SOC Phishing Alert Triage & Escalation Report

Incident Type: Phishing with Malicious Attachment

1. Introduction

This report documents the investigation and response to a phishing alert involving a malicious email attachment within a financial services environment. The purpose of this investigation was to evaluate the alert, determine the legitimacy and severity of the threat, and follow the organization's phishing incident response playbook to decide whether the alert should be escalated or closed. The analysis focuses on alert triage, threat validation, and professional ticket handling consistent with Tier 1 SOC responsibilities.

2. Alert Overview

A phishing alert was generated after an employee received an email suspected of delivering malware. The alert was classified as **medium severity**, indicating a potential security threat that required investigation but not immediate emergency response. Initial alert details suggested the employee may have opened an email attachment, raising concern for possible malware execution on the endpoint.

The alert ticket identified a known malicious file hash associated with the attachment, prompting further investigation to confirm the nature of the threat and determine the appropriate response.

3. Alert Evaluation

Upon reviewing the alert details, several indicators suggested the email was malicious. The sender information appeared inconsistent and suspicious, including an untrusted sender domain and an IP address unrelated to the purported organization. The subject line and message body were generic and aligned with common phishing tactics designed to appear legitimate while encouraging the recipient to open an attachment.

Most notably, the email contained an **executable file attachment (bfsvc.exe)**, which is unusual and high-risk in typical business communication. The presence of an executable attachment alone warranted further analysis, as executable files are commonly used to deliver malware payloads in phishing campaigns.

4. Artifact Confirmation

The alert ticket included the SHA256 hash of the attached file. This hash had already been verified as malicious through threat intelligence analysis. Hash-based verification is a standard SOC practice used to confirm whether a file is associated with known malware without directly opening or executing the file.

Because the attachment's hash had been confirmed malicious, the investigation did not require additional file execution or sandboxing at this stage. The presence of a known malicious hash significantly increased confidence that the phishing alert represented a real security incident rather than a false positive.

5. Playbook-Guided Investigation

Following the organization's phishing incident response playbook, the investigation proceeded through the required evaluation steps. The email was confirmed to contain an attachment, and the attachment was verified as malicious through threat intelligence. According to playbook guidance, phishing alerts involving confirmed malicious attachments meet the criteria for escalation to higher tier analysts.

The playbook emphasizes timely escalation in cases where malware delivery is confirmed, as delayed response increases the risk of endpoint compromise, persistence, or lateral movement within the environment.

6. Escalation Decision

Decision: Escalated

Based on the confirmed presence of a malicious executable attachment and the likelihood that the user interacted with the file, closing the alert was not appropriate. The risk of endpoint compromise required escalation to ensure proper containment, remediation, and further investigation by a Level 2 SOC analyst or incident response team.

The escalation decision aligned fully with the organization's phishing response procedures and SOC best practices.

7. Ticket Documentation

The alert ticket was updated to reflect the investigation findings and escalation rationale. Clear and concise documentation was provided to ensure downstream analysts could quickly understand the nature of the threat and actions already taken.

Final Ticket Comment:

> Investigation confirmed the phishing email contained a malicious executable attachment (bfsvc.exe). The attachment's SHA256 hash was verified as malicious using threat intelligence, and the user likely executed the file based on alert details. Due to confirmed malware delivery and risk of endpoint compromise, the ticket has been escalated for further containment and remediation.

8. Impact Assessment

The confirmed delivery of a malicious executable attachment posed a significant risk to the affected endpoint and the broader organization. If executed, the malware could enable persistence, unauthorized access, or additional payload delivery. Prompt escalation was necessary to limit potential impact and allow for endpoint isolation, forensic analysis, and remediation.

9. Analyst Assessment

This incident demonstrates a common phishing technique in which attackers use seemingly legitimate job-related emails to trick recipients into opening malicious attachments. The use of a known malicious file hash allowed for rapid validation of the threat, reducing investigation time and enabling decisive action. The case highlights the importance of playbook-driven response and accurate ticket documentation in SOC operations.

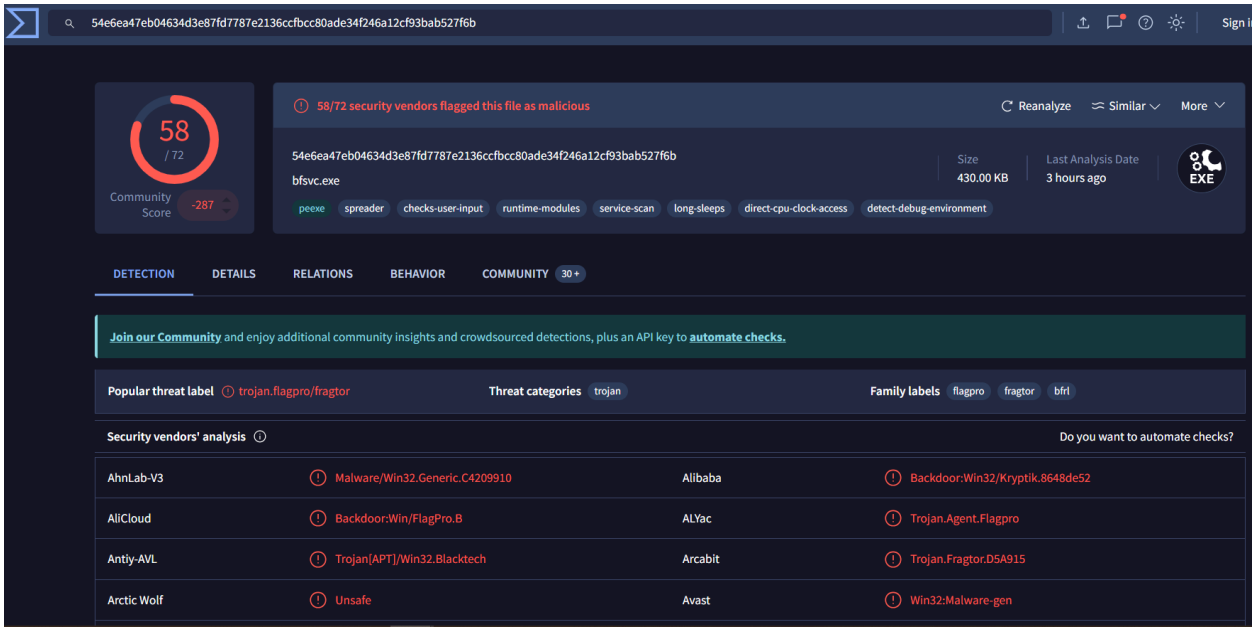
10. Conclusion

This investigation confirmed that the phishing alert represented a legitimate security incident involving a malicious attachment. By following established SOC procedures

and the phishing incident response playbook, the alert was properly evaluated, validated, and escalated. This case reflects real-world Tier 1 SOC responsibilities, including alert triage, threat validation, escalation decision-making, and professional documentation.

Appendix

VirusTotal detection summary screenshot
(Attached as supporting evidence)



Prepared by: Sambou Kamissoko
LinkedIn: https://www.linkedin.com/in/sambouk/