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 phishing alert involves a suspicious email containing a password-protected attachment that triggered a known malicious executable (`bfsvc.exe`) upon opening. The file hash has been verified as malicious via VirusTotal. The alert should be escalated for the following reasons: 1. The attachment (`bfsvc.exe`) matches a known malicious SHA256 hash: `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`. 2. The sender email (`76tguyhh6tgftrt7tg.su`) and IP address (114.114.114.114) appear suspicious and do not match the legitimate sender they are impersonating. 3. The email contains grammar issues and impersonates a job applicant in a format commonly used in targeted phishing campaigns.

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"