Alert ticket:

Ticket ID	Alert Message	Severity	Details	Ticket status
A-3123	SERVER-MAIL Phishing attempts possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	**Escalated**

Ticket comments
The alert revealed that an employee had downloaded and opened a malicious file from a phishing email. The sender's email address, "76tguy6hh6tgftrt7tg.su," did not match the name used in the email body, "Jordan Clark," or the displayed sender name, "Def Communications." Both the subject line and the email body contained noticeable grammatical errors. A password-protected attachment, "bfsvc.exe," was included in the email and subsequently downloaded and executed on the affected machine. Upon analyzing the file hash, it was confirmed to be linked to a known malicious file. Given the medium severity of the alert, I escalated the incident to a level-two SOC analyst for further investigation.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2024 11:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Engineer role

Dear HR at Hari Logistics LLC,

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,

Jordan Clark
Attachment: filename="bfsvc.exe"