Incident Final Report

Using a Playbook to Respond to a Pishing Incident

Wendy Alayon
27/07/2024 **@syszern**

Incident Final Report

Scenario

At a financial services company, a level-one security operations center (SOC) analyst has received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, it has been verified as malicious. Now that this information is known, the organization's process must be followed to complete the investigation and resolve the alert.

The organization's security policies and procedures describe how to respond to specific alerts, including what to do when a phishing alert is received.

In the playbook, there is a flowchart and written instructions to assist in completing the investigation and resolving the alert. At the end of the investigation, the alert ticket should be updated with findings about the incident.

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket comments

The alert identified that an employee had downloaded and opened a malicious file from a phishing email. Discrepancies were found between the sender's email address, "76tguy6hh6tgftrt7tg.su," the name used in the email body, "Clyde West," and the sender's name, "Def Communications." Additionally, the email contained grammatical errors in both the body and the subject line. The email also included a password-protected attachment, "bfsvc.exe," which was downloaded and opened on the affected machine. The file hash investigation confirmed it as a known malicious file. Given that the alert severity is classified as medium, the decision was made to escalate the ticket to a level-two SOC analyst for further action.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:

From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 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"