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
On July 20, 2022 at 9:30:14 AM, an employee received an email from a threat actor posing as a person sending their resume in for a job position. Attached to the email is a file with the name “bfsvc.exe”. When clicked, a malicious file hash known as “54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b” downloaded onto the victim’s device. Straight off appearance, the email is suspicious. The email from the sender doesn’t match the name given at the bottom, there’s numerous spelling and grammar mistakes, the attached “resume” file is an execute file, the ip address seems fake also. This ticket is being escalated, the user was targeted by a phishing scam and may or may not have opened the file containing the malware. Severely levels ranked at Medium, should further investigate.

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"