Cybersecurity Boot Camp

Security 101 Challenge

Cybersecurity Threat Landscape

Part 1: 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 on):

---

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

```
MAZE (TWISTED SPIDER)
```

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

```
Scam links offering people personal protective equipment(PPE), Stimulus
packages offering free money from the goverment, attacks to people working
from home with computers.
```

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

```
Crowdstrike Intelligence
```

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

```
Wicked panda originates from china. They are a cyber treat group known for carrying out espionage and financial crimes for personal and goverement benefit.
```

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

```
Outlaw-Spider
```

6. What is an access broker?

```
Cybercriminals that sell access to different networks or mainly corporate networks
```

7. Explain a credential-based attack.

```
It is when an attacker steals credentials such as passwords to get access. After that they use the stolen credentials to then bypass whatever security mesures are in place to then steal sensitive data.
```

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

```
Maze (Twisted Spider)
```

9. What is a DLS?

```
Dedicated Leak Site
```

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

```
79%
```

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

```
Wizard Spider
```

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

```
Both Sprite Spider and Carbon Spider were both able to encrypt multiple
systems easily.
```

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

```
They are the individuals that provide services for attackers
```

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

```
Services, distribution, Monetization
```

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

```
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 and September 2020?

```
Players
```

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

```
December 2019
```

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

```
60%
```

4. What is credential stuffing?

```
Attackers use a list of compromised user credentials to breach a system.
```

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

```
Half said they were compromised but only ⅕ were worried about it
```

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

```
An attack that relys on users filling out quizzes in exchange for a prize.
This then results in stolen personal information
```

7. Explain how Prolexic Routed defends organizations against Distributed Denial of Service (DDoS) attacks.

```
It redirects network traffic through akamai scrubbing centers making sure it
is only allowing clean traffic through.
```

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

```
August 17 2020
```

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

```
July 11 2020
```

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

```
August 20 2020
```

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?

```
An incident is mainly a security event compromising the CIA triad. A breach is a confirmed exposure of information to an unauthorized individual or organization.
```

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

```
66% outside and 37% internal
```

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

```
80%
```

4. In 2020, what percent of breaches were financially motivated?

```
92%
```

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

```
Denial of service: Attacks with the end goal of compromising the availability of networks and systems

Command control:A system controlled by a bad actor used to send commands to systems compromised by malware to receive data from a target network
```

Backdoor:a method of bypassing authentication or encryption of systems

Keylogger:A form of malware used to monitor and capture keystrokes on a system

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

credentials

7. What was the percentage of breaches that involved phishing?

36%