| 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 |
|---|
| Phishing email containing a malicious executable file was sent to an employee. The email contains typical phishing indicators, including grammatical errors and an unfamiliar domain. The attachment's hash has been verified as malicious.<br><br>1. The sender's email domain **(76tguyhh6tgftrt7tg.su) is suspicious** and **does not** resemble any trusted business domains.<br>2. There's a mismatch between the sender name ("Def Communications") and the signature ("Clyde West"), which is a common phishing tactic.<br>3. The subject line contains a spelling error ("Egnieer" instead of "Engineer"), a well-known phishing red flag.<br>4. The email body contains multiple grammatical errors, such as **"Dear HR at Ingergy"** and **"I am writing for to express,"** which often indicate phishing.<br>5. The attachment is a **password-protected executable file (.exe)**, an uncommon practice for legitimate emails, and is often used to bypass security filters.<br>6. The file hash was **confirmed as malicious** using VirusTotal, flagging the attachment as a serious threat.<br><br>Escalated to Level-2 SOC Analyst |

## 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"