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 is legit and the hash file has been flagged malicious by a number of security vendors. I have escalated the issue because of the following reasons: 1. The email address is inconsistent with the name that is signed at the bottom of the email; the email address is 76tguyhh6tgftrt7tg.su and the name of the author is Clyde West. 2. There are grammatical and spelling errors in the email; “I am writing for to express...”, “Infrastructure Egnieer role” 3. The contained a password protected file that infected the employee’s machine; "bfsvc.exe"

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"