Steel Door Data

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	Email Phishing – Marianne's credentials breached
Severity	3 - Serious
Justification for severity rating	Since the email address and password have been compromised due to Marianne filling in the form and clicking the 'set new password' button it means that the attacker has access to the Marianne's credentials which would allow them to gain confidential information depending on what information can be accessed using the user's credentials. However, having Marianne's credentials could also lead to the hacker gaining access to higher authorisation later.
Impact	With Marianne being emotionally stress judging on the message in the ticket, this attack could lead to a psychological impact such as confidence in her ability to work and to make good decisions for fear of making a similar mistake. Another impact would be service disruptions and possibly financial loss due to the fact of being able to gain access to higher authentication.
Ticket transferred to Response Squad?	Yes.
Communication sent to user?	Yes.

Steel Door Data

2. Investigation details

Investigation steps taken:

Step 1: I used the MXToolbox to get the results for SPF, DKIM, and DMARC tests.

The status for the SPF and DKIM for the phishing attack passes however DMARC could not be found and the policy is not enabled which means it can lead to fraud and worsen email security. The X-Haraka-Karma score is -1 which means that the email can be associated with malicious emails. In the 'the login.phph script', I noticed the variable $txt contained the word "Phished credentials" and for the mail header analyser it has provided 'DKIM-Signature Body Hash Not Verified' meaning the body of the email was altered which is a sign of a man in the middle attack.

Step 2: I looked at the email for any suspicious messages in the header and body. I notice that in the attachments for 'Phishing Email screenshot 1 and 2' there is no recipient in the email just the word 'Dear'. This will help In learning what to watch out for when it comes to receiving a malicious email.

Step 3: By using all the information gathered about the phishing email it will help in conducting the appropriate solutions to fix the security breach and to implement security measures to minimise or stop this cyberattack from happening in the future.

Attack sequence:

Step 1: Creates a domain name by using domain spoofing that makes the fake website look similar to the real website.
Step 2: Design website to make it similar to the legitimate website.
Step 3: Find an employee's contact details such as email address to send a fake email saying to reset your password.
Step 4: Create and add a link to the body of the website to redirect the user to the fake website.
Step 5: Writing an email that in a way that sounds urgent and appears real to make it believable.
Step 6: Wait for employee to fill in user credentials and click 'set new password' to receive user credentials.

Steel Door Data

Recommended actions:

Doing an investigation to anything irregular in the system following the attack such as checking log files taking place on the system to know any strange activities that are happening right now and to act in real time. Also, looking at audit trails to know what actions have been taken right now. Once we know how far the attacker has gone since the attack took place, we can quickly stop the attacker from causing further damage. Based on my investigation, It is crucial to configure email security technologies, this will verify where emails have originated and automatically reject emails that have been spoofed. Finally, implement phishing-resistant authentication for all staff including the junior developer as a security measure so if a similar situation happens in the future the attacker will not be able to gain access to sensitive data even with the user's login credentials as they would still need to get pass the additional authentication factor such as a code sent to a mobile device.

Additional information:

It is important for Marianne as well as all staff in every department to be trained in knowing how to identify suspicious emails and websites to prevent this issue from happening again.

Steel Door Data

II. Investigation #2

1. Incident information

Ticket number	#385076
User name	Alex Treemist
User email	alex.treemist@steeldoordataprotection.net
Type of incident	Email Phishing – Alex's computer affected by Malware
Severity	4 - Critical
Justification for severity rating	Malware can cause a wide range of issues for Alex's computer such as viruses spreading to other files resulting in them getting damaged and cause serious harm to the computer's system and security. The malware could also spread to other networks. If the attacker gains access to Alex's credentials this could lead to gaining access to confidential information and since Alex is a senior manager this means gaining access to more privileges and using the credentials could lead to gaining even higher privileges such as director privileges.
Impact	For this kind of impact it would compromise the security of Alex's computer causing the attacker to cause harm to the computer and potentially steal sensitive information in the background but not just Alex's computer but other devices connected to the same network within the organisation resulting in serious service disruption and loss of personal information.
Pertinent details of incident	What I noticed in the 'Phishing email screenshot 2' is in addressing the recipient as 'Hi Mister or miss' and that in the body it has 'before we go to justice' which it make it sound not realistic making a possible phishing email. I also noticed on 'SIEM Data' attachment on the ticket that the eventdata.threat Name is 'Trojandownloader' this information helps acknowledge that type of malware that has been used. Also, on the 'Any.run and VirusTotalReports' attachment on the ticket the screenshots shows strange behaviour with in the invoice file. It is possible that the hacker could have used malicious code onto Microsoft via Power shell which caused the malware when Alex opened the invoice.
Ticket transferred to Response Squad?	Yes.

Communication sent to user?	Yes.

2. Investigation details

Investigation steps taken:

Step 1 : I opened the ‘the raw email’ in an editor to get the X-Haraka-Karma: score which is -2 this means that the email can be associated with malicious emails.

Step 2: Looked at the email to notice any unfamiliar tone used in the email.

Step 3: Run anti-virus software to have a better understanding of the malware such as ‘Microsoft Office executes commands via PowerShell or Cmd’ to know the appropriate measures to put in place to resolve the error messages.

Step 4: Provide solutions to put in place to fix the security breach happening now and provide security measure to minimise and stop the attack before it happens.

Attack sequence:

Step 1: Decide which type of malware to use depending on the objective of the attacker.

Step 2: Attach the malware ‘Invoice1122023.xls.7z’ in the email and send it to user.

Step 3: Create an urgent message to convince user to download the malware.

Step 4: Wait for user to download malware to cause service disruptions.

Step 5: Use user’s credentials to gain access to higher authentication levels and spread malware to other systems.

Steel Door Data

Recommended actions:

The first thing to do is to revoking access to accounts that might be compromised by the malware or the hacker can get into. Use sandboxing as a way to test running programs and systems in a safe environment without affecting the host system. This will also help in knowing more about the malware and what systems have been affected. Finally, make sure to have a backup of all employees data to recover data that has been lost or damaged and for the systems that are affected to use malware removal tools such as McAfee to help with removing the malware. We will also plan on doing a factory reset to delete everything from the computer including windows and then install everything on the computer.

Additional information:

It is important for Alex as well as all staff in every department to be trained in knowing how to identify suspicious emails with attachments to prevent this issue from happening again. Also, to be trained in malware so that they know the basics on how to mitigate the malware to reduce the impact until a permanent solution has been implemented.