Phishing Incident Response Playbook

Redback Operations

Document Owner: Purple Team Last Modified By: Devika Sivakumar
Next Review Date: 17 June 2024 Last Modified on: 5 April 2024

Version	Modified By	Approver	Date	Changes made
1.0	Indiah Smith	Ben Stephens	17 December 2023	First draft
1.1	Pari	Joel Daniel	28 March 2024	Introduction, Attack types, Stakeholders
1.2	Devika Sivakumar	Joel Daniel	23 March 2024	Flow diagram
1.3	Priyanshu	Joel Daniel	28 March 2024	Incident Response Stages
1.4	Joel Daniel	Ben Stephens	2 April 2024	Removed DNS Spoofing and placed Terminology section last.
1.5	Joel Daniel	NA	5 April 2024	Grammatical modifications and update to vishing section
1.6	Devika Sivakumar	Joel Daniel	5 April 2024	Updated the flowchart with bolder letters and visible colours and given the usual starting symbol for the flowchart.
2.0	Joel Daniel	Ben Stephens	10 April 2024	Approved for publishing and company use.

Contents

1. Introduction

1.1 Overview

One of the most common, simple yet dangerous security threats that all types of companies now have to deal with are phishing emails. The confidentiality, integrity, and availability of vital assets and data are seriously jeopardised by these attacks. Organisations need to have a thorough and well-defined incident response policy in place to effectively counter this danger while adhering to the minimum actions and questions to be carried out as detailed in the Redback Operations Incident Response Policy.

1.2 Purpose

This playbook's main goal is to give organisation an organised, methodical strategy to identifying, stopping, and minimising the effects of phishing assaults. Its objectives are to help Computer Security Incident Response Team (CSIRT) teams avoid operational disruptions, secure sensitive data, respond quickly to phishing attacks, and preserve the organization's reputation. The playbook provides precise instructions and protocols for phishing attack preparation, detection, analysis, containment, eradication, discovery, and post-event actions. By adhering to the playbook's guidelines, an organisation can improve its incident response capabilities, quickly and effectively combat phishing threats, and solidify itself against changing cyberthreats in the modern digital landscape.

1.3 Attack Definition

The definition of phishing incidents is as follows: “Phishing is the deceptive activity of someone pretending to be a reputable organisation and sending emails, texts, or phone calls in an attempt to trick people into disclosing sensitive information including passwords, banking and credit card details, and personally identifiable information.” These fraudulent emails frequently include links to fake websites or harmful attachments that aim to infect the recipient's device with malware or steal personal information. Phishing attacks pose a serious risk to cybersecurity and data privacy because they utilise social engineering tactics to trick people.

1.4 Scope

The handling of phishing attacks is included in the scope of a phishing incident response playbook. It consists of post-event actions, coordination and communication, incident detection, response, and continuous improvement initiatives. The goal of the playbook is to assist CSIRT teams in efficiently identifying, evaluating, and countering phishing attacks while reducing the damage to the company's assets and operations. The playbook also intends to

help stakeholders communicate and work together during a phishing event. It is meant for use by everyone involved in phishing incident management.

2. Attack Types

The different types of phishing attacks include:

2.1 Email Phishing

This is the most common type of phishing attack, in which hackers send fraudulent emails to people or businesses pretending to be trustworthy organisations like banks, governments, or well-known corporations. Usually, these emails have harmful attachments or links that are meant to fool recipients into downloading malware or disclosing private information.

Signs of Email Phishing:

1. Requests for personal information: Reputable businesses will never send you an email requesting personal information.
2. Urgent issue: Exercise caution when you receive urgent notifications, such as failed payments or account breaches. To verify, visit the website/ call bank directly rather than clicking any links.
3. Shortened links: Be wary of condensed or shortened links since they could be hiding harmful URLs.
4. Fourth-party email addresses: Verify the integrity of the sender email address; scammers frequently use aliases or other versions of reputable domains.
5. Spelling and grammar issues: Any email that has misspellings or grammar faults should be taken seriously as it may be a sign of phishing.
6. File attachments: Stay away from opening attachments unless they have been confirmed, especially if they have the.exe,.zip, or .scr extensions.
7. Sigle or blank image: Emails with just an image or one blank picture should be avoided since they can include malware that starts downloading automatically.

2.2 Spear Phishing

Spear phishing consists of extremely focused attacks directed at particular people or departments within a company. To create phishing emails that are more likely to be successful, attackers perform in-depth research to obtain personal information about their targets.

Signs of Spear Phishing:

1. Unusual requests: To prevent possible scams, confirm through a different channel if coworkers ask for credentials beyond the scope of their position.

2. Shared drive links: Stay away from accessing links that appear to be from internal sources since you probably already have access to shared drives.
3. Unsolicited emails: Be wary of emails offering unsolicited downloads; always verify the sender's authenticity.
4. Personal information: Email scammers may utilise needless personal information to win your trust, so be cautious when responding to such mail.

2.3 Whaling

Whaling attacks, sometimes referred to as CEO fraud, targets high-profile individuals in an organisation, such as CEOs or senior managers, with the intention of committing financial fraud or stealing confidential data. These attacks may spoof reliable connections or business partners and frequently entail advanced social engineering techniques.

Signs of Whaling:

1. Inaccurate domain address: To trick people, scammers frequently utilise identical but false domain domains. While checking email addresses, exercise caution.
2. Use of personal email: To reduce the danger of phishing, only use professional emails to communicate with executives or business partners. Verify the sender's identification over an offline channel if the request occurs from a personal email.
3. Requests for new contacts: Be wary of emails from vendors or partners you are not familiar with. Check these messages via proper channels or get in touch with the person in charge directly.

2.4 Vishing (Voice Phishing)

This utilises voicemails or phone calls to trick people into divulging private information or carrying out specific tasks, such sending money or exposing up vulnerable networks. Attackers may pretend to be legitimate by using methods like caller ID spoofing.

Signs of Vishing:

1. Blocked or unidentified numbers: Phishing calls often originate from blocked numbers. If a caller sounds suspicious, hang up immediately.
2. Requests for sensitive information or money: Various entities such as Government organizations, Medicare centres and Financial institutions conduct business through official mail and never request personal information over phone calls.

2.5 Smishing (SMS Phishing)

Text messages, or SMS (Short Message Service), are used in smishing attacks to deceive targets into clicking on harmful links or compromising personal information. These messages, which frequently appear to be from reliable sources like banks or government organisations, may advise recipients to act immediately to prevent repercussions.

Signs of Smishing:

1. Unsolicited texts: Watch out for texts that provide you discounts or freebies on something you didn't sign up for. Phishing texts may also ask for personal information or account verification.
2. Unknown numbers: Exercise vigilance while sending information requests by text. For verification, use a free phone lookup service; stay away from links and other interactions.
3. Authentication requests: Requests for authentication that are not authorised can be signs of attempted account access. To protect your account, quickly change your password.

2.6 Clone Phishing

Clone phishing is the practice of copying and pasting authentic emails or messages, making little changes (like changing links or attachments), and then delivering them to targets pretending they were the original correspondence. This strategy tries to fool recipients into interacting with the malicious content by taking advantage of their familiarity with the original sender.

Signs of Clone Phishing:

1. Duplicate emails: Look for copies of emails and closely examine newly added links for any indications of phishing. Always cross-reference connections with earlier correspondence.
2. Misspelt email addresses: Small typos are a common feature of bogus emails, which are sometimes overlooked.
3. Text with hyperlinks: Hover your cursor over links to see the actual URL. Should it diverge from the text that is linked, it can be a sign of phishing.

2.7 Angler Phishing

Attackers that use social media to conduct angler phishing pose as customer service agents. They make up profiles and message unhappy persons they come across in posts or comments on social media. Once the fraudster has confirmed a few personal data, they offer help and a URL that claims to fix the problem. But the URL is infected with malware, which makes it possible to successfully exploit the victim.

Signs of Angler Phishing:

1. Unverified account: Official support pages are usually verified and linked directly to the main page. Check the company website for official support contacts.
2. Minimal profile history: Smaller businesses, though unverified, should have a history of customer interactions. New accounts with few followers and no posts are likely attempting to deceive unsuspecting users.

2.8 Evil twin phishing

Evil twin phishing involves creating a fraudulent Wi-Fi network that mimics a legitimate one, tricking users into connecting to it. Once connected, attackers can intercept sensitive information or deploy malware.

Signs of Evil twin phishing:

1. Duplicate Wi-Fi hotspots: If you see multiple Wi-Fi networks with the same name, connect only to the secured one requiring a password from the establishment. Connecting to unsecured networks is strongly discouraged for safety.
2. Unsecure warnings: If your device warns that a network is unsecured, consider connecting to a secure network or refrain from connecting altogether.

3. Stakeholders

To minimise the impact on the organisation and prevent further events, early and efficient reaction to a phishing attack depends on strong coordination and collaboration amongst key stakeholders. Responding to a phishing attack usually involves the following key stakeholders:

IT Security Team: The IT Security Team oversees identifying, researching, and preventing phishing attacks. They take the lead in technical response tasks such as phishing email analysis, malicious website blocking, and security breach containment.

Incident Response Team: They are responsible for coordinating responses to the phishing issue, which includes interacting with relevant parties, putting incident response protocols into action, and doing post-incident analysis to avert similar attacks in the future.

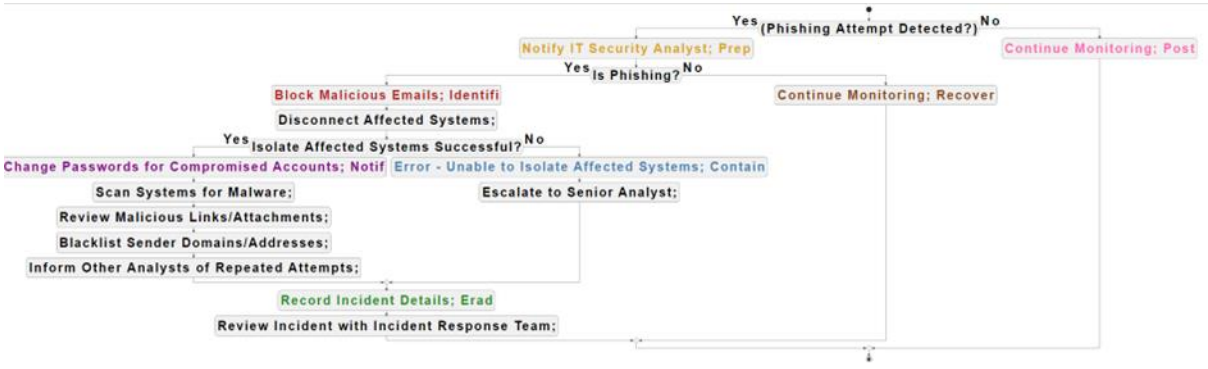
Communications Team: Oversees all internal and external communications regarding the phishing incident, including informing staff members, clients, and other relevant parties and giving them updates on the response activities.

Customers: They are the primary targets of phishing assaults and suffer damage instantaneously. This comprises:

- Customers whose financial and personal information might be lost.
- Businesses and educational institutions are among the organisations that experience financial losses, reputational harm, and data breaches.
- Banks and other financial institutions that experience fraudulent transactions and a decline in client confidence.
- Online retailers who may encounter fraudulent transactions and a decline in customer trust.

Third-party Vendors: Third-party vendors, like cybersecurity companies or incident response consultants, may be enlisted to offer specific knowledge and assistance during the response process, based upon the attack's nature and the structure of the organisation.

4. Flow Diagram



1. Preparation (Prep): Yellow

- Notify IT Security Analyst- The first thing to do is to alert the assigned IT security analyst as soon as you suspect a phishing attempt. To start the incident response procedure as soon as possible, the analyst must be notified. Important information including the threat's nature, the systems that are impacted, and any preliminary findings or proof are all included in this warning.

2. Identification (Identify): Red

- Block Malicious Emails: As soon as the phishing attempt is verified, all incoming emails that are suspected of being fraudulent should be blocked. By taking this preventive step, users are protected from possible danger and more intrusion into the company's systems are prevented.

- Disconnect Affected Systems: Meanwhile, all suspected or verified hacked systems are unplugged from the network. The goal of this isolation phase is to reduce possible harm to other systems or data while containing the danger and preventing its spread.

3. Notification (Notif): Violet

- Change Passwords for Compromised Accounts: Passwords for hacked user accounts are quickly changed as part of incident response to stop unwanted access. This preventive action reduces the possibility that malicious individuals will continue to abuse the situation.

- Scan Systems for Malware: The impacted computers are thoroughly scanned to find and eliminate any malware or harmful files. Through this scanning procedure, the systems' integrity is guaranteed, and any potential threats are stopped in their tracks.

- Review Malicious Links/Attachments: All attachments and URLs that might be connected to the phishing effort are carefully examined. This research provides light on the attackers' methodology and motivations in addition to helping to identify the strategies they employ.

- Blacklist Sender Domains/Addresses: Email addresses and sender domains connected to the phishing effort are blocked. Companies can actively fight against future attacks and protect customers from similar hazards by limiting communication from these sources.

- Inform Other Analysts of Repeated Attempts: Other security analysts are informed about the phishing effort, including attack tactics and indications of compromise (IOCs). This cooperative strategy strengthens protections against recurring threats and improves situational awareness.

4. Containment (Contain): Sky Blue

- Error - Unable to Isolate Affected Systems: If isolating the compromised systems doesn't resolve the issue, a senior analyst is notified so they may investigate it more and take appropriate action. By taking this action, you may be confident that the right steps are done to limit the problem and stop it from getting worse.

- Escalate to Senior Analyst: To help in reaching a well-informed decision, the senior analyst is briefed on the circumstances and given relevant details. By elevating the issue, you can make sure that it gets the focus and resources it needs to be handled successfully.

5. Eradication (Erad): Light Green

- Record Incident Details: Carefully documented are all the specifics of the happening, such as the timing, effects, and reaction activities. For post-event analysis, legal compliance, and future incident response planning, this material is an invaluable resource.

- Review Incident with Incident Response Team: Together with the incident response team, a thorough analysis of the occurrence is carried out. The objectives of this post-event study are to identify areas for incident response method improvement, security control gaps, and lessons learned.

6. Recovery (Recover): Brown

- Continue Monitoring: Ongoing monitoring operations are restarted following the mitigation of the immediate threat and the incident. This entails keeping an eye on user activities, system records, and network traffic to spot any remaining dangers or illegal access.

7. Post-Incident Actions (Post): Light pink

- Continue Monitoring: Even after the issue has been resolved, ongoing surveillance is still necessary to identify any reappearance of the danger or any fresh security flaws. To improve future issue handling skills, post-event steps should also involve a complete examination of incident response protocols and the implementation of any necessary enhancements.

5. Incident Response Stages

5.1 Preparation

- Create and record an incident response plan that outlines the steps, people involved, and their roles.
- Create an incident response team with responsibilities and escalation protocols well established.
- To find possible risks and weaknesses, do routine risk assessments.
- Install security measures including antivirus programmes, firewalls, and intrusion detection systems.
- Make and keep backups of important information and systems.
- Employees should get education and awareness campaigns to help them identify and report security problems.
- Create lines of communication and contact details for reporting and coordinating incidents.

5.2 Detection

- Use technology and monitoring tools to keep an eye out for any unusual behaviour, malware infestations, or illegal access.
- Keep an eye out for any indications of possible security breaches in system logs, network traffic, and security warnings.
- Correlate and analyse security events with the use of intrusion detection systems (IDS) and security information and event management (SIEM) solutions.
- Establish alerts and notifications so that security incidents may be quickly detected and addressed.
- To proactively find vulnerabilities and misconfigurations, conduct routine security audits and scans.

5.3 Analysis

- Examine security events to ascertain their type, extent, and effect on the company.

- Gather and examine supporting documentation, such as system snapshots, network traffic samples, and logs.
- Determine the attackers' tactics, methods, and procedures (TTPs) and indications of compromise (IOCs).
- Work along with pertinent parties, including as IT departments, legal advisors, and law enforcement, if needed.
- Keep a chain of custody for the evidence gathered during the enquiry and record the results.

5.4 Containment

- Act quickly to control the situation, stop more harm from occurring, and stop illegal access.
- To prevent malware or breach from spreading, isolate the compromised systems or networks from the rest of the infrastructure.
- Turn off hacked user accounts or services to stop hackers from getting private data.
- In order to lessen the effect of the event while the investigation and cleanup are ongoing, implement interim remedies or workarounds.
- Share information about containment efforts and anticipated downtime with all pertinent parties, including management and impacted parties.

5.5 Eradication

- Determine which impacted systems have malicious software or illegal access, then delete it.
- Fix any security flaws and vulnerabilities that were used during the incident.
- Perform thorough audits and scans to make sure that all signs of compromise have been removed.
- To make sure the impacted systems and data are clear of malicious malware and unauthorised alterations, restore them from clean backups.

- To avoid reoccurring instances, update firewall rules, antivirus signatures, and other security measures.

5.6 Recovery

- As soon as feasible, return all services and operations to normal while maintaining the security and integrity of all data and systems.
- To ensure their security and operation, test the restored systems and apps.
- Inform all relevant parties—staff, clients, and partners, for example—about the progress of the healing process and any lingering effects.
- To find opportunities for process and procedure improvement in incident response, conduct post-event evaluations and identify lessons learned.
- Based on the lessons learned from the occurrence, update incident response plans, policies, and training materials.

5.7 Post- Incident Review

- Keep a record of the incident response procedure, including deadlines, steps done, and results.
- Examine how well response activities worked and note any inadequacies or holes in incident response protocols.
- Have a lessons learned meeting with the incident response team and any pertinent parties to go over accomplishments, difficulties, and areas that may use improvement.
- Based on the results of the post-event evaluation, update the incident response paperwork, including the plans, processes, and contact lists.
- To strengthen the organization's overall security posture, share your observations and suggestions with upper management.

6. Terminology

- intrusion detection system (IDS): An intrusion detection system (IDS) is a security instrument that keeps an eye on system or network activity for any illegal activity or policy infractions.

- Security Information and Event Management (SIEM): A solution called Security Information and Event Management (SIEM) offers in-the-moment security alarm analysis from network hardware and application sources.

- Vulnerability assessment: Vulnerability assessment is the procedure for locating, measuring, and ranking security holes in a system.

- Threat Intelligence: Information concerning possible or existing dangers to the security infrastructure of an organisation is known as threat intelligence.

- Zero-day vulnerabilities: Zero-day vulnerabilities are security holes in hardware or software that are not known to the developer or vendor, leaving attackers free to take advantage of them before a patch or remedy is made available.