Incident Report

Date: February 19,2024

Report Prepared by: Incident Response Team7

Incident Details:

Description:

This incident report is regarding a suspected social engineering attempt via a malicious email supposedly from the address joyce@dashlanedata.com. The email displays various traits that suggest social engineering tactics are being used to manipulate recipients into clicking on a potentially harmful link.

Incident Timeline:

1. Initially, the recipient or an automated email filtering system identifies the questionable email (Email received on February 19, 2024).

2. During the initial assessment phase which was done on February 20th,2024, the recipient or IT security personnel assess the email's legitimacy and potential threat level.

3. Thorough Analysis: The email undergoes a comprehensive analysis from February 20th through March 2nd 2024, which primarily concentrates on its substance, the identity of the sender, and any attachments or connections that may be embedded.

4. Examination of the email's substance demonstrates several indicators of a social engineering endeavor, such as deceptive language, manipulation techniques, and the inclusion of a link that may cause damage.

5. Documentation: (February 19th, 2024): An exhaustive report is produced to record the results of the analysis, which will provide a detailed account of the incident. This report detailed

information on the observed tactics, the perceived nature of the threat, and potential consequences.

6. The incident response protocols start on February 20th,2024 which includes putting in place security measures that are meant to reduce the risks that suspicious emails and any other threats could pose.

7. Communication and Reporting: February 23rd,2024: Informed parties, including management, IT security teams, and other relevant stakeholders, are provided with the incident findings through the compilation of a formal report.

8. In the February 25th,2024, phase, remediation measures are executed to proactively prevent recurrences of comparable incidents and to resolve any security vulnerabilities or gaps that were discovered during the incident response procedure.

Incident Findings:

1. Analysis of Suspicious Email:

- The email displayed several red flags commonly associated with social engineering attempts, including generic salutation, urgent language, and manipulation of text formatting.
- Language used in the email aimed to induce panic and urgency, utilizing phrases such as "URGENT MATTER" and "EXPEDITE this request."
- Presence of a hyperlink labeled "click me" immediately following the ".com" domain, suggesting an attempt to deceive recipients into clicking on the link.

Investigation and Response Actions:

- Initial Assessment: As soon as the email was found, it was given an initial evaluation to see if it was real and how dangerous it might be.

Key Findings:

1.Sender Identity: The email seemed to come from joyce@dashlanedata.com, but this address might not be real, which suggests that it was spoofed or compromised.
2.Social Engineering Techniques: The email used several tricks, such as false urgency, flattery, and clever formatting, to trick people and get a reaction.

3.Signs of Manipulation: the email had many red flags, like using generic greetings, bringing up a sense of urgency quickly, and switching between formal and informal language to make people in our organization panic and feel like they need to act right away.
4.Deceptive Link: The email had a link labeled "clickme," which was put in a way that made its real location hard to see so that people in our organization would click it without thinking.

5.Psychological Exploitation: The sender used both flattery and command language to play with the emotions of the receivers, making them less alert to possible threats and more likely to click on the malicious link.

- The email's text, sender identity, and embedded links were all carefully looked over to find signs of social engineering and figure out how dangerous they were.

- The results of the analysis were written up in a detailed report that explained the methods used and how they might have affected people in our company.

- Incident Response: Steps were taken to deal with the situation, such as putting in place security measures to lower the risk that the suspicious email and any threats that came with it offered.

- Communication and Reporting: The incident was reported to the right people in our company, and a written report was made to be sent to management, IT security teams, and other important people.

Recommendations and Lessons Learned:

- Enhance email filtering and blocking measures to prevent similar social engineering attempts in the future.
- Conduct regular security awareness training sessions to educate employees on the latest social engineering tactics and best practices for email security.
- Review and update incident response procedures and policies to improve readiness and resilience against emerging threats.

Incident Reporting and Communication:

- Incident reports were prepared and shared to executive management, the IT security team, and relevant stakeholders for awareness and decision-making.
- Communication with affected parties, including employees and stakeholders, was conducted to provide updates and guidance on the incident response process.

Follow-Up and Ongoing Monitoring:

- Post-incident reviews were scheduled to evaluate the effectiveness of incident response actions and identify areas for improvement.
- Ongoing monitoring of systems and networks was established to detect and mitigate any further signs of suspicious activity or follow-up social engineering attempts.

Final Recommendations:

We recommend these activities and possibly implement these tools;

Email Security Gateways: Implement robust email security gateways equipped with advanced threat detection capabilities, including phishing and malware detection, content filtering, and URL scanning. Popular solutions in this category include Mimecast, Proofpoint, and Barracuda Email Security Gateway.

Security Information and Event Management (SIEM) Systems: Deploy SIEM systems to centralize and analyze logs from various sources, including network devices, servers, and applications. SIEM platforms such as Splunk, IBM QRadar, and LogRhythm can help detect anomalous activities indicative of social engineering attacks.

Endpoint Detection and Response (EDR) Solutions: Utilize EDR solutions to monitor and protect endpoints against sophisticated threats, including those initiated through social engineering tactics. Examples include CrowdStrike Falcon, Carbon Black, and SentinelOne.

Phishing Simulation and Training Tools: Implement phishing simulation platforms to conduct regular mock phishing campaigns and assess employees' adherence to social engineering attacks. These tools, such as KnowBe4, PhishMe (Cofense), and Proofpoint Security Awareness

Training, also provide interactive training modules to educate employees about phishing risks and best practices.

Web Filtering and Secure Web Gateways: Deploy web filtering and secure web gateway solutions to block access to known malicious websites and prevent users from inadvertently visiting phishing pages or downloading malware. Cisco Umbrella, Zscaler Internet Access, and McAfee Web Gateway are examples of such tools we can implement.

Conclusion:

The event shows that social engineering is still a threat and stresses how important it is for our group to take proactive steps to protect itself from these kinds of threats. Staying alert, teaching employees about security, and having strong security rules are all important for lowering the risk of social engineering threats and keeping company property safe.

Attachments:

Email analysis and Employee Interview

Report Prepared by: Team 7

Incident report Team7

Document Prepared: March 3rd, 2024