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
Phishing email identified with malicious attachment: `bfsvc.exe`. File hash analysis confirms it is malicious. Sender address (`76tguyhh6tgftrt7tg.su`) does not match display name, indicating possible spoofing. Email contains grammatical errors and includes a password-protected attachment — both common phishing indicators. Employee opened the file at 1:13 p.m.; IDS flagged suspicious activity at 1:20 p.m. **Reasons for escalation:** 1. The file has been confirmed as malicious through hash analysis. 2. Suspicious activity was detected shortly after execution, indicating possible compromise. 3. Alert severity is Medium, which per playbook guidance may warrant further investigation by a Level 2 analyst.

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"