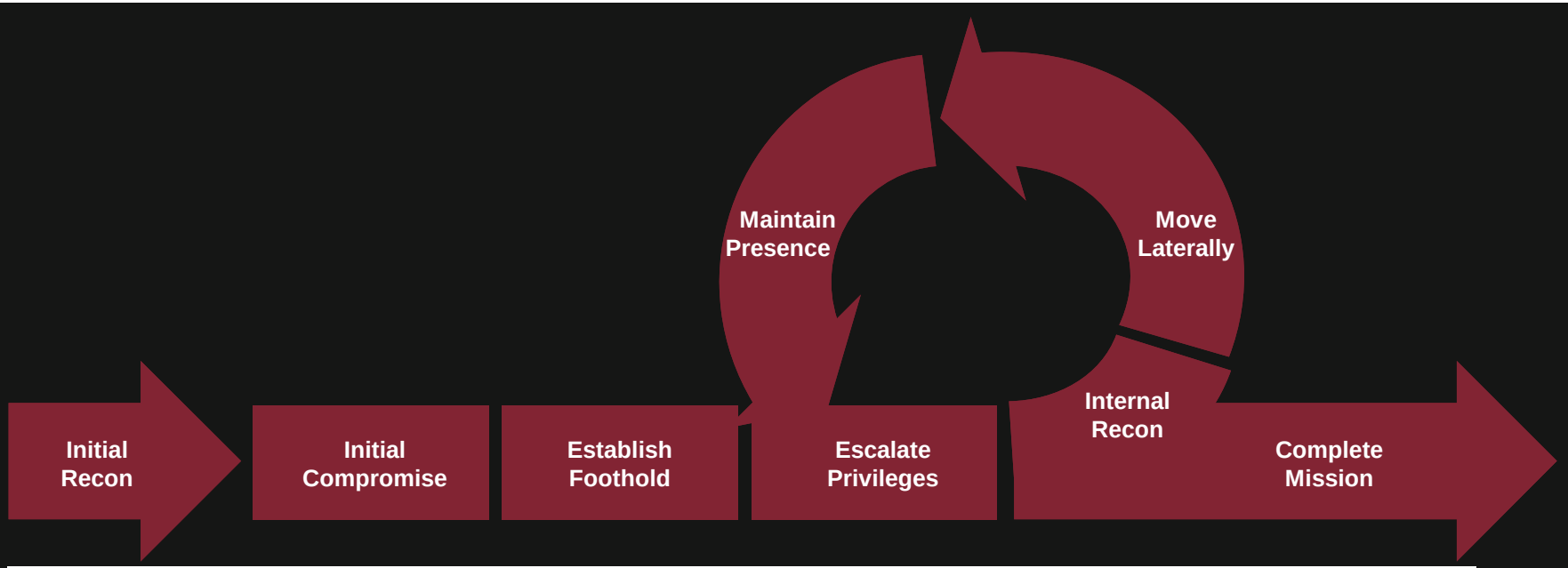
Posturing → *Remediation Event(s)* → *Strategic*

Caveats

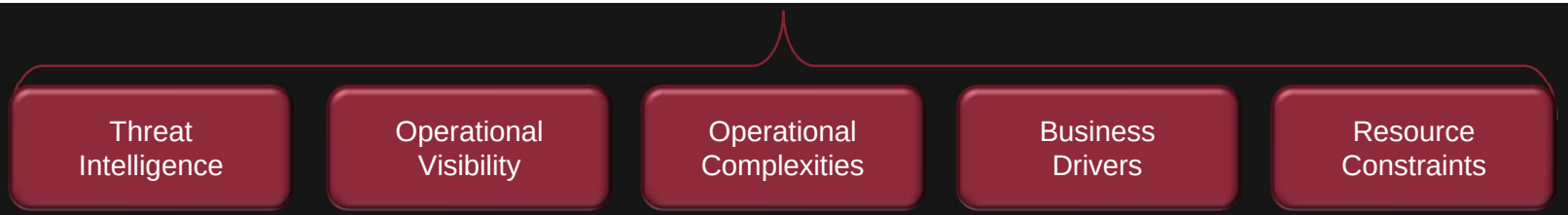
Examples of Caveats

- Example: financial breach, smash-and-grab
  - Attackers are about to steal millions in cash
  - Attackers are not interested in maintaining access
  - Contain immediately to limit damage
- Example: business depends 100% on a piece of information
  - “if they steal X, and start producing that widget, we will go out of business in a year”
  - Contain (limit access to X) immediately
  - Try to limit other actions (i.e. partially contain)

Prioritizing initiatives



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



Posturing

Strategic

Summary

- Targeted, persistent threats require a different approach for remediation success.
- Redefine winning: such attackers will return – make their job more difficult, find them more quickly.
- Plan countermeasures that directly address the attack lifecycle to optimize chances of success.

Contact information

- Jim.Aldridge at Mandiant.com
- +1 703 224 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.