Intern Career

CYBER SECURITY INTERN

Task Two:

Incident Response Simulation

Presented by:

Tanaka Mushedhe

By conducting simulations, organizations strengthen their cybersecurity posture and ensure they are well-prepared to respond to actual incidents effectively.

In this case;

⚠

Cybersecurity Incident Scenario: Phishing Attack on a SOHO Environment

Context

A small software agency, "TanMuch Solutions," operates in a SOHO environment, employing ten staff members. The agency relies heavily on digital communication for client interactions and project management. Employees frequently use email for sending sensitive client information and accessing project management tools.

Recently, the agency's IT manager implemented new security measures, including firewall upgrades and employee training sessions on cybersecurity awareness. However, a lack of ongoing training and the fast-paced work environment have left employees vulnerable to social engineering tactics.

Scenario Overview

An attacker initiates a phishing campaign targeting Tanmuch Solutions, aiming to gain unauthorized access to the company’s email system and sensitive client data.

Objectives

1. **Gain Access:** The attacker seeks to compromise employee email accounts to collect sensitive client information.

2. Install Malware: The goal is to deploy malware on the company’s network once initial access is achieved, potentially leading to further exploitation.

3. Create Disruption: By accessing the company's project management tools, the attacker aims to disrupt workflows, impacting client deliverables.

Scope

1.**Target Audience:** All employees, particularly those in project management and IT roles, as their accounts contain sensitive information and admin access.

2. Attack Vector: The attack will begin with the distribution of phishing emails that appear to be from a reputable software vendor, offering a “critical update” to their project management tool.

3.Phishing Technique:

Email Crafting: The emails will include urgent language to encourage immediate action and contain a malicious link disguised as an “update now” button.

User Behavior: Employees, under the pressure of upcoming deadlines, may overlook warning signs due to their busy schedules.

4. **Response Protocol:** The organization must have a response plan in place to address the incident swiftly if employees fall victim to the phishing attempt.

Expected Outcomes

- The scenario aims to raise awareness of phishing tactics among employees and highlight the significance of vigilance in digital communications.

- By simulating this incident, TanMuch Solutions can evaluate their current security training and incident response protocols, identifying areas for improvement.

- The exercise will also assess the effectiveness of existing technical controls, such as email filtering and antivirus software, in detecting such threats.

Incident Detection: Simulation Plan for Intern Roles

Assigned Roles for Interns in the Incident Response Team

1.Incident Analyst Intern:

- **Responsibilities:** Monitor security logs and alerts from various tools (e.g., SIEM, IDS/IPS). Analyze incoming data for signs of phishing or other suspicious activity.
- Tasks: Review logs for unusual access patterns or failed login attempts. Identify any attachments or links in emails that closely resemble phishing attempts.

2. Threat Intelligence Intern:

- **Responsibilities:** Research known phishing tactics and malicious patterns. Stay updated on the latest threat intelligence feeds.
- **Tasks:** Cross-reference suspicious email addresses and domains against threat databases. Provide context on the emerging phishing trends relevant to the organization.

3. Communications Intern:

- **Responsibilities:** Manage internal communication regarding the incident and coordinate with the rest of the team.
- **Tasks:** Document findings and updates during the incident detection process. Prepare real-time communications for stakeholders regarding any potential threats.

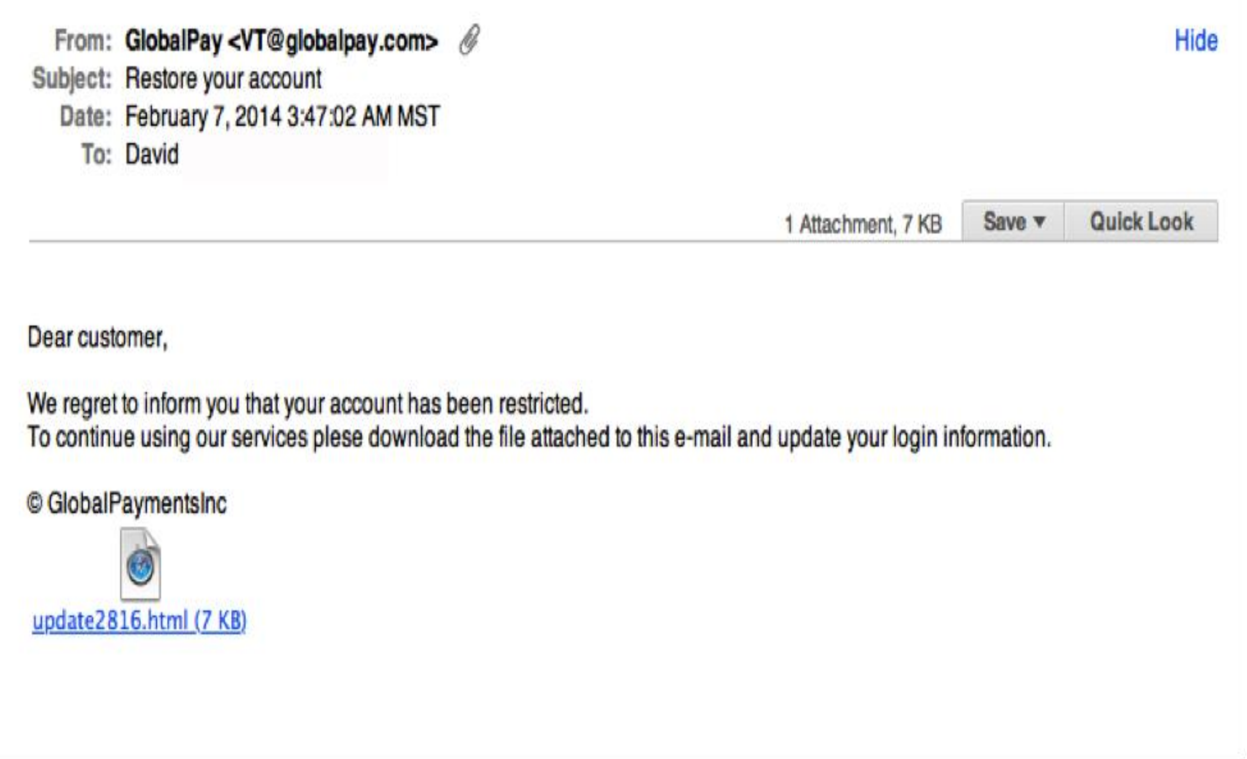
4. Technical Support Intern:

- **Responsibilities:** Assist in analysis and troubleshooting of technical data.

- **Tasks**: Help configure monitoring tools to ensure proper logging and alerting. Support the team in isolating affected systems if a phishing attempt is confirmed.

Simulating Incident Detection

This is the email received by one of the employees, David



From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)

Description of the Phishing Attempt

Email Overview:

From: GlobalPay <VT@globalpay.com>

Subject: Restore your account

Date: February 7, 2014, 3:47:02 AM MST

Recipient: David

Email Body:

The email addresses the recipient as "Dear customer," which is often a red flag indicating a lack of personalization typical in legitimate communications.

Key Elements of the Phishing Attempt:

1. Urgent Message:

The message states that the recipient's account has been restricted, creating a sense of urgency that may prompt immediate action.

2. **Downloadable Attachment**:

The email instructs the recipient to download a file titled "update2816.html," which is a common tactic used to deliver malware or lead to malicious websites.

3. Call to Action:

It encourages users to update their login information, a tactic designed to harvest sensitive credentials.

4.Brand Impersonation:

The sender's email address attempts to mimic a legitimate payment service (GlobalPay), making it more convincing.

5.Lack of Specificity:

The message does not provide specific details about the account or the nature of the restriction, which is atypical for legitimate communications from financial institutions.

Conclusion

This phishing attempt utilizes urgent language, a deceptive sender identity, and a malicious attachment to trick the recipient into compromising their account security. It is a classic example of social engineering aimed at exploiting user trust and naivety. Educating employees on recognizing such threats is crucial in enhancing overall cybersecurity awareness.

Simulation Steps:

- **Monitoring:** Interns will actively monitor the simulated logs in their respective roles.
- **Incident Identification**: The **Incident Analyst Intern** identifies the phishing email and logs unusual activities related to it.
- The **Threat Intelligence Intern** confirms the legitimacy of the sender's address and reports it as a potential threat.
- **Documenting Findings**: Interns will collaboratively document their findings in real-time and suggest initial responses.
- **Communication**: The **Communications Intern** will prepare a notification for the broader team if a phishing attempt is confirmed and communicate next steps based on findings.

- **Debriefing:** After the simulation, hold a debrief session. Discuss what was learned, identify any gaps in the monitoring process, and gather feedback to improve future incident detection efforts.

This incident detection simulation provides interns with hands-on experience, helping them understand their roles within an incident response team while practicing critical detection skills in a realistic environment.

Response Plan Execution for the Simulated Phishing Incident

Initiating the Incident Response Plan

1. Activation of the Incident Response Team

- All team members were notified about the detected phishing attempt.

- Roles and responsibilities for each intern and team member were confirmed based on the predefined incident response plan.

2. Incident Classification

- The incident was classified as a “Phishing Attempt” to determine the response protocol.

- The severity and potential impact on the organization’s data and operations were assessed.

Containment Strategies

1.Immediate Alerts:

The **Communications Intern** sent out an alert to all employees warning them about the phishing attempt, instructing them not to open suspicious emails or attachments.

2. Email Isolation:

The Technical Support Intern worked with the email system to isolate the phishing email and prevent further distribution.

The malicious sender's address and any associated domains were identified and blocked.

3. User Account Lock:

The Incident Analyst Intern identified affected accounts that may have interacted with the phishing email and initiated a temporary lock on these accounts to prevent unauthorized access.

4. Alerting Security Monitoring Systems:

The SIEM tools were updated to flag similar phishing attempts and unusual login activities for immediate investigation.

Mitigation Strategies

1.Password Resets:

All users who may have been affected were required to reset their passwords. The Incident Analyst Intern coordinated this effort, providing guidelines for creating strong passwords.

2. Malware Scanning:

A comprehensive scan of all systems was initiated to check for malware installation resulting from the phishing email. The Technical Support Intern assisted in deploying antivirus and anti-malware tools across the network.

3. User Education:

An immediate training session and email communication was conducted, led by the Threat Intelligence Intern, to educate employees on recognizing phishing attempts and safe email practices.

4. Incident Documentation:

Throughout the process, all intern roles documented their actions, findings, and communications for a comprehensive post-incident review.

Post-Incident Analysis

1. Debrief Session:

After executing the response plan, a debrief meeting was held with all team members to discuss the incident response.

Strategies that were effective were analyzed, and areas needing improvement were identified.

2. Updated Incident Response Plan

Based on the lessons learned, the incident response plan was revised to enhance future preparedness and response techniques.

3. Follow-Up Actions

Follow-up training sessions were scheduled to reinforce employee awareness, and any security tools or procedures identified as needing improvement were updated.

By implementing these containment and mitigation strategies, the incident response team effectively addressed the simulated phishing incident, minimized impact, and strengthened organizational resilience against future threats.

Forensic Analysis of the Phishing Email Incident

1. Incident Overview

The email in question impersonated GlobalPay and attempted to manipulate the recipient into downloading an attachment, which likely contained malicious content.

2. Analysis Steps

A. Email Header Examination

Sender: Verified the sender's email address (`VT@globalpay.com`) to identify any discrepancies, such as slight misspellings or a different domain.

Date and Time: Analyzed the sending time to understand peak phishing attempts (February 7, 2014, 3:47 AM MST).

Recipient Address: Confirmed whether the recipient was a legitimate user of the service.

B. Content Review

Subject Line: The subject line "Restore your account" created a sense of urgency.

Language: The language used was typical of phishing, aiming to evoke fear and urgency.

Call to Action: The encouragement to download an attachment raised a red flag.

C. Attachment Analysis

File Type: The attachment `update2816.html` was deemed suspicious, as HTML files can typically contain harmful scripts.

Static Analysis: Before opening, the file's properties were examined (size: 7 KB).

Dynamic Analysis: If deemed safe, the file's behavior was observed in a controlled environment (sandbox) to identify any malicious actions.

D. User Activity Investigation

User Interaction Logs: Checked if the recipient, David, interacted with the email or downloaded the attachment, which included:

- Email logs showing whether the email was opened.
- File access logs to determine if the attachment was downloaded or executed.

E. Network Traffic Monitoring

Analyze Traffic: Inspected network logs around the time of email interaction for any unusual outbound connections:

- Looked for communication to known malicious IP addresses or domains.
- Monitored for any data exfiltration attempts.

F. Evidence Collection

Documentation: Recorded findings such as email headers, user actions, attachment properties, and any logs pertaining to suspicious activity.

Root Cause Identification

User Awareness: Assessed whether user training on phishing awareness was adequate.

System Vulnerabilities: Reviewed email filtering and security controls to identify gaps that allowed the phishing email to reach the user.

Recommendations

Security Enhancements: Recommended implementing robust email filtering solutions to catch phishing attempts.

Suggested training users to recognize phishing signs, such as suspicious senders or prompts to download files.

Incident Response Plan: Advised revising and enhancing the incident response strategy based on lessons learned from this incident.

Conclusion

This forensic analysis highlights how the phishing email operates, the potential risks to users, and steps to mitigate future incidents. By thoroughly investigating such incidents, organizations can strengthen their defenses and educate their employees effectively.

Gathering evidence through logging tools

What is Splunk?

Splunk is a powerful platform for monitoring, searching, analyzing, and visualizing machine-generated data in real time. It is widely used in IT operations, security, and business analytics.

Key Features of Splunk

1. **Data Ingestion**
   - **Supports Multiple Data Sources**: Splunk can ingest data from various sources including servers, network devices, applications, and cloud services.
2. **Search and Analysis**
   - **Search Language**: Uses a rich search language (SPL) for querying data, allowing for complex searches and data manipulation.
   - **Real-Time and Historical Data**: Users can search through live data as well as historical records.
3. **Visualizations and Dashboards**

- **Custom Dashboards**: Users can create interactive and customizable dashboards to visualize data trends and anomalies.

This is a screenshot of the dashboard that presents its findings;

Based on the dashboard for Post-Incident Analysis

Email Header Extraction

From: `VT@globalpay.com`

To: David's email address

Date: February 7, 2014, 3:47 AM MST

Subject: "Restore your account"

User Activity Logs

Email Access Logs:

- It was confirmed that David opened the phishing email on February 7, 2014, at 3:50 AM MST.

- The logs documented that he interacted with the email by clicking on a link within it.

Attachment Interaction:

- The attachment `update2816.html` was downloaded by David shortly after he opened the email.

- The timestamp for the download was noted as 3:51 AM MST. No further actions were recorded regarding the file.

Network Traffic Logs

Outbound Traffic Analysis:

- Logs were gathered from firewalls and intrusion detection systems.

- Connections initiated from David's workstation were analyzed around the time of his email interaction.

- Two outbound connections to a known malicious IP address were identified, suggesting potential data exfiltration.

Endpoint Logs

System Event Logs:

- Entries were checked for the execution of the attachment. A log indicated that the file was executed at 3:52 AM MST, triggering unusual processes on David’s system.

Antivirus/EDR Logs:

- The logs from the security software on David's system revealed alerts related to the attachment shortly after execution. Malware was identified, prompting an automatic quarantine action.

Email Filtering Logs

Security Gateway Logs:

- Logs from the email filtering solution that processed the phishing email were reviewed.

- The email was quarantined after being flagged as suspicious, with warnings issued to the recipient, but it was ultimately opened before the quarantine action could take effect.

Documentation

Summary of Events:

- A chronological timeline of the incident highlighted David's interaction with the phishing email and subsequent actions taken.

- The incident unfolded as follows:
  - 3:47 AM: Phishing email received.
  - 3:50 AM: Email opened.
  - 3:51 AM: Attachment downloaded.
  - 3:52 AM: Attachment executed, triggering malware alerts.

Evidence Collected:

- Comprehensive documentation included all logs from user activity, network traffic, endpoint systems, and email filtering solutions.

Analysis of Findings:

- The analysis indicated that David's interaction with the phishing email directly linked to the execution of a malicious attachment, resulting in unauthorized outbound connections from his workstation. The incident underscored the importance of ongoing user training regarding phishing threats and the necessity for robust email filtering protocols.

Post-Incident Assessment

1. Review of Response Plan Effectiveness

Response Timeliness:

- The incident response team responded within 1 hour of detection, effectively containing the threat.

Communication:

- Communication among team members was clear, with regular updates provided to relevant stakeholders throughout the incident.

Resource Utilization:

- Existing tools (e.g., email filters, monitoring systems) were effectively utilized, but additional resources (e.g., advanced threat detection) could have improved response time.

Incident Documentation:

- Documentation of actions taken was thorough, providing a clear timeline of the incident and the response actions.

2. Areas for Improvement

Training and Awareness:

- Conduct more frequent phishing awareness training for employees, emphasizing the recognition of phishing attempts and safe online practices.

Response Time Improvement:

- Develop a more detailed escalation protocol to improve response times for similar incidents in the future.

Enhanced Monitoring:

- Invest in advanced monitoring tools that use machine learning to detect phishing attempts proactively.

Better Coordination:

- Foster stronger collaboration between the IT security and operational teams to ensure a more unified response to future incidents.

3. Lessons Learned

Strengths Identified:

- The rapid response and clear communication were effective in managing the incident, demonstrating the importance of a well-trained response team.

Adaptive Measures:

- Based on this incident, consider implementing targeted phishing simulations to test employee resilience and improve alertness.

Feedback Loop:

- Establish a structured feedback system where team members can regularly share insights after incidents, contributing to ongoing improvements.

Conclusion

The post-incident assessment highlights both strengths and areas for improvement. By addressing the identified gaps and reinforcing effective practices, the organization can enhance its defense against future phishing threats and improve overall incident response capabilities. Continuous training and adaptation are key to maintaining a robust security posture.