Incident handler's journal

Incident Summary

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

SHA256 file hash:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

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

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 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"

Date:	**Entry:**
Record the date of the journal entry.	July 20, 2022
Description	An employee received a phishing email containing a malicious attachment. Upon downloading and opening the file, multiple unauthorized executable files were created on the employee's workstation. The IDS detected this activity and generated an alert to the SOC.
Tool(s) used	IDS, VirusTotal (for hash analysis), SOC alert system (for detection & triage)
Alert Investigation Log (as per playbook)	**Alert severity:** Medium (May require escalation) **Receiver details:** The receiver's email & ip address <hr@inergy.com> <176.157.125.93> **Sender details:** The sender's email address & IP address: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> **Subject line:**

	Re: Infrastructure Egnieer role **Message body:** Dear HR at Ingergy, I am writing 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 **Attachments or links:** filename="bfsvc.exe"
Additional notes	The file was malicious and the IDS alert was a True Positive.

Reflections/Notes:
This case highlights the importance of **user awareness and email security training**. Quick detection via IDS prevented possible lateral movement or data exfiltration.