

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
<p>The alert detected that an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender's email address, "76tguy6hh6tgrt7tg.su," the name used in the email body, "Clyde West," and the sender's name, "Def Communications." The email's body and subject line contained grammatical errors and a password-protected attachment, "bfsvc.exe," which was downloaded and executed on the affected machine. Upon investigating the file hash, it was confirmed to be a known malicious file.</p> <p>Additionally, the alert severity is reported as medium. Considering the severity level, the grammatical errors in the email body, and the presence of the malicious attachment, I have escalated this ticket to a level-two SOC analyst for further action.</p>

## Additional information

### Known malicious file hash:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

### Email:

From: Def Communications <76tguyhh6tgfrt7tg.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 Inergy,

I am **writing 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"