Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Scenario

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: 07/30/2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	Who caused the incident? ● A group of hackers What happened? ● Hackers installed ransomware When did the incident occur? ● Tuesday 9:00 a.m. Where did the incident happen? ● A Small U.S. Health Care Clinic Why did the incident happen? ● The hackers were able to access the company systems through a phishing attack. They then launched their ransomware attack to encrypt the critical files. Their motivation was likely financial as they were asking for a large sum of money to decrypt the files.
Additional notes	The company needs phishing training to help reduce the chances of this happening again. If backups are available then they should not pay the ransom as we cannot guarantee they will actually give the decryption key

Scenario

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

SHA256 file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a timeline of the events leading up to this alert:

- **1:11 p.m.:** An employee receives an email containing a file attachment.
- **1:13 p.m.:** The employee successfully downloads and opens the file.
- **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.
- **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC.

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
IAn alert flagged that an employee downloaded and opened a known malicious file, "bfsvc.exe," from a phishing email. The email had inconsistencies: the sender's address was "76tguy6hh6tgftrt7tg.su," but the name in the email was "Clyde West," and the sender's name was "Def Communications." The email also contained grammatical errors. Given these findings and the medium severity of the alert, I've escalated the ticket to a level-two SOC analyst for 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"

Date: 07/30/2024	**Entry:** #2
Description	Potential Malicious File Analysis.
Tool(s) used	VirusTotal Website

The 5 W's	Who caused the incident? ● A hacker that sent the email and the end user What happened? ● Hackers were able to get user to open the file which installed the virus When did the incident occur? ● Around 1:10pm Where did the incident happen? ● A financial services company Why did the incident happen? ● The hackers were able to access the company systems by having a user download and open a file spreadsheet file which then delivered the malicious payload and was executed on their computer.
Additional notes	The company needs phishing training to help reduce the chances of this happening again. They also need to implement rules for what executables can be run without admin user permissions.