Maria Audu

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.	Closed

Ticket comments
The phishing alert was triggered by an email containing a malicious executable attachment (bfsvc.exe). The attachment's SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) was verified as malicious through threat intelligence sources. Email security controls successfully **quarantined the attachment prior to execution**. Review of email, endpoint, and user activity logs confirmed **no user interaction**, **no file execution**, and **no system or registry changes**. The sender's domain and email content exhibited clear phishing indicators, including impersonation and social engineering tactics. **Resolution:** The threat was fully contained with no impact to the user or corporate environment. No escalation or remediation actions were required. The ticket is closed as **Phishing – Malicious Attachment (Blocked / No Impact)**.

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"