Playbook Response: Phishing Incident

Date and Time

November 14, 2023, 09:30:14

Incident Description

Phishing attempt detected on an employee's computer, involving a suspicious email attachment (bfsvc.exe) with a verified malicious hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b).

Email

From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Tuesday, November 14, 2023, 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,
Clyde West

Attachment: filename="bfsvc.exe"

Investigation Steps

- Alert Severity: The alert severity is classified as Medium, indicating a potential need for escalation.
- Sender Details: The sender's email address is suspicious and not aligned with the purported sender's name ("Def Communications" from <76tguyhh6tgftrt7tg.su>). This inconsistency raises concerns about the legitimacy of the email.
- Message Body: The message body contains grammatical errors, a common characteristic of phishing attempts. The email claims to be expressing interest in an "engineer role" and includes a password-protected attachment, a red flag for phishing.
- Attachments or Links: The attachment, named "bfsvc.exe," is flagged as malicious based on its hash value. This aligns with the initial phishing alert, indicating potential malware.

5 W's Analysis

- Who: The employee who received the email and potentially interacted with the malicious attachment.
- What: A phishing attempt involving a malicious email attachment (bfsvc.exe).
- When: The email was sent on Wednesday, July 20, 2022, at 09:30:14 AM.
- Where: The incident occurred on the employee's computer.
- Why: The attacker aims to compromise the employee's system, possibly for unauthorized access or to deliver malware.

Final Update to Alert Ticket

Ticket ID	Alert Message	Severity	Details	Ticket Status
A-2703	Phishing attempt possible download of malware.	Medium	User may have opened a malicious email and opened attachments or clicked links.	Escalated
Ticket Comments				
• Malicious attachment "bfsvc.exe" confirmed on VirusTotal with hash value (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). • Suspicious sender details and grammatical errors in the message raise concerns. • Following playbook protocol, escalating to Level-two SOC for further investigation and action.				