Security Incident Report

I. Investigation #1

1. Incident information

Ticket number	488021
User name	Marianne Haut-Nîmes
User email	marianne.haut-nimes@steeldoordataprotection.net
Type of incident	*Phishing email*
Severity	3-Serious
Justification for severity rating	Compromised account credentials for a critical internal system were submitted to a phishing site. This breach could lead to compromised data or unauthorized access, severely impacting operations.
Impact site	Account
Ticket transferred to Response Squad? (*yes / no)*	Yes
Communication sent to user? (*yes / no)*	Yes

Investigation details

Investigation steps taken

Email Sender Analysis:

1. Analyzed the raw email for SPF, DKIM, and DMARC results:
    - SPF: Pass
    - DKIM: Pass
    - DMARC: Pass
    - Sender: sddp.cloudsec@proton.me
    - Reply-To: Same as sender.
    - Server: ProtonMail server (mail-4027.protonmail.ch), IP address 185.70.40.27, located in Switzerland.
2. Phishing Domain Analysis:
    - URL: https://pwreset.vilinter.net
    - Domain Registration Details:
        - Registrar: OVH SAS, France.
        - Registered On: February 6, 2022.
        - Last Updated: February 1, 2024.
    - Finding: While the domain's age suggests legitimacy, its activity and association with phishing indicate malicious intent.
3. Phishing Site and Script Investigation:
    - The phishing site hosted a password reset form designed to collect credentials.
    - Identified a PHP script that harvested credentials and saved them in a local file (credentials.txt).
4. User Interaction:
    - The user clicked on the phishing link and entered their credentials, which were harvested by the attacker.
5. Server Location:
    - The phishing email originated from a ProtonMail server located in Switzerland (IP: 185.70.40.27). This server is unrelated to Steel Door Data Protection's legitimate infrastructure.

Attack sequence

1. User received an email impersonating Steel Door Data Protection's Cloud Security team, urging a password reset.

2. The email directed the user to a phishing site (https://pwreset.vilinter.net).

3. The user entered credentials, which were captured and stored by the phishing server.

Recommended actions

1. Disable the compromised account immediately and enforce a password reset.

2. Notify ProtonMail about the abuse of their infrastructure for phishing.

3. Block the phishing domain (vilinter.net) and associated IP addresses in the organization’s DNS and firewall.

4. Conduct a security awareness session with employees to reduce phishing risks.

5. System Integrity Check: Since no malware was detected on the user's device, reimaging or reformatting is not required at this time. However, ensure a system integrity check is performed to rule out any suspicious activity.

Additional information

1. Investigate whether other employees received similar phishing emails.
2. Monitor for similar domains (e.g., typosquatting) that may target the organization.
3. Enhance email filtering to block emails with spoofed domains.

II. Investigation #2

1. Incident information

Ticket number	385076
User name	Alex Treemist
User email	alex.treemist@steeldoordataprotection.net
Type of incident	*Phishing Email (Malicious Attachment)*
Severity	3-Serious
Justification for severity rating	The infected machine attempted to execute malicious PowerShell scripts, which could allow external control or data exfiltration. This poses a risk of compromised data and high degradation of operations.
Impact	Local Machine
Pertinent details of incident	User received a phishing email from accounting@steelsupplier.com with a subject "Urgent invoice, late payment." The email contained an attachment (invoice11122023.xls.7z) which, upon extraction and execution, launched Excel with malicious macros. The macros triggered PowerShell commands that attempted to download and execute additional malicious payloads, as identified in the SIEM logs and confirmed by sandboxing tools like Any.Run and VirusTotal.
Ticket transferred to Response Squad? (*yes / no)*	Yes
Communication sent to user? (*yes / no)*	Yes

Investigation details

Investigation steps taken

1. Email Header Analysis:
    - Sender Address: accounting@steelsupplier.com
    - Reply-To: Same as sender.
    - Server Location: France (hosted on kali server frhb82923ds.ikexpress.com, IP: 185.246.86.11).
    - SPF check resulted in a Temporary Error, and DKIM was missing, indicating spoofing.
    - Email flagged as spam and sent to Junk folder.
2. SIEM Log Analysis:
    - Detection Time: November 24, 2023, at 4:47 PM.
    - Flagged Event: Windows Defender identified a malicious Excel file containing macros as TrojanDownloader:097M/Obfuse.JR!MTB.
    - Logs confirmed that the macros attempted to execute PowerShell commands and connect to external IPs for additional payload downloads.
    - Threat was quarantined successfully by Defender.
3. Sandbox Analysis (Any.run & VirusTotal):
    - Any.run: Simulated execution of the attachment revealed that macros initiated obfuscated Base64 PowerShell commands designed to download and execute further payloads. High malicious score (100/100).
    - VirusTotal: Flagged the file as malicious by 44/58 antivirus engines, identifying it as a Trojan Downloader. File hash: 616FF5B5E7E018A537530DDEE769C8B7.
4. User Interaction:
    - User opened the attachment believing it to be an overdue invoice.
    - The macros attempted to connect to external Command & Control servers.

Attack sequence

1. Attacker sent phishing email with a malicious attachment.
2. User opened the attachment, which triggered Excel macros.
3. PowerShell commands attempted to connect to external servers.
4. Windows Defender quarantined the malicious file.

Recommended actions

1. Containment:
    - Immediately remove the compromised system from the network to prevent malware propagation.
    - Block the sender's IP (185.246.86.11) and associated domains in the firewall.
    - Escalate the incident to the Response Squad to investigate whether the phishing email was sent to others in the organization.
2. Reimage the System:
    - Perform an antivirus scan to confirm no additional malware exists before reimaging.
    - Reimage the system as a precautionary measure to ensure no persistent malware remains.
3. Train Employees:
    - Conduct phishing awareness training to reduce the likelihood of similar incidents.
4. Block Malicious IPs:
    - Ensure malicious IPs identified during this incident are blocked organization-wide via firewall rules and endpoint protection systems.
5. Leverage Security Tools:
    - Configure Windows Defender to enforce stricter policies for handling flagged files.
    - Verify DNS filtering and email filtering rules to block similar phishing attempts in the future.

Additional information

1. Investigate network logs for signs of malware propagation or lateral movement.
2. Adjust email filtering rules to block suspicious attachments.
3. Reimage the affected endpoint as a precaution to ensure no residual malicious artifacts remain.

Steel Door Data

Dear Marianne,

Thank you for reporting the issue with your account. After investigating, we've determined that the problem occurred because of a phishing email you received, which led you to enter your account credentials on a fraudulent website.

We understand how convincing these emails can look, but entering your credentials on an unverified website has serious implications. This incident resulted in the compromise of your account, and if not addressed quickly, could have led to unauthorized access to sensitive business information.

This kind of mistake, while unintentional, could have significant consequences for the company, including financial losses or legal risks. It is important to be vigilant when responding to emails, especially those requesting sensitive information.

What You Should Do Moving Forward:

1. Always verify the legitimacy of emails by checking the sender's address and any links provided.
2. Use only trusted, official channels for password resets or other account-related actions.
3. Complete the attached phishing awareness training to better identify and avoid fraudulent attempts in the future.

Your cooperation in learning from this situation is crucial to protecting our organization. If such incidents are repeated, they could lead to formal corrective actions.

We've taken steps to secure your account and prevent further unauthorized access. Please follow the link below to reset your password immediately using our official site:
https://accounts.steeldoordata-oc.com/passwordreset

Thank you for your understanding, and please let us know if you have any questions.

Best regards,

Luis Cruz
Steel Door Data Protection - Security Team

Steel Door Data

Dear Alex,

Thank you for reporting the issue with the email and attachment you received. After investigating, we've confirmed that the attachment you opened contained malicious software. This file attempted to run harmful commands on your computer, which could have allowed attackers to gain further access to our network.

While the issue was contained and no additional damage occurred, opening unverified email attachments poses a significant risk to the company. It could lead to the compromise of sensitive business information, loss of customer trust, and even legal repercussions. Such actions could also result in formal corrective measures if repeated.

What You Should Do Moving Forward:

1. Never open email attachments from unknown or untrusted senders, especially if the email seems urgent or suspicious.
2. Verify the legitimacy of emails with the IT team before taking action.
3. Complete the attached training module to better identify potentially harmful emails and attachments.

To ensure there are no lingering risks, we will be reimaging your computer. This process will erase all files and settings and reinstall the operating system. Please back up any critical files you need immediately.

Your cooperation is essential to maintaining a secure working environment. If you have any questions about this process or need assistance, don't hesitate to reach out.

Best regards,

Luis Cruz
Steel Door Data Protection - Security Team