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
At 1:20 P.M., the SOC team was alerted on a possible phishing attempt by an outside threat actor. The ticket has been escalated to SOC Tier 2 because of two main indicators of compromise. Firstly, the attacker misspelled the word “Engineer” in the “Subject” line of the email, which is a normal sign of an email being illegitimate. Second, instead of the expected resume and cover letter in the “Attachment” line, he included an executable file which, when downloaded, triggers the delivery a malicious payload.

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"