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
An alert ticket, A-2703, has been generated with the message, “SERVER-MAIL Phishing attempt possible download of malware” and an alert severity of medium. The HR department received an email with the subject “Re: Infrastructure Egnieer Role” from an email account by the name of “Def Communications”, email address “76tguyhh6tgftrt7tg.su”, and IP address “114.114.114.114”. The contents of the email express interest in the engineer role posted online signed by “Clyde West”. The attachment provided in the email is said to be a resume and cover letter and to be password protected. The password is provided in the email and the filename is “bfsvc.exe”. In the email subject, there is a grammatical error, the name of sender does not match email address, and the email address is unusual. The filetype is also an executable with uncommon naming conventions. Having previously investigated the hash file for the downloaded file (see Entry #2), I have confirmed this is a malicious file. I have changed the status of this ticket to “Escalated” for further action by SOC analyst level II.

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"