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?

Maze

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

1.Financial assistance and government stimulus packages
2.Scams offering personal protective equipment
3.Exploitation of individuals looking for details on disease tracking, testing and treatment

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

Healthcare

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

```
WICKED PANDA is a cyber threat group that carries out Chinese state-
sponsored attacks. They also execute financially motivated attacks outside
of state control. Wicked Panda usually attacks their targets by employing
spear-phishing emails with malicious attachments for the initial compromise.
```

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

```
Outlaw Spider
```

6. What is an access broker?

```
Access brokers are bad actors that gain backend access to various
organizations(both corporations and government entities) and sell this
access either on criminal forums or through private channels.
```

7. Explain a credential-based attack.

```
Credential-based attacks occur when attackers steal information logs
typically containing data such as IP addresses, endpoint URLs, login
credentials, screenshots of the victim's desktop, cookies, and browser
autofill history that can be used to determine the type of system used as
well as provide a vector for initial access. This is useful to bypass an
organization's security measure and steal critical data.
```

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

```
Twisted Spider
```

9. What is a DLS?

```
Data Leaked Sites
```

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

```
79% of intrusions came from eCrime intrusions.
```

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

```
Twisted Spider
```

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

```
By deploying Linux versions of their respective ransomware families on ESXi
hosts during BGH operations.
```

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

```
Enabler plays a pivotal role  in the eCrime ecosystem because it allows
criminal actors to have access to capabilities that they normally do not
have access to. These actors provide malware as a service operator and
deploy mechanisms or exploit networks in order to sell initial access to a
criminal.
```

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

```
Services, Distribution, and 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 to September 2020?

The users were the most vulnerable targeted element of the gaming industry - Specifically the daily credentials abuse attempts.

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

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?

More than 60% of all the phishing kits monitored by Akamai were active for only 20 days or less.

4. What is credential stuffing?

Credential stuffing is a cyber attack method in which cybercriminals use lists of compromised credentials to breach into 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?

More than half of frequent players had their accounts compromised but only one-fifth were worried about having their account compromised.

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

These attacks rely on users to fill out a quiz in exchange for a prize. This usually ends up with the users information being stolen.

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

Prolexic Routed is used to defend organizations against DDoS attacks by redirecting network traffic through a centralized cleansing station. This allows the center to analyze and remove malicious traffic and only allow the clean traffic forward.

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

July 4, 2020

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

July 11,2020

10. What 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?

The difference between the two is that an incident violates an organization's security’s policy by compromising the C.I.A triad. A breach on the other hand, is an incident that results in data, applications, network, devices etc. being disclosed to an unauthorized party/actor.

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

External actors made up of 75%-85%. Internal actors made up of 25%-30%

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

80% of breaches were perpetrated by organized crime.

4. What percentage of breaches were financially motivated?

90%-95% of the breaches were financially motivated.

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

Denial of service: Denial of service is a cyber attack method that redirects traffic or sends information at a target to cause the machine to crash/shutdown.

Command control:These attacks occur when bad actors infiltrate a system and install malware that allows them to remotely control them from a C2 server.

Backdoor: The deployment of malware/virus/technology to allows an actor to bypass normal security measures and gain unauthorized access to the application/network/system remotely.

Keylogger:Is a hardware device or malware used to record a keyboard's key strokes.

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

Credentials remain one of the most sought-after data types for hackers.

7. What was the percentage of breaches involving phishing?

The percentage of breaches involving phishing was 36%