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

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

Exploitation of individuals looking at disease tracking, testing and treatment. Financial assistance and government stimulus packages. Scams offering personal protective equipment.

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

Industrial and engineering sector.

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

```
WICKED PANDA is a state-sponsored, well-known, and effective cyber crime
group from China.
```

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

```
OUTLAW SPIDER.
```

6. What is an access broker?

```
A person/persons that gain access to public or private organizations and
sell this access to others.
```

7. Explain a credential-based attack.

```
When someone steals credentials to get passed security measures, gain access
to data, and carry out an attack.
```

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

```
TWISTED SPIDER.
```

9. What is a DLS?

```
Dedicated leak sites.
```

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.

```
They developed Linux versions of ransomware that are very effective against
the virtualization solutions employed by many organizations.
```

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

```
They provide criminal people/organizations with capabilities they may not
otherwise have access to.
```

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

```
eCrime Enablers, Axcess Brokers, BGH Ransomware Operators.
```

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

```
SUNSPOT.
```

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?

```
The 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?

Using stolen account credentials to gain access to an account through large-scale automated log-in requests.

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

Half had their accounts compromised, only 1/5th were worried about it.

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

People fill out a quiz in exchange for a “prize” which results in stolen information.

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

By redirecting network traffic through scrubbing centers and only allowing the clean traffic forward.

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

Aug. 17, 2020.

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

```
Jul. 11, 2020.
```

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

```
Aug. 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 any event outside of normal operations that compromises
security of a network, data, or hardware, not necessarily caused by anyone.
A breach is when someone intentionally compromises the security of a
network, data, or hardware.
```

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

```
External:70%-80%
Internal-20%-30%
```

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

```
80%
```

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

```
90%
```

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

Denial of service:Attacks intended to compromise the availability of networks and systems. Includes both network and application layer attacks.

Command control:Attacks where a person infiltrates a server and installs a program that allows the person to remotely send commands to infected devices.

Backdoor:Method of bypassing authentication processes in software to gain access.

Keylogger:A computer program that records all keystrokes made by a user.

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%