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
An email was sent to an employee under the guise of a job application. A suspicious file was downloaded on an employee's computer, an executable under the filename "bfsvc.exe". 1. The alert is of medium severity and therefore may require escalation. 2. Receiver details - email : hr@inergy.com ip: 176.157.125.93 3. Sender details - email: 76tguyhh6tgftrt7tg.su ip: 114.114.114.114 4. Subject line: Infrastructure Egnieer role Comments - obscure sender email address and suffix - no identification, .su country code and spelling mistakes in subject line. 5. Message body contains grammatical and spelling errors. 6. Attachment containing supposed ‘resume’ and ‘cover letter’ - password protected with potential for malicious download. File is .exe which will execute, and is not a document format. The email demonstrated key indicators of phishing email, including spelling mistakes within subject line and the body of the text, the obscure email address and the file being .exe rather than a text format

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"