

CYBER SECURITY TASK 2

HETRICIA TSUNDZU CHAUKE



February 13, 2024

INTERN CAREER

CYBER SECURITY

# **Task 2: Incident Response Simulation**

**Scenario Creation:**

The following scenario is a Malware Attack on Corporate Network.

**1. Scenario Context:**

* Company Profile*:* ABC Corporation is a multinational company with a significant online presence and a vast network infrastructure.
* Industry*:* Technology and Manufacturing.
* Recent Changes*:* The company recently implemented a new software update across all systems.

**2. Objectives:**

* Objective 1*:* Simulate a malware attack that originates from a phishing email targeting employees.
* Objective 2*:* Evaluate the incident response team's ability to detect, analyze, and mitigate the malware.
* Objective 3: Test the company's incident response plan effectiveness.

**3. Scope:**

* Affected Systems: Windows-based wo b rkstations, servers, and some IoT devices.
* Timeline*:* The incident occurred overnight, and the detection window is within the first 24 hours.
* Impact*:* Aim for business disruption, potential data exfiltration risk, and financial consequences.

**Incident Detection:**

**1. Incident Response Team Roles:**

* Incident Commander*:* Oversees the entire incident response process.
* Lead Analyst*:* Responsible for malware analysis and determining the scope of the attack.
* Network Security Analyst: Monitors network traffic for unusual patterns and identifies the source of the attack.
* Endpoint Security Analyst: Analyzes logs and activities on individual workstations.
* Communication Coordinator: Handles internal and external communication throughout the incident.

**2. Simulating Incident Detection:**

* Initial Alert: The network security monitoring tool generates an alert about unusual outbound traffic patterns from a specific department's subnet.
* Email Phishing Simulation: An employee reports a suspicious email received yesterday; the incident response team traces it back to a phishing campaign.
* Endpoint Protection Logs: Unusual activities on several workstations trigger alerts in the endpoint security solution.
* Anomaly Detection: Abnormal login patterns are detected in the corporate VPN system.

**3. Incident Response Timeline:**

* T0*:* Initial alert triggers incident response team activation.
* T1*:* Investigation reveals phishing email as the likely source; communication coordinator informs employees about the potential threat.
* T2*:* Malware analysis indicates a new variant with data exfiltration capabilities; lead analyst assesses the scope.
* T4*:* Network security analyst identifies the affected systems and isolates them from the network.
* T6*:* Endpoint security analyst starts cleaning malware from workstations; communication coordinator updates stakeholders.
* T8*:* Confirmation that the malware is contained and eradicated; post-incident analysis begins.

**4. Debriefing:**

* Lessons Learned: Evaluate the effectiveness of incident response processes and identify areas for improvement.
* Documentation*:* Document incident details, actions taken, and recommendations for future prevention.
* EmployeeAwareness: Conduct awareness training based on the incident findings to prevent similar future attacks.

This simulated scenario helps interns develop incident response skills, from detecting the initial signs of a malware attack to coordinating an effective response and conducting a thorough post-incident analysis.

**Response Plan Execution:**

**1. Incident Response Plan Initiation:**

* IncidentCommander*:* Confirms the incident and activates the incident response team.
* CommunicationCoordinator*:* Initiates communication channels to keep stakeholders informed.
* LeadAnalyst*:* Coordinates the incident response efforts and ensures adherence to the response plan.

**2. Containment and Mitigation:**

* Network Security Analyst*:* Isolates affected systems and segments from the network.
* Endpoint Security Analyst: Coordinates with IT to disconnect infected workstations and start cleaning malware.
* Incident Commander: Monitors the overall response progress and adjusts strategies as needed.
* Communication Coordinator: Regularly updates employees on the situation and provides guidance.

**3. Communication with Stakeholders:**

* Communication Coordinator: Provides regular updates to executives, IT teams, and employees.
* Public Relations Liaison: If required, liaises with PR to prepare statements for external communication.
* Legal Advisor: Provides guidance on compliance and legal obligations regarding data breaches.

**4. Recovery Actions:**

* IT Support Team: Restores affected systems from clean backups.
* Incident Commander: Verifies the success of recovery actions and authorizes the gradual return to normal operations.

**Forensic Analysis:**

**1. Incident Documentation:**

* Lead Analyst: Documents the incident timeline, actions taken, and initial findings.
* Communication Coordinator: Ensures all communication during the incident is documented.

**2. Forensic Analysis Process:**

* Lead Analyst: Directs the forensic analysis team to identify the root cause of the incident.
* Forensic Analysts: Collects system images, logs, and memory dumps from affected systems.
* Network Security Analyst: Analyzes network logs to trace the malware's entry point and lateral movement.
* Endpoint Security Analyst: Examines logs for any indicators of compromise (IoCs) and traces the malware's behavior on workstations.

**3. Evidence Collection:**

* Lead Analyst: Oversees the collection of evidence for legal and post-incident analysis.
* Forensic Analysts: Catalogs and preserves relevant data, ensuring the chain of custody is maintained.

**4. Post-Incident Analysis:**

* Lead Analyst: Conducts a comprehensive review of the incident, identifying gaps in security and areas for improvement.
* Communication Coordinator: Prepares a post-incident report for internal stakeholders.
* Training Coordinator: Recommends additional training based on the incident's findings.

**5. Remediation Recommendations:**

* Lead Analyst: Provides recommendations for improving security measures to prevent similar incidents.
* IT Security Team: Implements the recommended changes in security policies, procedures, and technologies.

**6. Legal and Compliance Review:**

* Legal Advisor: Reviews the incident details to ensure compliance with relevant laws and regulations.
* Compliance Officer: Implements any necessary changes to maintain compliance.

This comprehensive response plan ensures that the incident is contained, mitigated, and thoroughly analyzed. It also focuses on communication, recovery, and continuous improvement to enhance the organization's cybersecurity posture.

**Documentation:**

Title*:* Malware Attack Incident Response Report

Date*:* 01/02/2024

Preparedby*:* Incident Response Team

A malware Attack occurred in the ABC Corporation, the malware attack affected the company’s system, the incident response team had some tasks to do to know how they will to what extent the attack origin is.

**3. Incident Overview:**

* Incident Type: Malware Attack
* Timeline: Detailed chronology of events, from initial detection to containment and resolution.
* Scope: Affected systems, departments, and potential data exposure.

**4. Incident Response Actions:**

**Roles of the Incident Response Team:**

The incident commander oversees the whole incident response procedure.

Lead Analyst: Determines the scope of the attack and carries out malware analysis.

Network Security Analyst: Tracks unusual activity on the network and locates the source of the assault. Analyzes activity and logs on specific workstations as an endpoint securityanalyst. During the incident, the coordinator of communication oversees both external and internal communication.

Coordinator of Communications: Opens lines of contact and provides updates to interested parties. Communication Coordinator: Frequently informs staff members of developments and offers direction. Stakeholder communication: Executives, IT teams, and staff receive regular updates from the communication coordinator. Liaison with Public Relations: Cooperates with PR as needed to draft remarks for dissemination to the outside world. Guidance on compliance and legal requirements with data breaches is provided by a legal advisor.

The Network Security Analyst is essential to the incident response process because they isolate the compromised systems and network segments, stopping the issue from spreading further. Concurrently, the IT staff and the Endpoint Security Analyst unplug compromised computers and start malware removal processes. The entire response effort is managed by the incident commander, who keeps an eye on developments and modifies tactics as needed to effectively handle the situation. In the meantime, the coordinator of communication makes sure that staff members receive regular, educational updates. She also provides direction to help staff members stay informed and take the necessary steps during the incident response process.

The root cause of the incident was identified as a successful phishing attack that led to the deployment of malware within the corporate network. The attack exploited vulnerabilities in the company's email security protocols, allowing the malicious actors to bypass traditional security measures and deliver a payload via an email attachment. Upon opening the attachment, the malware executed and began its malicious activities, including spreading across the network, exfiltrating sensitive data, and establishing backdoor access for remote control.

Catalog of Collected Evidence, Logs, and Forensic Analysis Findings:

1. **Email Logs:**
   * Logs detailing the receipt and delivery of the phishing email.
   * Metadata analysis of the email headers to trace its origin.
2. **Network Traffic Logs:**
   * Records of unusual outbound traffic patterns indicating communication with malicious command and control (C2) servers.
   * Analysis of network flow data to identify lateral movement of the malware.
3. **Endpoint Logs:**
   * Logs from infected workstations showing execution of malicious processes.
   * System event logs capturing abnormal activities, such as unauthorized access attempts and file modifications.
4. **Memory Dumps:**
   * Memory dumps from compromised systems to analyze the runtime behavior of the malware.
   * Examination of memory artifacts for evidence of process injection and persistence mechanisms.
5. **File System Forensics:**
   * File system analysis to identify and quarantine malicious files.
   * Examination of file timestamps and attributes for indicators of compromise.
6. **Registry Analysis:**
   * Registry forensics to detect registry keys created or modified by the malware.
   * Identification of registry persistence mechanisms used by the malware.
7. **Malware Samples:**
   * Collection of malware samples for further analysis and signature creation.
   * VirusTotal or similar analysis results to determine the malware's characteristics and prevalence.

List of Indicators of Compromise (IoCs) Identified During the Investigation:

1. **Email IoCs:**
   * Sender email address: [Phishing email sender]
   * Subject line: [Phishing email subject]
   * Attachment filename: [Name of malicious attachment]
2. **Network IoCs:**
   * IP addresses of malicious C2 servers: [IP addresses]
   * Domain names associated with the attack: [Domain names]
3. **Endpoint IoCs:**
   * File hashes of the malware executable: [MD5/SHA256 hashes]
   * Registry keys associated with malware persistence: [Registry keys]
4. **Behavioral IoCs:**
   * Unusual outbound network traffic patterns.
   * Abnormal process execution and file modification activities on endpoints.

The incident underscores the critical importance of ongoing phishing awareness training for employees to recognize and report suspicious emails effectively, thereby reducing the risk of successful phishing attacks. Additionally, enhancing email security measures, such as advanced threat protection solutions and regular assessments, can improve the detection and prevention of phishing attempts. Network segmentation is highlighted as crucial in limiting the spread of malware across the network, emphasizing the need to isolate zones to contain potential breaches. Deploying Endpoint Detection and Response (EDR) solutions provides real-time visibility into endpoint activities, aiding in the rapid detection and response to malware infections. Regularly reviewing and updating the incident response plan based on lessons learned from such incidents ensures organizational readiness to address future cybersecurity threats, with feedback incorporation enhancing the plan's effectiveness and adaptability.

To enhance incident response capabilities, organizations should focus on several key strategies. Firstly, strengthening integration with external threat intelligence sources enables proactive identification of emerging threats and Indicators of Compromise (IoCs). Automation and orchestration tools streamline incident response processes, reducing manual effort and improving response times. Regular tabletop exercises test the incident response plan and provide valuable hands-on experience for team members. Cross-functional collaboration among departments, including IT, security, legal, and compliance, ensures a coordinated response effort. Continuous monitoring and proactive threat hunting initiatives detect and mitigate threats before they escalate. Lastly, conducting thorough post-incident reviews and implementing corrective actions based on lessons learned from past incidents continuously improves incident response capabilities and resilience against future threats.

Following the malware attack, several actions were taken to restore normal operations within the organization. IT support teams prioritized the restoration of critical systems and services, utilizing clean backups to rebuild compromised systems and ensure data integrity. Endpoint security analysts thoroughly cleaned and reimaged infected workstations, verifying their integrity before reconnecting them to the network. Network security analysts reconfigured network settings to remove vulnerabilities exploited by the malware, conducting scans to identify and remediate compromised devices. Additional training sessions were conducted to educate employees about the incident, reinforce phishing awareness, and promote safe computing practices. Furthermore, enhanced monitoring and surveillance measures, including intrusion detection and prevention systems, were implemented to continuously monitor network and endpoint activities and detect/prevent future attacks.

The organization proposes comprehensive changes to its policies, procedures, and technologies to bolster cybersecurity defenses. This includes enhancing the email security policy to mandate encryption, multi-factor authentication (MFA), and regular phishing simulation exercises for employees. Advanced endpoint protection solutions, such as endpoint detection and response (EDR) tools, will be implemented to improve visibility and control over endpoint activities, alongside enforcing strict application whitelisting and privilege management. Network segmentation policies will be revised to create more granular network zones, incorporating micro-segmentation to isolate critical assets and contain malware spread. The incident response plan will be updated to streamline communication protocols, clarify roles, and integrate automation and orchestration capabilities for enhanced agility. Patch management processes will be strengthened with automated deployment solutions and regular vulnerability scanning. Third-party risk management practices will be enhanced to assess and monitor vendors' security posture, while data backup and recovery procedures will undergo review and improvement to ensure data resiliency through regular backups, offsite storage, and disaster recovery testing.

The legal advisor conducted a thorough assessment of the incident's legal and regulatory implications, focusing on data privacy laws, contractual obligations, regulatory compliance, litigation risks, and cyber insurance coverage. They identified potential liabilities and provided recommendations to mitigate legal risks, including proactive communication with affected parties and regulatory authorities, updating contracts with cybersecurity provisions, and ensuring ongoing compliance with industry-specific regulations. Following the assessment, the organization promptly took steps to address compliance issues, including notifying affected parties, updating contracts, implementing regulatory compliance measures, preparing for potential litigation, and initiating the cyber insurance claims process to expedite claims settlement. These proactive measures aimed to minimize legal liabilities and ensure compliance with relevant laws and regulations.

**Presentation:**

KINDLY DOUBLE CLICK THE PICTURE ABOVE:

