Ticket Analysis and Escalation

Completed by: Hope Tan (github.com/hope-tan)

Phishing incident response playbook

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
I am escalating this ticket to level-two SOC for the below reasons. 1. The receiver downloaded and opened the attached file on their machine. I verified that the executable attachment is malware. According to VirusTotal, this file's hash is associated with malware called Flagpro that has commonly been used in Trojan and phishing attacks. 2. The email has multiple reasons to raise suspicion: a. The sender's email address originates from outside the company and appears suspicious, as it is a random string of characters. b. The email name says Def Communications, while the email is signed off as Clyde West. c. There are grammatical errors throughout the email..

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"