Malicious Email Detection

Problem Statement

You have been assigned a medium-severity security alert regarding a possible phishing attempt. An employee has received a malicious email, downloaded a password-protected attachment, and opened the file. Your task is to apply the PASTA framework to analyze the incident, confirm the threat, and recommend the appropriate next steps to contain the security risk and prevent further compromise.

Brief PASTA Framework

The PASTA framework provides a structured approach for incident handlers to manage and respond to security incidents. The acronym stands for:

- **Problem:** Identify and define the core issue.
- **Analysis:** Investigate the incident and gather all relevant information.
- **Solution:** Determine the best course of action to mitigate the threat.
- **Threat Modeling:** Assess the type and severity of the threat.
- **Action:** Execute the planned solution and escalate as needed.

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
The alert detected that an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender's email address "76tguy6hh6tgftrt7tg.su'" the name used in the email body "Clyde West," and the sender's

name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. Having previously investigated the file hash, it is confirmed to be a known malicious file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.

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"