

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.	Investigating

Ticket comments
<p>On July 20, 2022, a phishing alert was generated after an employee received an email containing a suspicious executable attachment. The attachment (bfsvc.exe) was identified as malicious based on its SHA256 hash, indicating a malware delivery attempt.</p> <p>Investigation and Disposition Rationale:</p> <p>The sender's email address and domain do not align with legitimate business communications and appear to impersonate a job applicant, which is consistent with phishing behavior. The email content contains grammatical errors and attempts to entice the recipient to open a password-protected executable file, a common phishing tactic. Although the attachment hash is confirmed malicious, security controls quarantined the file, and log analysis shows no evidence of user interaction, execution, or system changes; therefore, escalation is not required at this time.</p>

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 Inergy,

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"