Contribute to Digital Investigations and Incident Response

By Darius Richardson

Contents

- Describing the incidents one at a time, the type of incident, the severity, pertinent details and the attack sequence I identified.
- Describing the steps I took to investigate each incident.
- Describing the remediation actions I recommended. Explaining why I chose them and how I expect that they would aid in resolving the incidents.
- Explaining which incidents I chose to communicate and why.
- Explaining any other considerations I had when preparing my emails.

Ticket number: #488021

User name: Marianne Haut-Nîmes

Severity: 3 - Serious

Type of incident: Email Phishing

Marianne’s credentials breached

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.

Investigation

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 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.

Remediation 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.

Email to Marianne

Dear Marianne,

We understand that the situation is serious but please remain calm.

I have been working on the incident (with the help of the information provided to me from Fatima Osei) to get to the root cause of the incident. Chances are that the attacker has access to your login credentials which means that the cyber-attacker can gain unauthorised access to confidential information.

I would recommend you familiarise yourself with phishing attacks. I have contacted the Incident response team to recommend setting up an employee training programme in phishing attacks to prevent this situation from happening in the future. It is important to keep up to date with phishing attacks and to distinguish a real email from a malicious email.

By using the information that has been given to me to help investigate this further you will know whether the security measures I have suggested will be made in due course regarding phishing emails so to prevent this incident from happening again.

You should reset your password as soon as possible.

Jose from level 1 security team provided the most up-to-date legitimate link for you to reset your password.

Please copy and paste this hyperlink into your web browser:

https://accounts.steeldoordata-oc.com/passwordreset

Make sure to also delete the phishing email to prevent accidentally clicking on it.

Yours sincerely,

Darius Richardson
Junior analyst

Ticket number: #385076

User name: Alex Treemist

Severity: 4 - critical

Type of incident: Email Phishing Alex's computer affected by Malware

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.

Investigation

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.

Remediation 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.

Steel Door Data

Email to Alex

Dear Alex,

I have taken serious action on addressing the severity and impact of the incident as well as providing solutions and security measures to put in place to recover any potential data loss and prevent this situation from happening in the future.

The invoice that you downloaded is what caused the malware to affect your computer causing it to not work and possibly cause the malware to spread to other systems because of your callous action.

To inform you, we will do a factory reset to delete everything from the computer including windows and then install everything.

I also propose that an employee training programme is taking for all employees to identify what a malicious email looks like to prevent this from happening again.

Make sure to delete the email with the attachment to prevent accidentally clicking on it.

Yours sincerely,
Darius Richardson
Junior Analysis

Summary

Investigation #1: Email Phishing Incident

- User: Marianne Haut-Nîmes
- Incident Type: Email Phishing
- Severity: Serious (3)
- Impact: Compromised credentials led to emotional stress for the user and potential financial loss.

Key Findings:

- Phishing Mechanism: The attacker used domain spoofing and created a fake website resembling a legitimate one, tricking Marianne into entering her credentials.
- Email Analysis: SPF and DKIM passed, but DMARC was not enabled, indicating potential vulnerabilities. Suspicious email content (e.g., generic greetings) was noted.

Recommended Actions:

1. Immediate system investigation for irregularities.
2. Implement email security measures (SPF, DKIM, DMARC).
3. Train staff on identifying phishing emails.
4. Introduce multi-factor authentication for sensitive access.

Summary

Investigation #2: Malware Infection Incident

- User: Alex Treemist
- Incident Type: Email Phishing leading to Malware
- Severity: Critical (4)
- Impact: Malware risks damaging Alex's computer and spreading through the network, threatening sensitive information.

Key Findings:

- Malware Type: Identified as "Trojan downloader," potentially spread through a malicious attachment disguised as an invoice.
- Email Analysis: The email's tone raised suspicion, and malware was confirmed through virus detection tools.

Recommended Actions:

1. Revoke access to potentially compromised accounts.
2. Use sandboxing techniques to safely analyze malware.
3. Ensure data backups are available for recovery.
4. Train employees on recognizing malicious emails and handling malware incidents.

Any Questions