Jasper Davis

Incident Handler's Journal

Date: Tuesday, 2023-06-20	**Entry:** 1
Description	U.S. Health Care Clinic - Ransomware Attack After Phishing
Tool(s) used	n/a
The 5 W's	On Tuesday morning at ~9:00 AM, employees of a U.S. healthcare clinic reported being unable to use their computers to access files. This lockout was accompanied by a ransom note demanding a large sum of money in exchange for the decryption key. This ransomware incident was perpetrated by a group of unethical hackers known for targeting organizations within the healthcare and transportation industries. This incident was enabled by a successful phishing attack that led to an employee unintentionally installing malware onto their company computer. This incident caused severe disruptions to business operations and necessitated reporting to outside organizations.
Additional notes	Better education must be provided to employees to reduce susceptibility to phishing campaigns. What technical solutions could be implemented to minimize the impact of an event like this in the future?

Date: Tuesday, 2023-06-20	**Entry:** 2
Description	Financial Services Company - Investigation of Suspicious Web Domain From Email Flagged as Phishing Attack
Tool(s) used	Chronicle (SIEM Tool) & VirusTotal

The 5 W's	While working as a security analyst at a financial services company, I received an alert that an employee received a phishing email containing a suspicious domain "`signin.office365x24.com`". Using Chronicle, the following was determined: ● VirusTotal shows that one security vendor has flagged this domain as suspicious. ● This domain is placed within the "drop site for logs or stolen credentials" category by the ET Intelligence Rep List. ● Chronicle's "Assets" section shows access from 6 distinct users, all on the same day (2023-01-31). ○ Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, Roger Spence ● Chronicle's "Timeline" section shows POST requests from two users, Ashton and Emil, to the signin page. This indicates that information was submitted and likely compromised, denoting a successful phishing attack. ● Chronicle's "Resolved IPs" section shows a single IP address: "`40.100.174.34`". ○ Related to this IP address is one additional (likely malicious) domain: "`signin.accounts-gooqle.com`" ○ There are two new assets: Amir David, Warren Morris ○ The timeline view shows that Warren also sent a POST request to a fake login page.
Additional notes	This web domain is highly likely to be a malicious actor's attempt to steal login credentials.

Date: Tuesday, 2023-06-20	**Entry:** 3
Description	E-Commerce Store Buttercup Games - Investigate Mail Server Security Issues
Tool(s) used	Splunk

The 5 W's	Used Splunk Cloud to explore an event log containing 109,864 events. Used search filters to find failed SSH logins for the root account within the company's mail server.
Additional notes	Found over 300 events that met the specified criteria.

Date: Tuesday, 2023-06-20	**Entry:** 4
Description	Exploring Captured Packets with Suricata Using Custom Rules
Tool(s) used	Suricata
The 5 W's	I used the CLI to view a custom rules file to be used with Suricata. This file consisted of the action (pass, drop, reject, alert), a header, and rule options. The header specified the protocol (in this case http), the local/home network address and ports, and the destination IP address and port(s). Within the rule options were the following: • A message to accompany the alert • The flow • What content to target and in which portion of the packet ("`GET`" within `http.method`) • The signature ID for the rule • The revision number I then ran Suricata with elevated privileges to analyze a sample file of network traffic using the previously described rules file. I concluded by examining the "`fast.log`" file to examine the alerts that were generated based off of the provided rules.
Additional notes	I learned about using the `jq` command to view json files in an easy to read format. I also learned the commands for extracting specific data fields from a json file. Example Command:

	`jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json`

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?
    - The activities weren't particularly difficult though I found it very important to read carefully, follow instructions precisely, and take notes on the new terms and commands I learned along the way. Thankfully, each activity progressed at a pace that felt manageable while often still providing a bit of challenge to encourage growth.

2. Has your understanding of incident detection and response changed since taking this course?
    - Certainly! There are a wide variety of tools available for use in incident detection and response. Being familiar with these different tools, especially in being able to use them quickly will be particularly helpful during actual incident response.

3. Was there a specific tool or concept that you enjoyed the most? Why?
    - I thoroughly enjoyed using Chronicle and found that after the activity, I felt much more comfortable with the interface (which at first seemed complex and a bit daunting). It appears to be a powerful tool and I can envision being able to use it fluidly during a detection & response event.