RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AIR-T01**

Best Teacher is Last Mistake: Improving and Applying Incident Response Plan

Mike Jankowski-Lorek, Ph.D.

Director of Consulting
CQURE Inc.
@MJL_PL

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Impactful Hacking Stats for 2021

1318%

year-on-year increase in ransomware attacks in the first half of 2021

54%

of malicious apps impersonated TikTok, in total 164 malicious apps related to COVID-19 scams were detected

94%

of malware is delivered via email

77%

of organizations do not have a cyber security incident response plan

Source: Source: Trend Micro, IBM, CSO (2021)

Phish Biting

69% OF IT SECURITY PROS SAY THEY COME ACROSS PHISHING MESSAGES THAT GET PAST SPAM FILTERS

USERS TRAINED IN AVOIDING PHISHING AND SCAM EMAILS FELL FOR THESE MALICIOUS EMAILS 42% LESS THAN THOSE WITHOUT TRAINING

27% OF IT ORGANIZATIONS HAVE TOP EXECUTIVES OR PRIVILEDGED USERS WHO HAVE FALLEN FOR MALICIOUS EMAIL ATTACKS

Uneducated Employees

THE TOP CAUSE OF ORGANIZATIONAL DATA BREACHES IS ‘NEGLIGENT INSIDERS’

TODAY’S ORGANIZATIONS EXPERIENCE AN AVERAGE OF **14 INCIDENTS/YEAR** OF UNINTENTIONAL DATA LOSS THROUGH EMPLOYEE NEGLIGENCE

Demo

Initial Access Privilege Escalation

What is an **Incident**?

An **INCIDENT** is an adverse event in an information system, and/or network, or the threat of the occurrence of such an event

Incidents implied **harm**, or the attempt to do **harm**

The fact that an incident has occurred may mean a **law has been broken**

Incidents

Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

Examples

- Denial of service attack causes web server to crash
- Malware installed from a phishing attack infects user computers and establishes connections with an external host
- An attacker obtains sensitive data and demands ransom from your CEO to prevent release
- Sensitive information from your company is being disseminated through peer-to-peer file sharing services

Why is it important?

- Sooner or later an incident is going to occur

  Do you know what to do?

- It is not a matter of IF but WHEN
- Planning is everything
- Similar to backups
- You might not use it every day, but if a major problem occurs you are going to be glad that you did

Incidents

Incidents would not happen if:

- We had infinite security budgets, and
- We had infinitely capable security personnel

However, things can go wrong

- In spite of your best attempts
- We call them incidents

Useful to develop standard procedures to respond to incidents

- And refine these procedures based on experience
- Typical business process improvement exercise

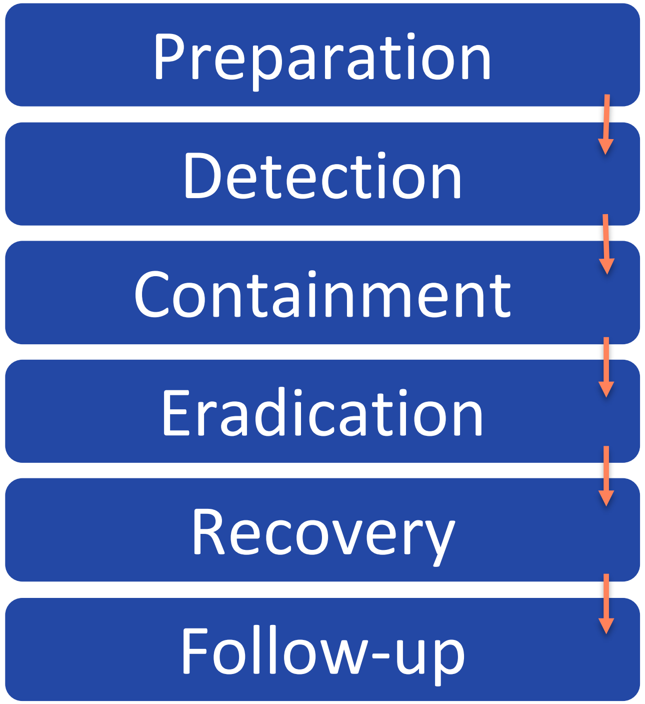
Incident handling

Overall process similar for most incidents

(with minor incident-specific variations)

Described in NIST 800-61

- Preparation
- Detection and Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Analysis (Follow-up)



Demo

Something is odd

Demo

Power of PowerShell

Initiating an Investigation (1/2)

- **DO NOT** begin by exploring files on system randomly
- Establish evidence custodian - start a detailed journal with the date and time and date/information discovered
- If possible, designate suspected equipment as “off-limits” to normal activity. This includes back-ups, remotely or locally scheduled house-keeping, and configuration changes
- Collect email, DNS, and other network service logs

Initiating an Investigation (2/2)

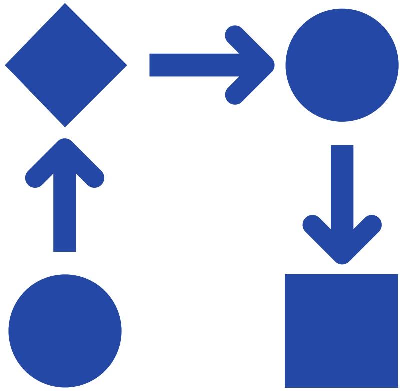
- Capture exhaustive external TCP and UDP port scans of the host

  Could present a problem if TCP is wrapped

- Contact security personnel [CERT], management, Federal and local enforcement, as well as affected sites or persons

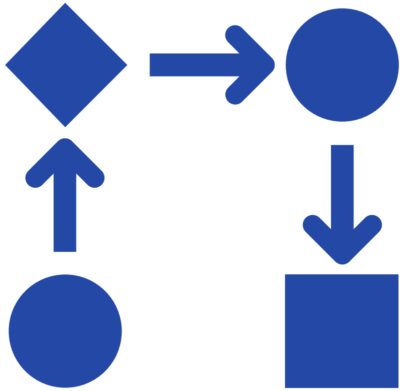
Incident Response (1/2)

- Identify, designate, or become evidence custodian
- Review any existing journal of what has been done to system already and/or how intrusion was detected
- Begin new or maintain existing journal
- Use monitoring tools (sniffers, port detectors, etc.)
- Without rebooting or affecting running processes, perform a copy of physical disk
- Capture network information



Incident Response (2/2)

- Capture processes and files in use (e.g. dll, exe)
- Capture config information
- Receipt and signing of data



Handling Information (1/2)

Information and data being sought after and collected in the investigation must be properly handled

Volatile Information

- Network Information
  - Communication between system and the network
- Active Processes
  - Programs and daemons currently active on the system
- Logged-on Users
  - Users/employees currently using system
- Open Files
  - Libraries in use; hidden files; Trojans (rootkit) loaded in system

Handling Information (1/2)

Non-Volatile Information

- This includes information, configuration settings, system files and registry settings that are available after reboot
- Accessed through drive mappings from system
- This information should be investigated and reviewed from a backup copy

RSAConference2022

Demo

EVTX from memory

RSAConference2022

Demo

Automatic destinations

Preparation

First step in creating an incident response plan:

- Not an enumeration process…
  - Listing all possible threat scenarios
  - And appropriate response to each of these scenarios
- More productive:
  - Identify basic steps common to all events
  - Plan execution of each of these steps

Incident Preparation Components

Peacetime activity

- Incident response policy
- Incident response team
- Supporting team
- Incident communication
- Compliance
- Hardware and software
- Training

Summary

Identify the major components of dealing with an incident

The elements of disaster recovery and business continuity planning

Prepare a basic policy outlining a methodology for the handling of an incident

Report on the incident to improve preparation for a similar incident in the future

Understand the incident handling lifecycle

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AIR-T01**

Best Teacher is Last Mistake: Improving and Applying Incident Response Plan

Mike Jankowski-Lorek, Ph.D.

Director of Consulting
CQURE Inc.
@MJL_PL