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
Considering all the issues in this email, the ticket status should be changed to 'Escalated'. The reasons can be seen in the journal entry at the bottom of this document.

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"

Incident handler's report - inergy

Date: Record the date of the journal entry.	**Entry: #3** 07.04.24
Description	A report about Flagpro attack on inergy
Tool(s) used	Attack: Spear phishing, Flagpro. Detect and analyze: Virus Total, IDS, EDR
The 5 W's	Capture the 5 W's of an incident. • Who? - An untrained employee at inergy, and BlackTech (Threat Actor) • What? - A user opened a spear phishing email with a malicious file that was opened. • When? - Wednesday, July 20, 2022 09:30:14 AM • Where? - HR department at inergy • Why? - An untrained employee was spear-phished to open a malicious file. A Threat Actor named BlackTech aimed to steal technology from Inergy for financial gain or cyber espionage. inergy is a solar panel power company, which may be related to a Chinese need to gain an unfair advantage in this market.
Additional notes	1. The email contained a malicious file that was opened. 2. Any part of the email that raised my suspicion is marked with Orange. 3. Please notice that Def Communications isn't a real company. 4. This Ticket should be escalated further, due to: a. A malicious file appearing in the email and being opened. b. Grammar errors appear several times in the email. c. A generic name is being used: 'Clyde West'.

	5. Cyber training should occur on a regular basis.