Isaac Aylor
Google Certificate
Incident Handling

Incident handler's journal

Date: 07.09.2024	**Entry: Journal Entry #1**
Description	The Documentation of a Security Incident Suspected phishing attack spreads ransomware throughout a Healthcare Clinic. The current NIST stage is Eradication.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. ● A Healthcare targeting group of unethical hackers caused the event. ● Ransomware from a phishing email security incident ● Tuesday at 9:00am. ● A U.S. Healthcare Clinic ● Employees fell victim to a targeted phishing attack. After receiving socially engineered emails, employees opened and downloaded an attachment. Within the attachment, a malicious ransomware worm installed itself and spread to every other device on the network. The worms encrypted all stored data on infected devices, with a note left requesting a large sum of money for the encryption key. This ransomware has halted business operations.
Additional notes	● Training on phishing attacks and safe email practices could help prevent such attacks in the future. With IT notified, such risks can be evaluated and properly responded to. ● Does the company pay for the key? Or are there backups to default to?

Date: 7.22.2024	**Entry: Journal Entry #2**
Description	The Documentation of a Security Incident A false resume email was sent to the HR department, infecting the receiving station with a trojan. The current NIST stage is Detection and Analysis.
Tool(s) used	www.virustotal.com
The 5 W's	Capture the 5 W's of an incident. ● Threat actor 76tguyhh6tgftrt7tg.su (114.114.114.114), sent an email with a false resume attachment to hr@inergy.com (176.157.125.93) ● The employee in regards, downloaded the attached file ● 1:11pm the email was acquired, 1:13pm the file is successfully downloaded ● Financial Services Company, US ● The email sent appears to be a phishing attempt for a few reasons. Firstly, the organization and sender's email don't match (sender's email looks to be a proxy email). Secondly, the Subject Line and Body both contain a multitude of grammatical errors and misspelling. Finally utilizing VirusTotal, the file's hash was evaluated and found dangerous. It is a known malware named the Flagpro trojan.
Additional notes	● A 'verified files list' should be curated, blocking downloads of files not meeting approved hashes listed. ● Employees should be required to receive email and download training. ● Elevate this to a SOC 2 for containment and recovery

Below is the ticket from the security alert for the above entry

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
Threat actor 76tguyhh6tgftrt7tg.su (114.114.114.114), sent an email with a false resume attachment to hr@inergy.com (176.157.125.93) at 1:11pm. The organization (Def Communications) and sender's email don't match. The Subject Line and Body both contain a multitude of grammatical errors and misspelling (Egnieer, Ingergy, etc). The attachment bfsvc.exe contains a known malware named Flagpro, a trojan program. It demonstrates Evasion and Permission Elevation, the infected device should be elevated to a SOC II Analyst for further investigation.

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: 7.22.2024	**Entry: Journal Entry #3**
Description	The Documentation of the Final Report for a previous Security Incident Lack of sanitization allowed injection on an ecommerce site. This gave a threat actor access to PII that is now leveraged against the company. The current NIST stage is Containment.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. ● An anonymous threat actor ● The e-commerce site was breached and PII was extracted, payment was demanded 'as to not share the leaked data' ● December 22nd 3:13pm was the first ransom email, December 28th an increased Ransom was sent ● Mid-sized retail company, US ● Utilizing the purchase confirmation page, the actor enumerated the browser bar to execute injected code. This enabled the actor to navigate between thousands of order confirmation screens with PII. This data was collected, and then leveraged in an attempt of $25,000 and then an increased $50,000 'silence payment'.
Additional notes	● Are there other pages at risk of injection within the site? ● Is sanitization utilized for all points of text entry on the site? ● Is the ransom paid?

Date: 7.25.2024	**Entry: Journal Entry #4**
Description	The Documentation of Security Events Multiple employee stations visited a suspected phishing site, resulting in a successful phishing attack. The current NIST stage is Detection and Analysis.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● office365x24.com (40.100.174.34) is the suspected threat actor ● Multiple employee devices accessed the suspicious domain repeatedly ● January 31st 2023 to July 09th 2023 ● Financial Services Company ● Six employee stations initially visited the site 'office365x24.com' in January. This site's URL is meant to emulate an Office365-associated site but bears no credentials from Microsoft. Since then, each of the six devices has repeatedly visited the site in unison, and always outside business hours. During these visits, the logs capture unknown IPs `GET`ing data and utilize the `POST` command to the /login.php. IP Address 40.100.174.34 was the predominant resolved address with these requests, accessing /login.php across all affected devices. Focusing on this IP address, I highlighted two more additional machines affected that did not visit office365x24.com. The address is also associated with the URL signin.accounts-gooqle.com, another suspected phishing site. Utilizing VirusTotal, the site may have come back only as a 10/92, but major names like Kaspersky tagged it as 'malicious' or 'phishing'. The address, however, came back as a Severity HIGH from Virus Total.

Additional notes	- The devices acting together suggests they may be part of a botnet now - Suspected phishing site, but was something downloaded or did visiting the site somehow compromise devices? - Suggests successful phishing attack - Possible worm malware

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. - **Who** caused the incident? - **What** happened? - **When** did the incident occur? - **Where** did the incident happen? - **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?

   The final two entries challenged me to put to use my enumeration understanding. Utilizing Hack the Box, I've been enumerating machines to strengthen my attacker mindset. This gave me a unique understanding of the situations I was presented with, allowing me to show personal expertise.
2. Has your understanding of incident detection and response changed since taking this course?

   My understanding of Incident Detection has changed, via emphasizing the need for clear documentation. This allowed me to improve my concise writing style, and to better address the needs of security documentation.
3. Was there a specific tool or concept that you enjoyed the most? Why?

   The tool I relished utilizing the most, was Google's Chronicle. The direct links to TotalVirus, and ease of exploring logs made it easy to love.