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?

```
[Twisted spiders is the ransomware family]
```

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

```
[1. they used Finacial assistance and government stimulated packages in
emails and messages for phishing themes. 2. They sent emails with scams
offering personal protective equipment. 3. They would impersonate medical
bodies such as, The World Health Organization, U.S. Centers for disease
control and prevention. ]
```

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

```
[BGH operators was targeted with the highest number of ransomware-associated
data extortion operations. 18 bgh families infected 104 healthcare
organizations with Twisted Spider being the most prolific.]
```

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

```
[Wicked Panda is a Ransomware family that originates in The Republic of
China.]
```

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

```
[Viking Spider’s Ragnar Locker was the first actor observed using data
extortion in a ransomware campaign first being identified in December of
2019 and first Dls Discovered on Feburary 10th 2020.
```

6. What is an access broker?

```
[They are threat actor who gain backend acess to many different
organizations and sell their access to either criminal forums or private
channels.]
```

7. Explain a credential-based attack.

```
[a credential based attack is when someone attacks a company or person
trying to obtain credentials that will give them access to sensitive and
secure data.]
```

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

```
[Enter answer here]
```

9. What is a DLS?

```
[A DLS stands for a “Dedicated Leak Site” it is a cite that people using
data extortion uses to obtain or give out leaked/sensitive data.]
```

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

```
[90%]
```

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

```
[Wizard Spiders]
```

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

```
[they were able to quickly encrypt multiple systems with few actual
ransomware deployments that inflicted the same amount of damage ass
individually deploying ransomware on each VM hosted on a server. ]
```

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

```
[Enablers are the ones providing actors with the capabilities and necessary
hard ware and programs that they would not have access too otherwise.]
```

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

```
[ Services, Distribution, and monetization are the three parts highlighted
in the ecosystem.]
```

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

```
[UNC2452 is the name of the cose used to exploit a vulnerability in the
solarwinds orion it management software.]
```

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 is its
players.]
```

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

```
[December of 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?

```
[^0%]
```

4. What is credential stuffing?

```
[credential stuffing is when Criminals buy your leaked credentials and use
bots to try to login in with your credentials.]
```

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 the frequent players said their accounts compromised but
only one fifth of them are worried about it.]
```

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

```
[Enter answer here]
```

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

```
[it is a scam pretending to be a known brand where they try to get you to do
a three question survey in hopes of obtaining personal information.]
```

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

```
[Enter answer here]
```

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

```
[December 9th 2019]
```

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

```
[August 20th, 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?

```
[a breach is when someone accesses something they should not be accessing
and they know it. And incident is something that happens to someone without
them meaning to or knowing.]
```

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

```
[61% of breaches were by outside actors and 85% of breaches were by internal
actors.]
```

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

```
[80% was perpetrated by organized crime.]
```

4. What percentage of breaches were financially motivated?

[about 65% of breaches were financially motivated]

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

Denial of service:An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.

Command control:the running of an armed force or other organization

Backdoor:an attempt to infiltrate a system or a network by maliciously taking advantage of software's weak point.

Keylogger:a program that records every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.

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

[web applications is one of the most sought after data types for hackers.]

7. What was the percentage of breaches involving phishing?

[25% of breaches involved phising]