| Ticket ID | Alert Message | Severity | Details | Ticket status |
|---|---|---|---|---|
| A-2703 | SERVER-MAIL Phishing attempt possible download of malware | High | The user opened a malicious email and opened an attachment with which downloaded malicious codes in the employee's computer. | Escalated |

| Ticket comments |
|---|
| The employee received a malicious email containing an attachment from a threat actor. The attachment was downloaded which immediately ran the malicious code – prompting an indicator of compromise (IoC) alert at the SOC. The file's hash was checked on a VirusTotal, and it was discovered that it is a malicious file with severe damage capabilities. |

## 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"