Phishing attacks

Incident Team:

Anas Khalil

Nour Omar

Abdelrahman Zaki

Mohamed Ibrahim

Ahmed Shawky

Mohamed Yousry

Ahmed Khaled

Fady Emad

Ali Ibrahim

Supervised by:

Ahmed Abu el7amd

Overview:

We should ask ourselves 1 question before any process we take in this case and that is:

Are you sure that email from "Ahmed for SOCR" is actually from "Ahmed for SOCR"?!!

About:

Cybercriminals frequently target businesses and individuals using emails that are crafted to appear as though they were sent by a reputable bank, government agency, or other entity. The sender of these emails requests that the recipients click on a link to a page where they can verify account details, personal information, etc.

Table of Contents

Description:

Phishing is a common cyber-attack where attackers attempt to trick individuals into revealing sensitive information by posing as a legitimate entity. In the context of Incident Response (IR) , handling phishing attacks typically involves the following steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

And let’s go to discover every step in IR about phishing

Incident Report

1.Preparation:

1.1 Policies

use policy (AUP) that employees and contractors sign when they join that serves the following:

- define terms like phishing, social engineering, vishing, ransomware
- Explain the risks phishing poses, such as business disruption, financial loss, legal penalties, and damage to reputation.
- Educate employees that phishing can come through email, social media, texts, phone calls, or even in-person scams.
- Provide clear steps on what to do if phishing is suspected.

1.2 Employee Training:

Regularly train all employees on how to identify phishing attempts, including common red flags and suspicious behaviors.

training content like the Phishing Analysis Module we provide would be vital to internal and external stakeholders to know how to detect and respond to phishing attacks

1.3 Communication Plan:

Have team members on call 24/7 to receive and respond to reports of incidents.

When an incident is reported, it should initiate a series of predefined actions, such as when to notify law enforcement, media, or other third parties.

Create a clear communication strategy to ensure all stakeholders are
Informed and can respond quickly in the event of a phishing incident.

1.4 Technical Controls:

Implement email filtering, anti-phishing tools, and multi-factor authentication to reduce the likelihood of phishing attacks being successful

Set up robust spam filters to automatically filter out suspicious emails that could be phishing attempts

Require multi-factor authentication to add an extra layer of security, making It harder for attackers to gain access even if they obtain login credentials.

1.5 Mock Phishing Attack

is a proactive way to see how well your team can recognize and respond to phishing attempts

Steps:

- Decide which employees or departments to include in the test
- Pick the type of phishing attack to simulate, such as fake emails or text messages that look like they come from someone trustworthy
- Create phishing messages that look convincing
- Send out the phishing emails or messages to your chosen group
- Watch how employees respond who clicks, who reports, and how quickly your security team reacts
- Record how many people clicked the link and how many reported it
- See how well your security team handled the situation
- Check how well your security team responded to the threat

2. Identification

2.1 Analyze the email Header and Authentication Records:

1. **Check the email header** to see if it comes from a reputable domain.
2. **Look for email spoofing such as , mismatched domain names of altered email address**
3. Look for **SPF (Sender Policy Framework) : verify the sending mail server is authorized from the domain administrators server**
4. **DKIM (DomainKeys Identified Mail)** : Adds a digital signature to emails, allowing recipients to verify that the email content has not been altered in transit and that it came from the claimed domain.
5. and **DMARC (Domain-based Message Authentication, Reporting & Conformance)** Builds on SPF and DKIM to provide policies for email authentication and reporting. It helps ensure that email authentication is properly enforced and reports on failures.

2.2 Inspect the email content :

1. look for red flags in the mail body such as : urgency and threats
2. Spelling and Grammer: as poor grammer and spelling mistakes may indicate for phishing
3. URLs and attachment and unexpected files as it may carry malicious data
4. so to solve this we can use : Microsoft email 365 as it contain ai model that can detect all this and prevent the

email from sending to the user if it think that the mail is malicious

2.3 conduct technical analysis:

1. **IP Address**:

   Verify the IP address in the email header. Use tools to check its reputation and perform a reverse DNS lookup to see if the domain matches the IP. This helps confirm if the email is sent from a legitimate server.

2. **WHOIS Lookup**:

Perform a WHOIS request for the domain to check its registration details. New or disposable domains and mismatched registrant information can be red flags.

3. **Impact Assessment**:

Determine who else received the email and if it was part of a phishing campaign or targeted attack.

Check if the recipient clicked on links, opened attachments, or if there's any sign of account compromise.

We can use proof print tool in this method

Review and Monitor user behavior :
user interaction : determine if the user try to open the link that will let malicious enter the network

behavior monitoring: check if there unusual from user account or traffic such login to the account through different places or increase in the traffic of the network

additional steps:

1. Remove the malicious email from the receptionist's inbox to prevent accidental interaction with the malicious content Report and respond: Report the phishing email attempt to phishing

3. containment

3.1 contain affected accounts

- change the infected device or user's credentials to prevent unauthorized access
- isolate the affected device
- block the sender's email, malicious URL, and Ip address at the firewall and proxy
- disconnect it from all the services or network in a Vlan for example to prevent infection spreading
- investigate to know more about the attack
- enhance security measures
- add more securing factors to avoid it happens again
- Instruct the affected user to not interact with the email
- Reset the credentials of all involved systems

3.2 block activity

- block malicious domains using DNS, firewalls, or proxies
- reduce access to critical services, systems, or data until investigation is complete
- Implement forensic hold or retain forensic copies of messages to investigate on them
- block the sender and similar emails to prevent any other users to interact with them
- Confirm endpoint protection (FIM, DLP, EDR, SOAR, etc.) is up-to-date and enabled on all systems
- Deploy a signatures to endpoint protection and network security tools based on result of investigation

4. Eradication

4.1 Thorough System Scan

- malware and virus scan across the network to identify and remove any malicious software that may have been downloaded during the phishing attack
- can achieve that using EDR and NTA tools

4.2 Patch Vulnerabilities

- patching unpatched systems, and tightening configurations
- tools like Nessus and Rapid7 can scan for vulnerabilities and ensure that systems are up to date

4.3 Rebuild Compromised Systems

- Go back to the last trustworthy backup if the system is deeply compromised.
- Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.

4.4 Isolate and Monitor Affected Accounts

- Temporarily isolate and monitor the accounts that were targeted or compromised during the phishing attack to prevent future unauthorized access.

4.5 Clean Up Email Filters and Rules

- Check for malicious email rules or filters that may have been created by the adversary to avoid future exploitation. like a backdoor.

4.6 One-click containment and remediation

- introduced in many XDRs' which is a solution that uses either pre-built playbooks or is AI driven to automate the eradication and the containment phase

4.7 IBM Resilient

- automates the patching of systems and resetting passwords automatically using AI and ML

5. Recovery

- Check on the integrity of the data and search for any malicious code or backdoor.
- If there is anything wrong with the original data, we need to check the integrity of the backup data and that there is no malicious code in it.
- Retrieve the backup to ensure that the data is correct and there are no unauthorized changes into it or any malicious code that can change into the data or make a backdoor to any other data
- Enforce password resets upon all the employees and that is to ensure that the affected employees specifically is now secured and well not cause any more harm to the company
- Implementing multi factor authentication to make sure that this will not happened again and if by any chances the attacker has the new password of any employee it won't make a difference.
- Intense monitoring to the traffic to ensure that there is no other phishing email sent and monitoring logs to ensure that there is no unauthorized changes happening and generally to see if there any weird or unusual

6. Lessons Learned

6.1 Educate and Train: Regularly educate users about recognizing phishing attempts and the importance of cybersecurity practices.

6.2 Be Cautious with Links and Attachments: Avoid clicking on suspicious links or downloading attachments from unknown sources.

6.3 Strengthen Email Security: Use advanced email security solutions that can filter out or flag potential phishing messages.

6.4 Verify Sources: Always verify the authenticity of emails, messages, or calls before taking any action or providing sensitive information.

6.5 Use Strong Authentication: Implement multi-factor authentication (MFA) to add an extra layer of security beyond just passwords.

6.6 Avoid Pop-Ups: One must avoid following random pop-ups thatadvertise games or enticing monetary rewards for clicking on them.Designed to dupe innocent users, these pop-ups are primarily used toinject malware into a target system or steal important credentials.