

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

Following the Phishing Incident Response Playbook, the email was evaluated and it was confirmed that it was a phishing email as the sending address is suspicious, the body has grammar errors, and there is an attached file.

Next, the file needs evaluating to see if the attached file is suspicious. Using the VirusTotal tool, the hash value of the attachment was put into the tool's search function. The results were that the attachment was malicious as seen in the following attachment:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

58/71 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size: 430.00 KB | Last Analysis Date: 36 minutes ago

peexe service-scan runtime-modules spreader long-sleeps direct-cpu-clock-access checks-user-input detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan:flagpro/fragtor Threat categories trojan Family labels flagpro fragtor bfri

Security vendors' analysis

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Kryptik.8648de52
AllCloud	Backdoor:Win/FlagPro.B	ALYac	Trojan.Agent.Flagpro
Antiy-AVL	Trojan(APT)/Win32.Blacktech	Arcabit	Trojan.Fragtor.D5A915
Arctic Wolf	Unsafe	Avast	Win32-Malware-gen
AVG	Win32-Malware-gen	Avira-Cloud	Win32:Malware-gen

Link for further investigation: [VirusTotal - File - 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b](https://www.virustotal.com/file/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/analysis/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/)

Based on the phishing incident response playbook, this ticket is to be escalated to the level-two SOC analyst. Thanks!

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"