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.

```
One pandemic-related eCrime Phishing theme is the exploitation of
individuals looking for details on disease tracking, testing, and
treatment. Another Phishing theme is the impersonation of medical bodies,
including the World Health Organization (WHO) and U.S.Centers for Disease
Control and Prevention (CDC). A third Phishing theme is offering
financial assistance and government stimulus packages.
```

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 an adversary group that began in 2020 by conducting a wide-ranging campaign focused on exploiting multiple vulnerabilities that also cut across verticals and geographies. WICKED PANDA originates from China due to the moniker PANDA.
```

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 threat actors, or hackers, that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels like the dark web.
```

7. Explain a credential-based attack.

```
Scanning and Exploiting a remote service to harvest user account credentials. Then, using those credentials to brute force, password spray, or credential stuff to obtain more access. Finally, sell accounts, data, or exploit further.
```

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.

```
SPRITE SPIDER and CARBON SPIDER deploy Linux versions of their respective
ransomware families on ESXi hosts to gain access to all VMs using the
hypervisor.
```

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

```
Enablers are an important part of the eCrime ecosystem, they provide
criminal actors with capabilities they may otherwise not have access to.
These criminal actors run malware-as-a-service operations, specialize in
delivery mechanisms or exploit networks in order to sell initial access
to other criminal actors.
```

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

```
1. Services
2. Distribution
3. 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 Players
```

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

```
Dec 2019
```

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

```
More than 60%
```

4. What is credential stuffing?

```
Credentials obtained from a data breach on one service are used to attempt
to log in to another, unrelated, service.
```

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 gaming industry players said they’ve had their
accounts compromised, but only one-fifth of the players were worried about
such things happening.
```

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

```
The user answers three questions related to the imitated brand, then the
user wins a prize associated with that brand. The user is forwarded to a
website requesting their private information.
```

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. The clean data is then
allowed through while the rest is not.
```

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

```
Aug 17, 2020
```

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

```
Jul 11, 2020
```

10. What 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 a security event that compromises the integrity,
confidentiality, or availability of an information asset while a breach is
an incident that results in the confirmed disclosure - not just potential
exposure - of data to an unauthorized party.
```

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

```
External Actors: ~79%
Internal Actors: ~21%
```

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

```
~80%
```

4. What percentage of breaches were financially motivated?

```
~70%
```

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.

Command control: Bad actors infiltrate a system and install malware that lets them remotely send commands from a C2 server to infected devices.

Backdoor: Any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application.

Keylogger: Maleware on the victim’s computer that will read all of the key presses and log them to the attacker.
```

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

```
Credentials
```

7. What was the percentage of breaches involving phishing?

```
36%
```