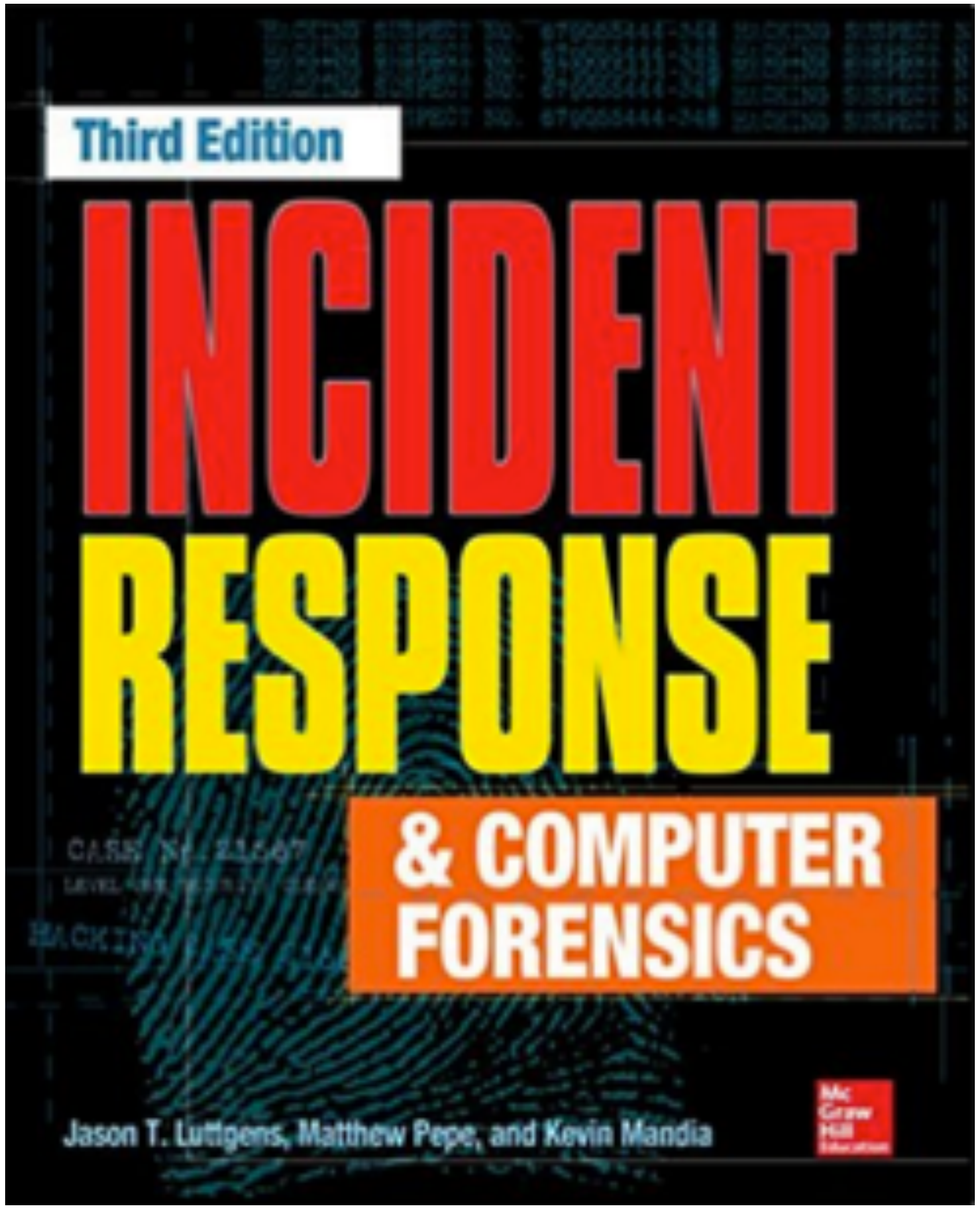
CNIT 152: Incident Response



1 Real-World Incidents

Updated 8-19-2021

Events and Incidents

- **Event**
  - ***Any observable occurrence in a system or network***
- **Incident**
  - ***Violation or threat of violation of security policies, acceptable use policies, or standard security practices***

Incident Response

- **Confirm whether an incident occurred**
- **Rapid detection and containment**
- **Determine scope**
- **Prevent a disjointed, noncohesive response**
- **Determine and promote facts and actual information**
- **Minimize disruption to business and network operations**

Incident Response

- **Minimize damage to the compromised organization**
- **Restore normal operations**
- **Manage public perception**
- **Allow for legal action against perpetrators**
- **Educate senior management**
- **Enhance security posture against future incidents**

IR Teams

- **Investigation team**
  - **Determines what has happened and performs a damage assessment**
- **Remediation team**
  - **Removes the attacker and enhances security posture**
- **Public relations**

Live Response

- Classical forensics was done post-mortem
  - On a hard disk image
- Now mody analysis id performed on systems that are powered on (live)
  - Including memory analysis to see running processes, network connections, etc.

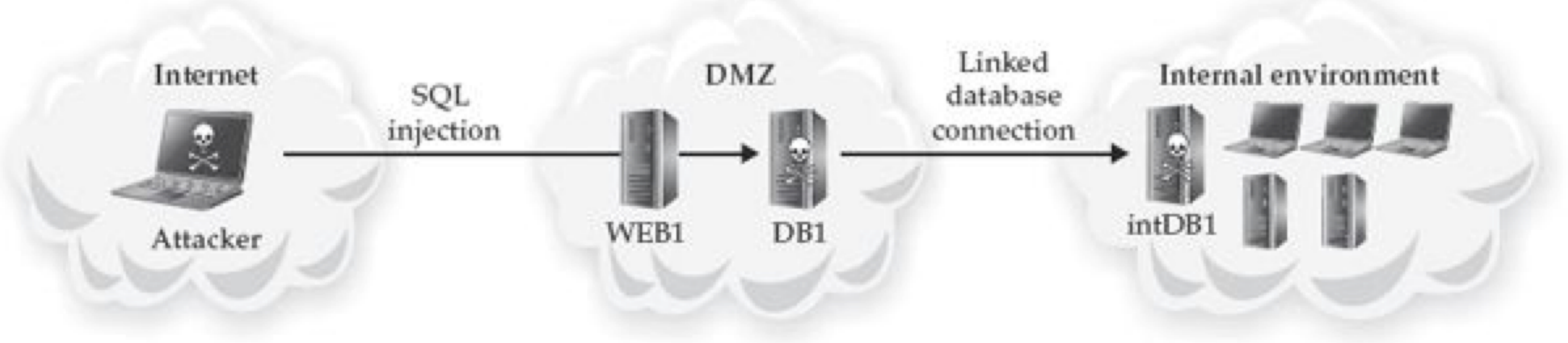
Case 1
Show Me the Money

Initial Compromise

- **Early January: SQL injection vulnerability exploited on server WEB1**
  - **In a DMZ belonging to a small business unit purchased by the parent organization four years prior**
- **Command execution on database server DB1, with privileges of the SQL Server service (local administrator)**
  - **Using xp_cmdshell**
  - **Download malware and execute it on DB1**

Escape DMZ

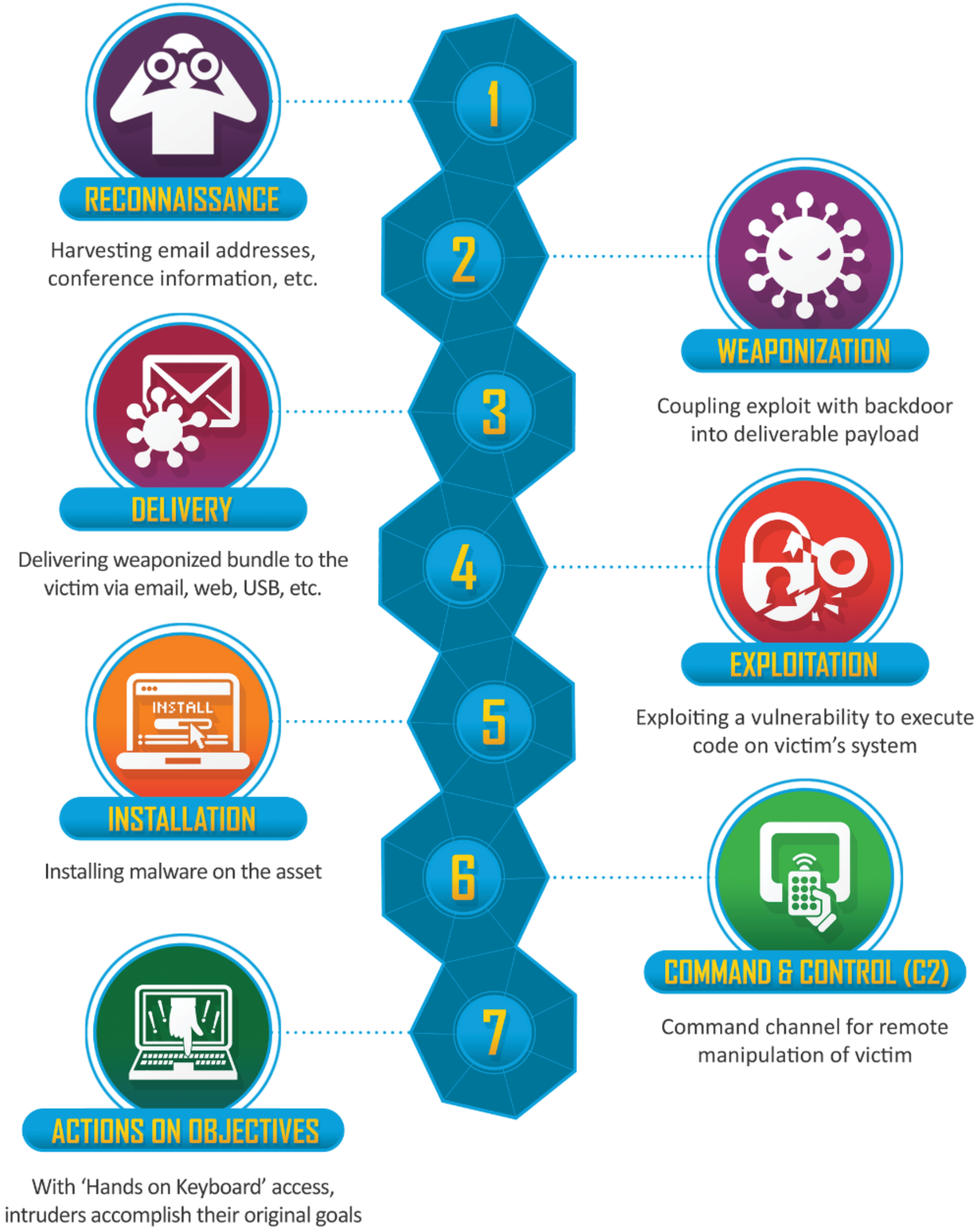
- **Misconfiguration in DMZ firewall allowed malware to execute SQL commands on a database server intDB1**
  - **Located within the corporate environment**



Recon

- **Attacker spent weeks performing reconnaissance of corporate environment**
- **For first week, attacker used SQL injection**
- **Then the attacker implanted a backdoor**
- **Extracted and cracked password hash for local administrator account on intDB1**
- **Now the attacker has local admin on most systems**

Lockheed -Martin Kill Chain



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

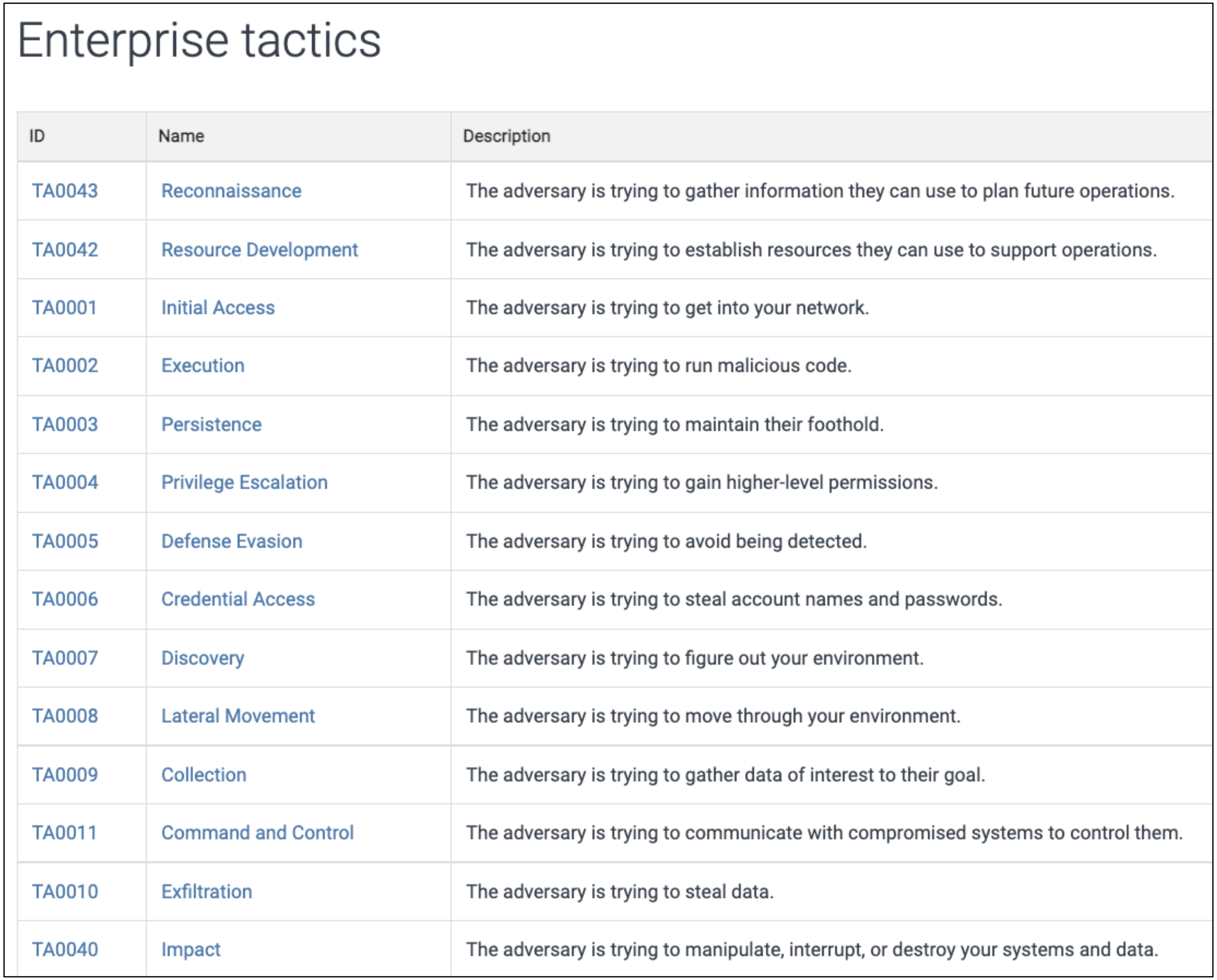
COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Mitre ATT&CK v9



Enterprise tactics

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Exploit Domain Controller

- **Installed keylogger malware**
- **Obtained password hashes from multiple systems for administrator accounts**
  - **Including hashes from the Domain Controller**

Mid-February

- More than 20 backdoors, spanning three distinct malware families
- We'll call the primary backdoor family BKDOOR
  - Custom malware creation kit
  - Allowed attacker to modify binaries to avoid antivirus detection

BKDOOR

- **Full control of victim system**
- **File upload and download**
- **Tunnel Remote Desktop Protocol traffic into the environment**
- **Proxy network traffic between backdoors**
- **Encrypts command-and-control (C2) traffic with RC4 "C2 data"**
- **Persistence through "DLL search-order hijacking"**

PROXY Malware Family

- **Redirected connections to destination address specified in its configuration file**
  - **Can also accept original destination address from the BKDOOR malware**

BKDNS Malware Family

- **Tunneled C2 traffic through DNS queries and responses**
- **A backup system, not used during this investigation**
- **Used on both Windows and Linux systems**

Late March

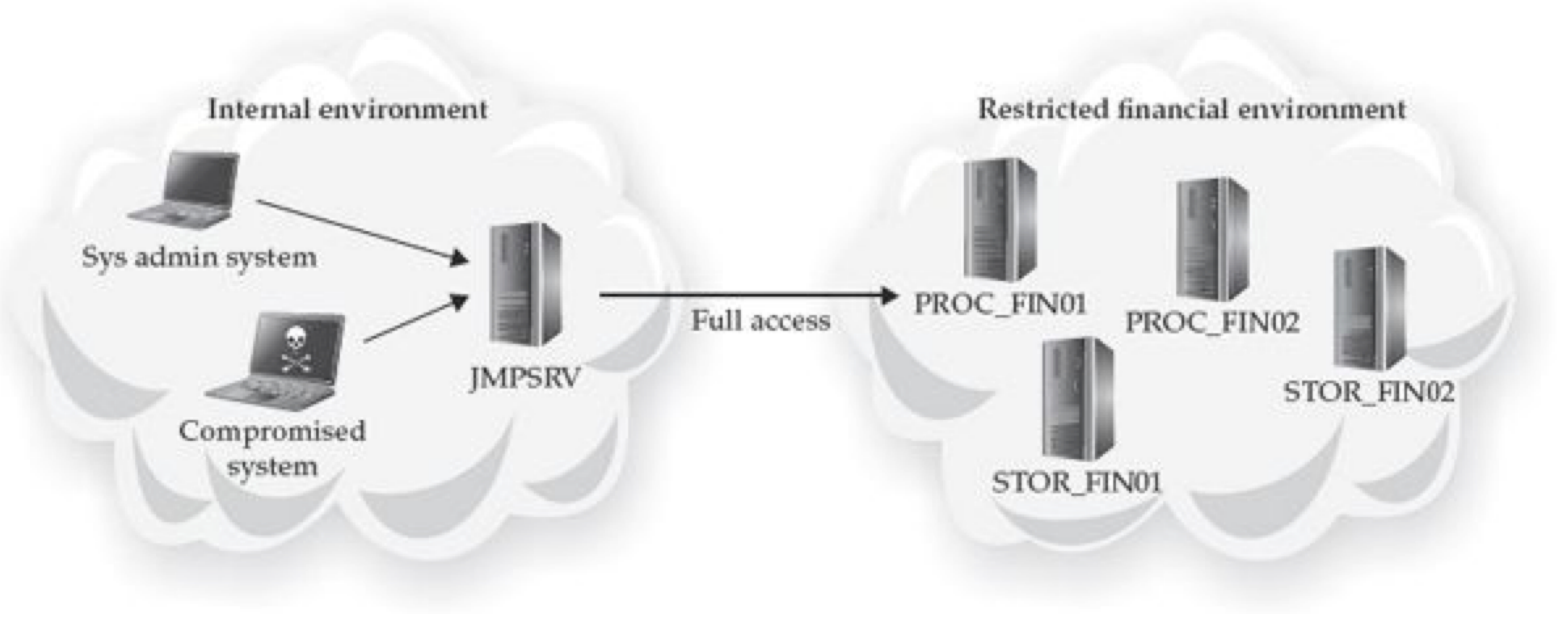
- **Attacker stole data multiple times**
- **Took usernames and passwords**
- **Network architecture and IT information**
- **Information about financial systems and how financial data was handled**

Stealing Financial Data

- **Outbound FTP connection to an attacker-controlled FTP server**
- **Also used a backdoor to send financial data to C2 server**
- **Compressed the data as ZIP, RAR or CAB files**

Jump Server

- **Gateway into restricted financial environment**



PCI Data

- Payment Card Industry data
- Magnetic stripe has two tracks
  - Track 1 & Track 2 (similar data)
- CVV/CVV2 number used to verify physical possession of the card
- Not all merchants collect the CVV/CVV2 number

Compromise JMPSRV

- Gained access with stolen domain administrator password (two-factor authentication not used)
- Transferred reconnaissance tools to JMPSRV
- Begin reconnaissance of restricted financial environment
- Took password hashes from RAM on JMPSRV

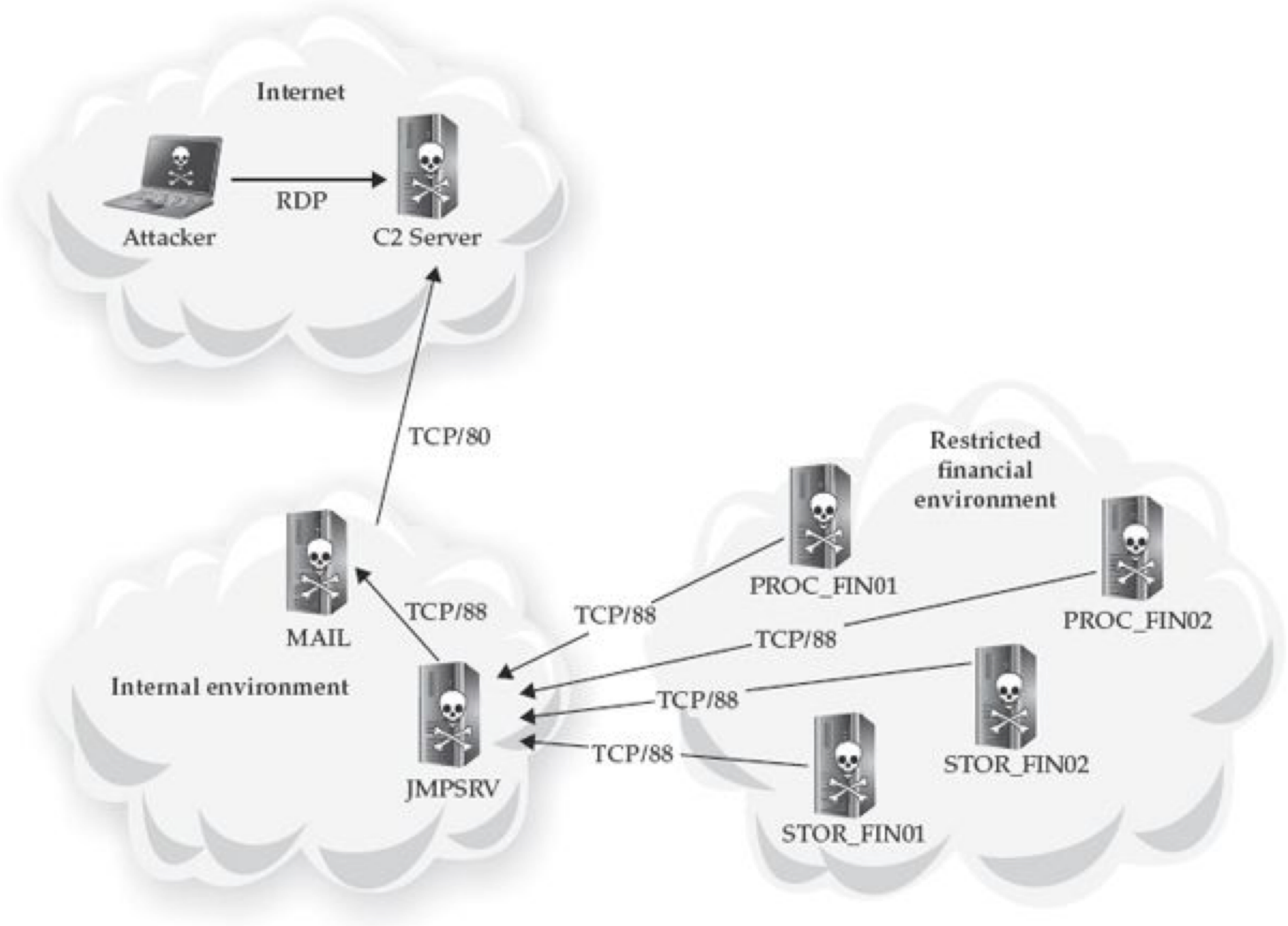
Recon

- **Next two months finding**
  - **Systems that processed or stored cardholder information**
  - **Systems with direct Internet connections**
- **Stole documents that described the infrastructure**

Naming Convention

- **90 systems processed or stored financial information**
- **PROC_FIN01, PROC_FIN02, STOR_FIN01, STOR_FIN02, etc.**
- **None connected directly to the Internet**
- **Attacker sent data through JMPSRV and MAIL to get out**

Proxy Connections



Testing Methods

- Put Sysinternals "PsSuite" on PROC_FIN01
  - Used pslist to see running processes
  - Dumped RAM from multiple processes
  - Created a RAR archive and transferred it out
- Trying to find processes that contained cardholder data

Cardharvest

- **Two days later, attacker installed a custom binary named "cardharvest.exe" onto PROC_FIN01**
  - **Searched process RAM for Track 2 data every 15 seconds**
  - **Hashed the data to prevent duplicate collection**
  - **Encrypted it using RC4 and a hard-coded static key**
  - **Saved it to a local file**

Three Months

- **Over the next three months**
- **Attacker stole millions of cardholder data records**
- **From all 90 financial systems**

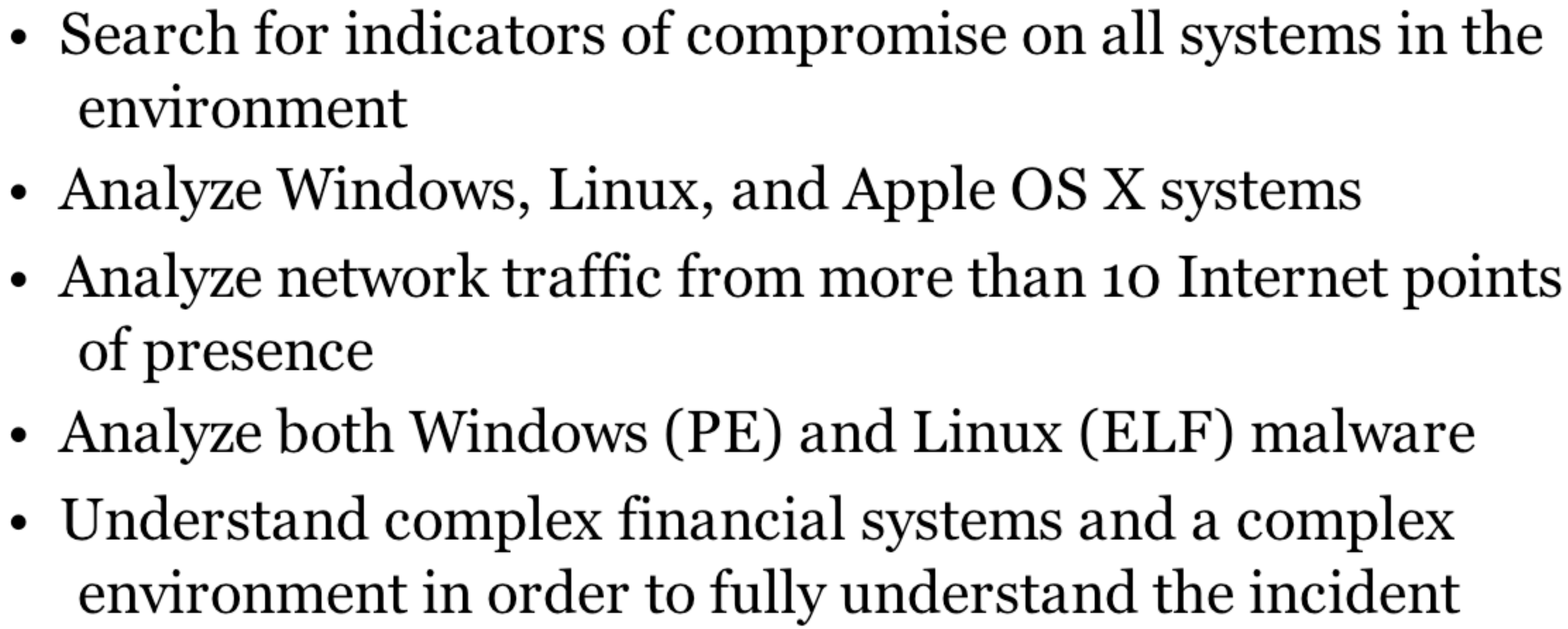
Detection

- **After ten months of exploitation**
- **A system administrator noticed that MAIL was communicating with a server in a foreign country over port 80**
- **Triage showed that there was a compromise**
- **Initiated incident response**

Incident Response

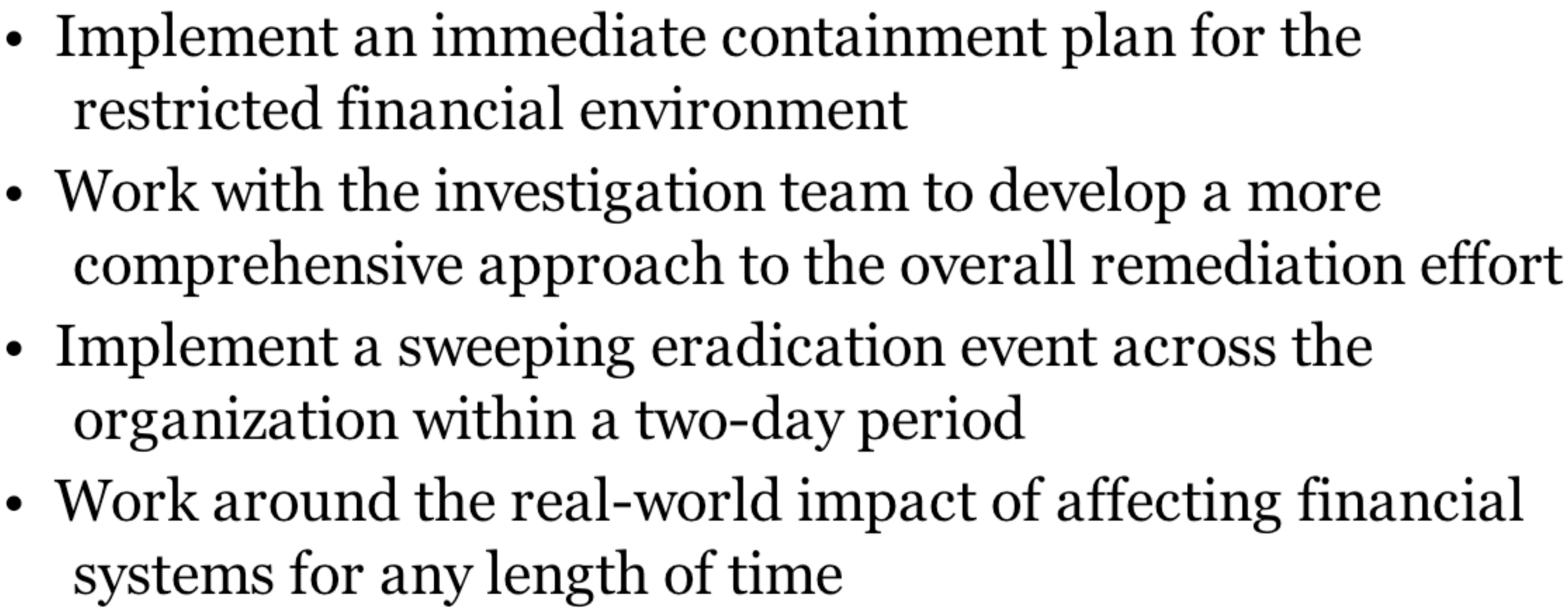
- **Team travelled to client location**
- **Immediate containment plan**
- **Comprehensive incident investigation**
- **Eradication event to remove all traces of the attacker**
- **Less than two months for complete IR**

Investigation Team



- Search for indicators of compromise on all systems in the environment
- Analyze Windows, Linux, and Apple OS X systems
- Analyze network traffic from more than 10 Internet points of presence
- Analyze both Windows (PE) and Linux (ELF) malware
- Understand complex financial systems and a complex environment in order to fully understand the incident

Remediation Team



- Implement an immediate containment plan for the restricted financial environment
- Work with the investigation team to develop a more comprehensive approach to the overall remediation effort
- Implement a sweeping eradication event across the organization within a two-day period
- Work around the real-world impact of affecting financial systems for any length of time

Case 2
Certificate of Authenticity

Initial Compromise

- **In mid-May, attacker sent 100 spear-phishing emails**
  - **Targets chosen because of business relationship to speakers at an industry conference**
  - **Most had local administrator privileges**
  - **None had domain administrator privileges**

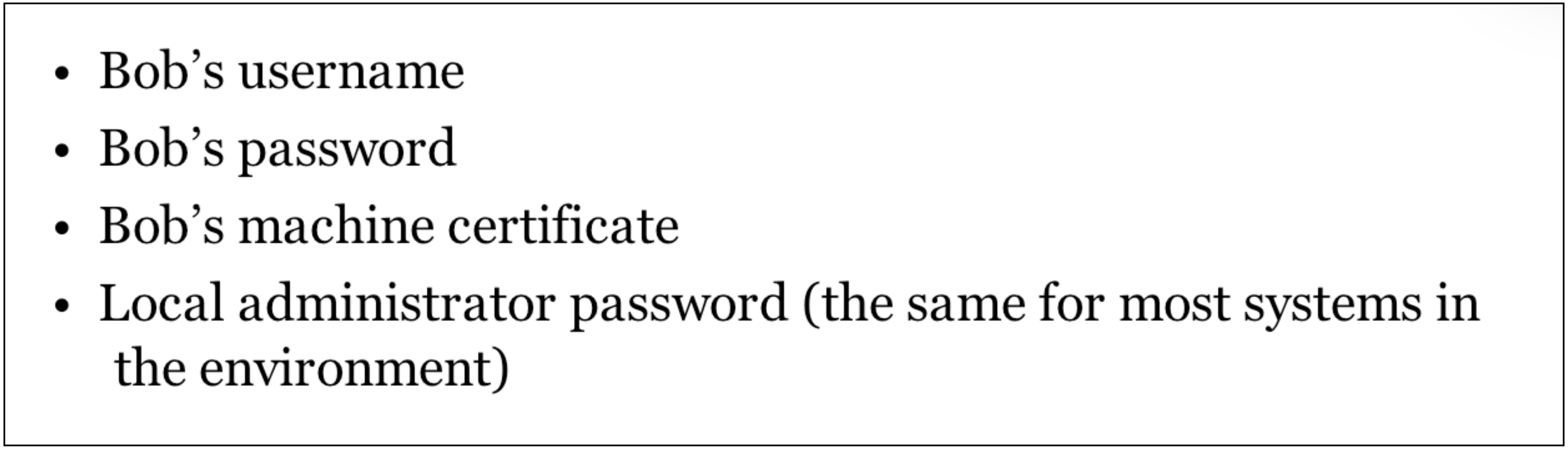
Malicious PDF

- **One recipient, Bob, opened the attachment with a vulnerable version of Adobe Acrobat**
- **Exploit installed GHoST RAT (Remote Access Trojan)**
- **Attacker gained control of BOBSYS01 from the C2 server**

VPN Compromise

- **Two days later, attacker performed reconnaissance on BOBSYS01**
- **Bob was an engineer**
- **Had VPN software that used a machine certificate, username, and password**
- **Obtained and cracked local administrator password hash**
- **Used mimikatz.exe to extract Bob's password and VPN machine certificate**

The Attacker Obtained



- Bob’s username
- Bob’s password
- Bob’s machine certificate
- Local administrator password (the same for most systems in the environment)

- **No longer needs Bob's system**
- **Attacker can now VPN in from any system**

HOME3

- **Less than one week later**
- **Attacker connected via VPN from a system named HOME3**
- **Used RDP but ended the session by closing the window instead of logging out**
- **Caused an event to be logged in the Security event log**
  - **Capturing attacker's host name and IP address (from Texas)**

Recon

- **Attacker spent the next 2 weeks performing reconnaissance**
- **Mapped network shares and directory listings**
- **Installed keyloggers**
- **Accessed email through Outlook Web Access (OWA) with stolen credentials**

SENS1

- **Two weeks later, attacker started accessing business-critical data from a share on file server SENS1**
- **Sensitive engineering data for a new product**
- **Access Control Lists (ACLs) restricted this data to engineers working on the project**
  - **But the attacker had local administrator access and modified the ACLs to gain access**

Next Four Weeks

- Attacker sporadically stole data
- Created encrypted RAR files
- Renamed them to CAB files
- Uploaded to an attacker-controlled FTP server
- Then deleted RAR file and ran Windows defragmentation utility
  - In an attempt to cover tracks

SIEM

- **Two weeks after the attacker began stealing data**
- **Company started evaluating a new Security Information and Event Management (SIEM) utility**
- **Included VPN logs in the data sets**
- **SIEM showed Bob logging in from multiple systems and IP addresses simultaneously on multiple days**

Chasing Attacker

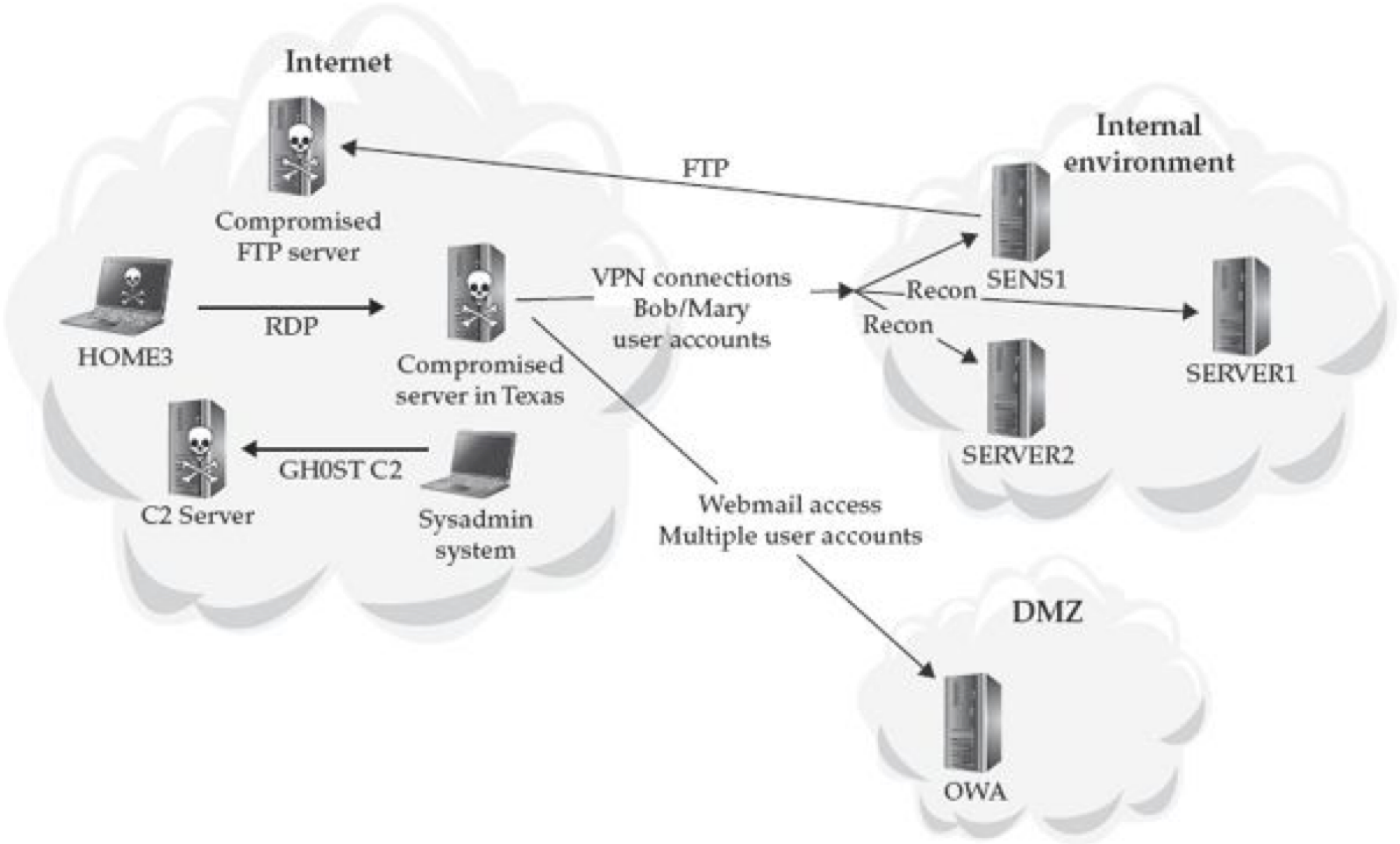
- **Security staff disabled Bob's account**
- **Attacker started using another account, Mary's**
- **SIEM quickly discovered malicious use of Mary's account**
- **Initiated incident response and called IR specialists in**

Real IR

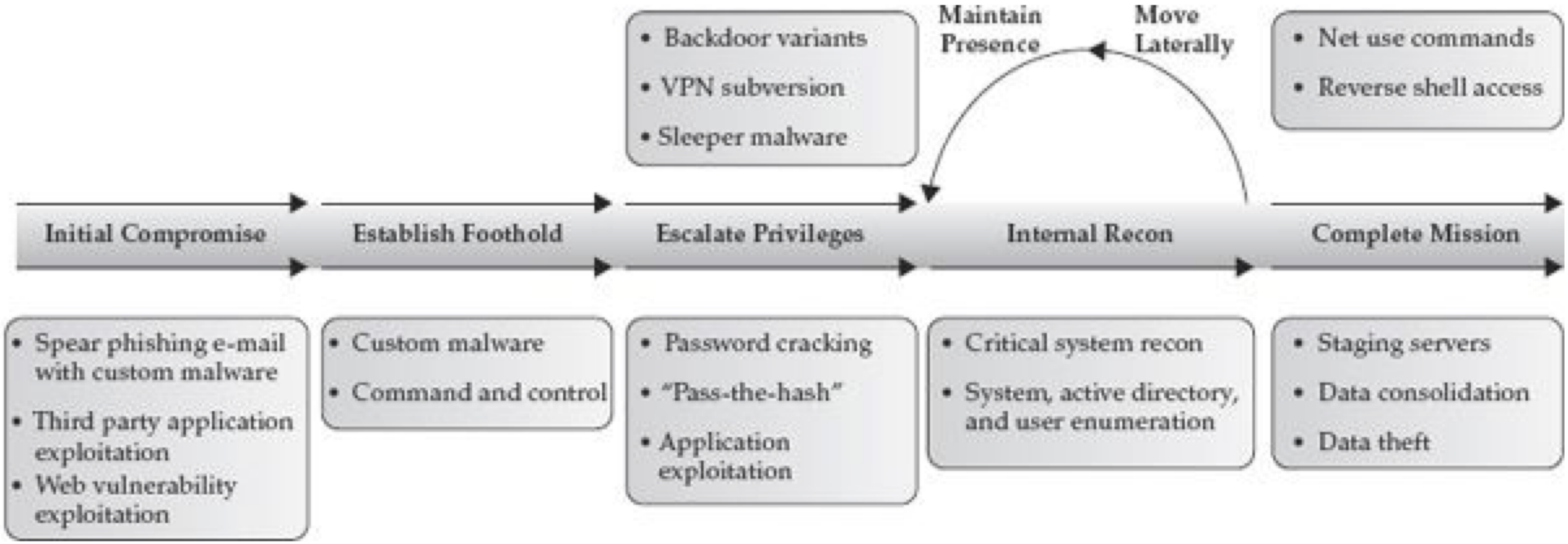
- **Identify IP addresses attacker used to VPN from**
- **GHoST RAT was sending beacons to one of those same IPs**
- **This led to discovery of compromise on BOBSYS01**
- **Comprehensive eradication event performed two weeks after IR initiated**

OWA Access

- **Two days after the eradication event**
- **SIEM detected one of attacker's IP addresses attempting access to OWA, with multiple user accounts**
- **Even though company had changed all passwords during the eradication event, not all users had actually changed their passwords**
- **A second enterprise-level password change disabled all accounts that failed to change passwords within 24 hours**


Internet
Compromised FTP server
FTP
Internal environment
HOME3
RDP
Compromised server in Texas
VPN connections Bob/Mary user accounts
SENS1
Recon
Recon
SERVER1
SERVER2
C2 Server
GH0ST C2
Sysadmin system
Webmail access Multiple user accounts
DMZ
OWA

Attack Lifecycle



Initial Compromise

- Spear phishing e-mail with custom malware
- Third party application exploitation
- Web vulnerability exploitation

Establish Foothold

- Custom malware
- Command and control

Escalate Privileges

- Password cracking
- "Pass-the-hash"
- Application exploitation

Internal Recon

- Critical system recon
- System, active directory, and user enumeration

Maintain Presence

- Backdoor variants
- VPN subversion
- Sleeper malware

Move Laterally

Complete Mission

- Net use commands
- Reverse shell access
- Staging servers
- Data consolidation
- Data theft

Kahoot!