Cybersecurity Boot Camp

Security 101 Challenge

Cybersecurity Threat Landscape

Part I: Crowdstrike 2021 Global Threat Report

For Part 1 of your homework assignment, use the *Crowdstrike 2021 Global Threat Report* along with independent research to answer the following questions. (Remember to make a copy of this document to work in.)

---

1. What was the dominant ransomware family that impacted the healthcare industry in 2020?

```
The most dominant ransomware family that impacted the healthcare industry in
2020 was the group TWISTED SPIDER which used Maze and Egregor ransomware.
They were able to achieve 26 infections in the healthcare sector.
```

2. Describe three different pandemic-related eCrime Phishing themes.

```
Three pandemic-related eCrime Phishing themes that were mentioned in the
Crowdstrike article were, scams offering personal protective equipment,
financial assistance and government stimulus packages, and tailored attacks
against employees working from home (CROWDSTRIKE 2021).
```

3. Which industry was targeted with the highest number of ransomware-associated data extortion operations?

```
The industry that was targeted with the highest number of ransomware-
associated data extortion operations was the industrial and engineering
```

sector with 229 incidents while the manufacturing sector had 228 incidents (CROWDSTRIKE 2021).

4. What is WICKED PANDA? Where do they originate from?

WICKED PANDA is a Cyber threat group and they originate from China. They are state sponsored and carry out intelligence and financial crimes for personal and government benefits.

5. Which ransomware actor was the first observed using data extortion in a ransomware campaign?

The first ransomware actor observed using data extortion in a ransomware campaign was OUTLAW SPIDER.

6. What is an access broker?

Access brokers, according to the crowdstrike article are threat actors who have gained backend access to a number of corporate or government organizations and sell these accesses to other threat actors on criminal forums or private channels (CROWDSTRIKE 2021). Access brokers eliminate the process of identifying and gaining access to targets which allows the cybercriminals to deploy quicker and increase their monetization.

7. Explain a credential-based attack.

A credential based attack is when attackers use methods such as phishing, keylogging or man in the middle to steal your credentials. Once they have your credentials they use it to bypass the organization's security and steal information that they can use or sell.

8. Who is credited for the heavy adoption of data extortion in ransomware campaigns?

TWISTED SPIDER is credited for the heavy adoption of data extortion in ransomware campaigns.

9. What is a DLS?

DLS stands for dedicated leak sites. This is a website whose purpose is to sell data that has been stolen after successful ransomware attacks.

10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?

According to Crowdstrike Falcon OverWatch 79% of intrusions came from eCrime.

11. Who was the most reported criminal adversary of 2020?

The most reported criminal adversary in 2020 was WIZARD SPIDER.

12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.

SPRITE SPIDER and CARBON SPIDER impacted virtualization as they targeted Linux machines on ESXi hosts during BHG operations. By targeting these hosts, the ransomware operators were able to encrypt multiple systems with very few ransomware deployments. The crowdstrike article mentions that encrypting one ESXi server will cause equal amounts of damage as deploying ransomware on each VM server (CROWDSTRIKE 2021). Targeting EXSi hosts also enhances the speed of BGH operations and EXSi hosts lack endpoint protection software which means that these ransomware attacks may go undetected (CROWDSTRIKE 2021).

13. What role does an Enabler play in an eCrime ecosystem?

The crowdstrike article tells us that enablers provide criminal actors with the resource they would not have any access to. These groups run “malware-as-a-service operations, specialize in delivery mechanisms or exploit networks in order to sell initial access to other criminal actors” (CROWDSTRIKE 2021).

14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

The three parts of the eCrime ecosystem that have been highlighted in the current article are **Services** (access brokers, ransomware, hardware for

sale), **distribution** (spam email distribution, exploit kit development, social network and instant message spam) and **monetization** (reshipping fraud networks, money laundering, ransom payment extortions).

15. What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?

The name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software was called SUNBURST.

Part 2: Akamai Security Year in Review 2020

In this part, you should primarily use the *Akamai Security Year in Review 2020* and *Akamai State of the Internet / Security* along with independent research to answer the following questions.

---

1. What was the most vulnerable and targeted element of the gaming industry between October 2019 to September 2020?

The most vulnerable and targeted element of the gaming industry was the human element or in other words, the players.

2. From October 2019 to September 2020, which month did the financial services industry have the most daily web application attacks?

The month December 2019 had the most daily web application attacks.

3. What percentage of phishing kits monitored by Akamai were active for only 20 days or less?

60% of phishing kits were active for only 20 days or less.

4. What is credential stuffing?

```
Credential stuffing is a type of cyberattack where the attacker uses a list of compromised usernames and passwords to breach into a system.

Mueller, N. (2023). Credential stuffing Software Attack | OWASP Foundation. Owasp.org. https://owasp.org/www-community/attacks/Credential_stuffing
```

5. Approximately how many of the gaming industry players have experienced their accounts being compromised? How many of them are worried about it?

```
More than half of frequent players had their accounts compromised and only one-fifth of players are worried about it.
```

6. What is a three-question quiz phishing attack?

```
The three question quiz phishing attack is a quiz that asks the user 3 questions related to the brand that is being abused. No matter what the user says in their answer, they will always get it right and always win a prize associated with that brand. The victim is then sent a link that forwards them to a website which requests their personal details, such as email, home address and age (Katz, 2018).
```

7. Explain how Prolexic Routed defends organizations against DDoS attacks.

```
Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing clean traffic forward. Individuals at Akamai security operations center then mitigate and stop the attacks immediately, and conduct a live analysis of the remaining traffic to determine further mitigation as needed (Akamai 2020).
```

8. What day between October 2019 to September 2020 had the highest Daily Logins associated with Daily Credential Abuse Attempts?

```
August 17th, 2020 had the highest daily logins associated with daily credential abuse attempts.
```

9. What day between October 2019 to September 2020 had the highest gaming attacks associated with Daily Web Application Attacks?

```
July 11th, 2020 had the highest number of gaming attacks associated with
daily web application attacks.
```

10. What day between October 2019 to September 2020 had the highest media attacks associated with Daily Web Application Attacks?

```
August 20th, 2020 had the highest number of media attacks.
```

Part 3: Verizon Data Breaches Investigation Report

In this part, use the *Verizon Data Breaches Investigation Report* plus independent research to answer the following questions.

---

1. What is the difference between an incident and a breach?

```
The difference between an incident and a breach is an incident is an event
that occurs which compromises that integrity, confidentiality and
availability of an information asset. A breach is an incident that confirms
disclosure of data to an unauthorized party; this is not just a potential
exposure of data.
```

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?

```
The percentage of breaches by both external and internal actors have varied
over the years. The number of external breaches between 2016-2020 is
approximately 75.6%. The number of internal breaches between 2016-2020 is
approximately 27.2%.
```

3. What percentage of breaches were perpetrated by organized crime?

```
80% of breaches were perpetrated by organized crime according to the
article.
```

4. What percentage of breaches were financially motivated?

```
The rough average between 2016-2020 the percentage of breaches that were financially motivated were approximately 77.5%.
```

5. Define the following (additional research may be required outside of the report):

```
Denial of service:Cyber attack that is used to render a machine or network unavailable to its users by temporarily or indefinitely disrupting services. These can include network and application layer attacks (Verizon 2021).

Command control:A command and control attack is one where bad actors are able to infiltrate a system and install malware that lets them remotely control infected devices over a network (Verizon 2021).

Backdoor:A backdoor is any method that allows authorized and unauthorized users to gain high level access to a system while bypassing regular security and authentication measures (Verizon 2021).

Keylogger:A keylogger is a type of spyware that is able to record a user's keystrokes on a device which allows them to steal sensitive information such as passwords and login information (Verizon 2021).
```

6. What remains one of the most sought-after data types for hackers?

```
The most sought-after types of data for hackers are credentials.
```

7. What was the percentage of breaches involving phishing?

```
Just under 40% of breaches involve phishing (approximately 36%).
```


References:

1. The 2021 CROWDSTRIKE® Global Threat Report. 2021 CrowdStrike Global Threat Report. (n.d.). Retrieved March 13, 2023, from https://go.crowdstrike.com/crowdstrike-global-threat-report-2021.html

2. [state of the internet] / security a year in Review. (n.d.). Retrieved March 13, 2023, from https://v4.iplookup.akamai.com/site/en/documents/state-of-the-internet/soti-security-a-year-in-review-report-2020.pdf
3. (PDF) 2021 Verizon Data Breach Investigations Report - Researchgate. (n.d.). Retrieved March 13, 2023, from https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report
4. Katz, O. (2018, December 15). Quiz Phishing: One Scam, 78 Variations. Akamai.com; Akamai Technologies. https://www.akamai.com/blog/security/quiz-phishing--one-scam--78-variations
5. *What is a credential-based attack?* Palo Alto Networks. (n.d.). Retrieved March 10, 2023, from https://www.paloaltonetworks.ca/cyberpedia/what-is-a-credential-based-attack