Benjamin Taylor – Google Cybersecurity

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
The alert detected that an employee downloaded then opened a malicious file, sourced from a phishing email. There is an inconsistency between the sender's email address (which is "76tguyhh6tgftrt7tg.su"), the name that is used in the body "Clyde West", and the sender's name, "Def Communications". The email body and subject line contain grammatical errors as well. There is also a password-protected attachment in the email body, "bfsvc.exe," which was the file downloaded and opened on the affected machine. This is now known to be a malicious file after investigating the file hash. The alert severity is reported as medium, as well. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.

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"