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
After reviewing the phishing alert, we confirmed that the attached file "bfsvc.exe" from the email titled "Re: Infrastructure Engineer role" is malicious. We checked the file's hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) on VirusTotal, where more than 50 security vendors marked it as dangerous. It also has a very low community score (-243), showing strong agreement that it's harmful. The email came from a suspicious domain and IP address (76tguyhh6tgftrt7tg.su, IP: 114.114.114.114) and was sent to our HR inbox. The message used social engineering tricks and included a password-protected executable file — a common method used to avoid email security filters. Based on the steps in the phishing playbook, this alert qualifies for escalation because malware has been confirmed and there could be an impact to users.

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"