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
1. After detecting an alert indicating that an employee had downloaded and opened a malicious file from a phishing email, several observations were made. Firstly, there was an inconsistency between the sender's email address, "76tguy6hh6tgftrt7tg.su," the name used in the email body, "Clyde West," and the sender's name, "Def Communications." This raised suspicions of potential impersonation or spoofing. Both the email body and subject line contained grammatical errors, which are red flags for phishing attempts. 2. The email included a password-protected attachment named "bfsvc.exe," which was successfully downloaded and opened on the affected machine. Prior investigation of the file hash confirmed that it is a malicious file. These combined indicators prompted a classification of medium severity for the alert. 3. Based on these findings, the decision was made to escalate the ticket to a level-two SOC analyst for further investigation and action. The ticket status was promptly updated to "Investigating," and a detailed analysis of the email from sender "Def Communications" to recipient "hr@inergy.com" was started.

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"