Incident Response

April 18, 2024

Austin Peay State University
Cybersecurity Club

Agenda

- Introductions
- Definitions
- Incident Response Process Overview
- OPM Breach High-Level Walkthrough
- Other Major Breaches
- Questions and Answers

Andrew Scharlott

Education

Purdue University - M.Sc. Computer Science

University of Missouri
B.Sc. Computer Engineering
B.Sc. Computer Science

Current Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Microsoft Azure Fundamentals (AZ-900)
- ForeScout Certified Administrator (FSCA)
- AWS Cloud Practitioner Essentials
- Proofpoint Certified Insider Threat Specialist

Professional Experience

Ampsight - Principal Cybersecurity Architect *

Sylvan Road Capital - Vice President of Information Security

University of Denver - Cybersecurity Bootcamp Instructor

U.S. Dept of the Interior:
Cybersecurity Operations Section Chief
Information System Security Officer (ISSO)
Project Manager
Security Program Manager
Security Operations Team Lead
Security Engineer
Security Analyst

Dish Network:
Security Analyst
Security Administrator

linkedin.com/in/ascharlott

Definitions

"An **event** is any occurrence that can be observed, verified, and documented, whereas an **incident** is one or more related events that negatively affect the company and/or impact its security posture." *Dave Shackleford (SANS)*

Event - Any occurrence that takes place during a certain period of time

Incident - An event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization’s data

Incident Response (IR) is the process by which an organization handles a data breach or cyberattack. It is an effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

Incident Response Frameworks - NIST vs SANS

SANS Incident Response Steps

NIST IR Steps

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

1. Preparation

Functions needed to have in place (ahead of time) in order to detect and respond to a potential incident, including items like:

- Incident Response Plan
- Personnel Plan
- Communication Plan and Contact Information (including external partners)
- Asset Information
- Monitoring and Alerting
- Data Sensitivity
- Log Storage/Analysis Tools

2. Detection and Analysis

Detection involves collecting data from IT systems, security tools, publicly available information and people inside and outside the organization, and identifying precursors (signs that an incident may happen in the future) and indicators (data showing that an attack has happened or is happening now).

Analysis involves investigating data collected as part of detection activities in order to determine criticality of events and importance of response

3. Containment, Eradication, and Recovery

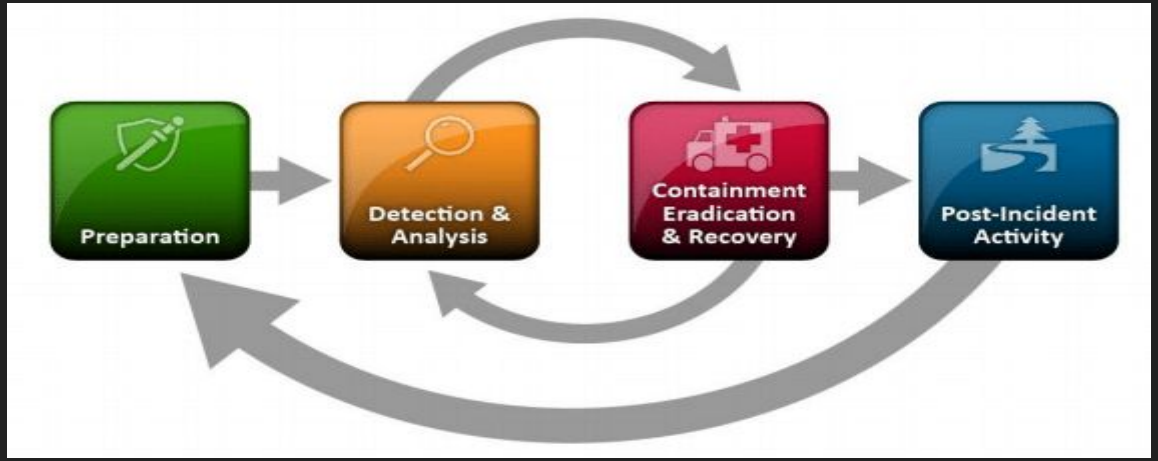
Containment: stopping the attack before it overwhelms resources or causes (additional) damage

Eradication: removing all elements of the incident from the environment

Recovery: restoring systems to normal operations, taking steps to ensure the same assets are not attacked again.

4. Post-Incident Activity

Compiling all relevant information about the incident in order to improve the process, adjust your incident response policy, plan, and procedures, and feed the new data into the preparation stage of your incident response process.



End Result: **Incident Report** (Who, What, Where, When, Why, How, Lessons Learned, Areas for Improvement, etc.) which aids/improves **Preparation** for future incident response

4. Post-Incident Activity - Questions to Ask

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do differently next time if the same incident occurred?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

IR - Good Things To Have

- Leadership
- (Single) Person In Charge
- Flexibility
- Patience
- Cool Head Under Pressure

OPM Breach - Overview

- What is OPM and what is DOI’s relationship with OPM?

In April of 2015, IT staffers within the United States Office of Personnel Management (OPM), the agency that manages the government’s civilian workforce, discovered that some of its personnel files had been hacked. Among the sensitive data that was exfiltrated were millions of SF-86 forms, which contain extremely personal information gathered in background checks for people seeking government security clearances, along with records of millions of people’s fingerprints. The OPM breach led to a Congressional investigation and the resignation of top OPM executives, and its full implications—for national security, and for the privacy of those whose records were stolen—are still not entirely clear.

www.csoonline.com

Initial Alert (Snort)

```
Alert rule_id: 1:49914 [EVENT] MALWARE-CNC
Level: Warning [Classification]
Msg: Suspected Malware CNC Communication
Date/Time: 3/15/2015-22:15:24
Source: 10.100.1.193
Destination: 101.96.128.154
Port: tcp 80
Protocol: tcp
```

Detection & Analysis

1. Investigate details of alert
   - Source server
   - Destination
   - Any captured traffic

2. Contact necessary parties
   - Internal management
   - FBI
   - DHS

Preparation Required

- Alerting system (Snort) in place monitoring correct traffic
- People with ability to investigate alerts
- Inventory Data
- Packet/data capture capability
- Server log data offloaded to SIEM or other system
- Contact information for needed help

```
Alert rule_id: 1:49914 [EVENT] MALWARE-CNC
Level: Warning [Classification]
Msg: Suspected Malware CNC Communication
Date/Time: 3/15/2015-22:15:24
Source: 10.100.1.193
Destination: 101.96.128.154
Port: tcp 80
Protocol: tcp
```

Detection & Analysis (Continued)

3. Log analysis from server

4. Analyze impacted system memory

5. Deploy additional monitoring tools across organization and analyze information

Determination: compromised customer administrator account being used to access sensitive data and exfiltrate information and install additional malicious software (including keyloggers) on impacted servers

Containment, Eradication, and Recovery

1. Block outbound activity from compromised servers
2. Reset all compromised admin accounts
3. Take systems offline and restore to known good state before bringing back online

Containment, Eradication, and Recovery

1. Block outbound activity from compromised servers
2. Reset all compromised admin accounts
3. Take systems offline and restore to known good state

WE DIDN’T DO ANY OF THAT

Containment, Eradication, and Recovery

What we did instead:

1. Continued to monitor outbound connectivity to attempt to identify other C&C or data exfiltration targets
2. Enhance monitoring of impacted servers to identify additional lateral movement and compromised servers and accounts
3. Create new admin accounts to allow for continued administration of servers (legitimately)
4. Additional logging enabled for all known compromised accounts

Eventually: terminate all compromised accounts and block IPs at once

Post-Incident Activities

1. Deploy additional security monitoring software (permanently)
2. Additional security requirements for customer/external administrators
3. Enforce MFA for all remote and admin access
4. Share information with all federal government to improve their monitoring

Other actions:

- DOI CIO and OPM leadership testified in front of US Congress
- OPM Director resigned
- OPM CIO resigned

Other Major Breaches

- MGM Resorts
- Equifax
- Target
- DNC Emails
- Adult Friend Finder
- SolarWinds*

Note: some of this data is taken from reporting and other public sources and may not be 100% accurate

MGM Resorts - Breach Info

When: September 2023

Who: Scattered Spider (US/UK Criminal Gangs)

Impact: $100M+

Attack Vector(s) / Methods:

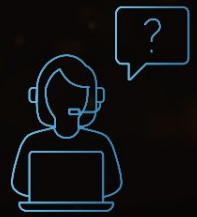
1. Social Engineering attack on IT Service Desk (to reset MFA of Okta admin)
2. Compromise Okta server admins and other system admins
3. Encrypt and exfiltrate sensitive data

MGM Attack Flow (September 2023)

1. Gather intelligence about MGM and its employees

2. Choose targeted victims – those likely to have high privilege in Okta's systems – through LinkedIn

3. Perform vishing (voice phishing) attack:
   - Contact the MGM's IT Desk
   - Impersonate a privileged victim
   - Get IT to reset the MFA of the victim user



6. Encrypt 100 ESXi servers and disrupt all the VMs and services that run on top of them

Domain admins on the domain controllers

Admins on the Okta syncing server

Global administrator in Azure

4. Compromise Okta super administrator and then more admins

5. Exfiltrate sensitive data from the network

Image Credit: CyberArk

MGM Resorts - Lessons Learned

- (New) social engineering techniques are a big risk
- Administrators are big targets
- Managing permissions is hard (Help Desk admin access)
- Implementing good authentication/MFA (Okta) is not enough

Equifax - Breach Info

When: September 2017

Who: Chinese State Actors (Suspected)

Impact: 163M accounts with sensitive data (SSNs, DOB, driver’s license numbers, names addresses); $1.4B in clean-up costs + $575M settlement

Attack Vector(s) / Methods:

1. Hackers exploited unpatched Apache Struts vulnerability
2. Moved laterally internally due to lack of segmentation
3. Found credentials stored in plain text that allowed further access
4. Data exfiltration undetected due to failure to renew expired certificate

Equifax - Lessons Learned

- Vulnerability and patch management
- Network segmentation and internal network monitoring
- Protect credentials
- Keep up with maintenance of your security tools

Target - Breach Info

When: September 2013

Impact: 40M credit/debit cards stolen, 70M customer records, $200M+ (including $18.5M settlement), 46% reduction in earnings in following quarters

Attack Vector(s) / Methods:

1. Third-party contractor (Fazio Mechanical Services) victim of phishing
2. Stolen credentials used to access Target network and install malware* on Point-Of-Sale (POS) machines
3. Malware collected and exfiltrated sensitive customer data

* security tool alerted to this

Target - Lessons Learned

- Vendor/Partner management is critical
- Proper tuning of security tools (and investigating alerts) is critical
- All components of your network (like POS systems) are targets
- Know where sensitive data is

DNC Emails - Breach Info

When: 2016

Who: Russian Intelligence

Impact: 19k+ emails and 8k+ attachments leaked (strategy information, donor information, etc.)

Attack Vector(s) / Methods:

1. Spearfishing email sent with link to reset password (simulating Google notification)
2. Keyloggers and other malware installed
3. Data exfiltrated

DNC Emails - Lessons Learned

- Email security still paramount
- User training on how to identify phishing emails can help
- MFA is important

Adult Friend Finder - Breach Info

When: November 2016

Who:

Impact: 412M user accounts (inc. 15M deleted user accounts) with data like usernames/passwords and email addresses (inc. gov/mil)

Attack Vector(s) / Methods:

1. Local File Inclusion (LFI) vulnerability provided initial access
2. Passwords stored in plain text allowed further access
3. Data exfiltration

Adult Friend Finder - Lessons Learned

- Keep security systems up to date to protect against modern attack techniques (some reporting stated minimal updates since 1996)
- Protect credentials
- Check for common vulnerabilities, especially on external-facing systems
- Don’t use your primary email account if cheating on your SO

SolarWinds - Overview

SolarWinds makes software (“Orion”) to manage IT infrastructure (networks, databases, cloud systems, etc.) for 30k customers (including a lot of government)

When: 2019-2020

Who: Russian State Actors

What: Threat actors gained access into SolarWinds internal systems and injected malware into software updates

Impact: 18k+ customers (including a large number of federal agencies) installed malicious updates into their environments

SolarWinds - Timeline & Detection

September 2019: Threat actors gain access into SolarWinds network

October 2019: Threat actors test initial code injection into Orion

February 2020: Malicious code known as “Sunburst” injected into Orion

March 2020: SolarWinds distributes Orion software updates to customers (including the injected malicious code)

Initial Detection: FireEye detected malicious traffic in customer networks (and found that it was infected as well)

SolarWinds - Response

Response: Organizations scrambled to determine if they had the impacted version and to remove it from or isolate it in their network (denying internet access)

Domain used by malware turned into Killswitch:

“Depending on the IP address returned when the malware resolves avsvmcloud[.]com, under certain conditions, the malware would terminate itself and prevent further execution. FireEye collaborated with GoDaddy and Microsoft to deactivate SUNBURST infections.

“This killswitch will affect new and previous SUNBURST infections by disabling SUNBURST deployments that are still beaconing to avsvmcloud[.]com. However, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the SUNBURST backdoor.

This killswitch will not remove the actor from victim networks where they have established other backdoors. However, it will make it more difficult to for the actor to leverage the previously distributed versions of SUNBURST.”

SolarWinds - Lessons Learned

- Need to be aware of supply-chain / vendor risks
- Tracking internal software update procedures / version control is critical
- Understand what your management tools can do (e.g. do they need to talk to the internet?)

Q & A