|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ticket ID** | **Alert Message** | **Severity** | **Details** | **Ticket status** |
| A-2703 | SERVER-MAIL Phishing attempt possible download of malware | Medium | O usuário pode ter aberto um e-mail malicioso e aberto anexos ou clicado em links. | Escalated |

|  |
| --- |
| **Ticket comments** |
| Recebemos um alerta de phishing indicando o possível download de malware através de um anexo malicioso. O e-mail, enviado por "Def Communications," apresenta características suspeitas, incluindo inconsistências entre o domínio do endereço de e-mail e o nome mencionado no corpo da mensagem, "Clyde West."  Além disso, o e-mail contém erros gramaticais e inclui um anexo protegido por senha chamado "bfsvc.exe," que foi baixado e aberto na máquina afetada. Após a análise do hash do arquivo, foi confirmado tratar-se de um malware conhecido como FlagPro.  Dado o nível médio de gravidade do alerta e as evidências coletadas, optei por escalar este tíquete para um analista SOC de nível dois para que ações adicionais possam ser tomadas. |

### **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 rol**e**

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"