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
Our security alert system has detected that one of our employees downloaded and opened a malicious file from a phishing email. Upon closer examination, several inconsistencies were identified within the email itself. The sender's email address appeared as "76tguy6hh6tgftrt7tg.su," whereas the name used in the email body was "Clyde West," and the sender's name was listed as "Def Communications." Furthermore, the email displayed grammatical errors in both the body and subject line, raising additional concerns. Within the email, there was an attachment named "bfsvc.exe," which was found to be password-protected. Regrettably, the employee proceeded to open the attachment on their machine. Our prior investigation into the file hash has confirmed its status as a known malicious file. Given the severity of the alert, which has been classified as medium, I have made the decision to escalate this ticket to a level-two SOC analyst. They will assume responsibility for taking the necessary further actions to address this security incident promptly and effectively.

Additional information

Attachment: filename="bfsvc.exe"
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"