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
This alert has been escalated appropriately. The file was deemed as malicious. After evaluating the alert using step 2 of the playbook, it was noted that the email came from a suspicious address. There was also a spelling mistake in the subject and grammar issue in the main body of text, furthering suspicions. Using step 3 of the playbook, the malicious attachment was also investigated. After acquiring the hash fingerprint, the service VirusTotal confirmed that this file was in fact malicious. It was an overall security vendor score of 61/73, with multiple community notes supporting this claim. This file was also tested in multiple sandbox environments, and the results also support this claim that the file is malicious. Because of this identified information, this has been escalated.

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"