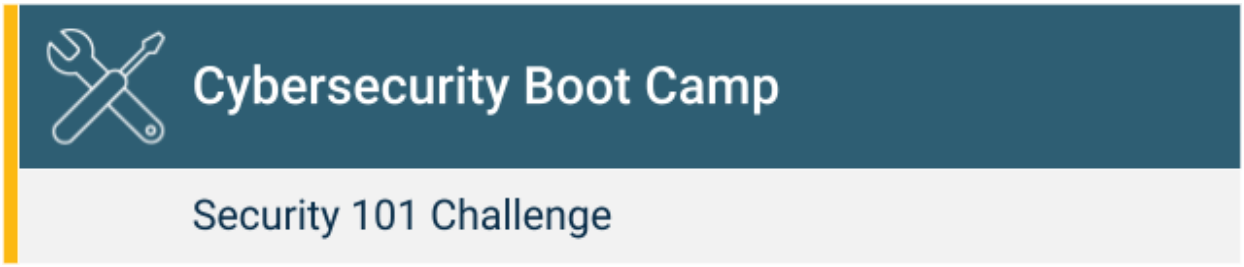

Cybersecurity Threat Landscape

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 is a well-known ransomware variant that gained attention for its
advanced tactics.
```

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

```
Healthcare scams involve phishing emails impersonating health organizations,
providing false pandemic information. Financial relief scams exploit
economic uncertainties, with cybercriminals using phishing campaigns for
fake financial aid. Remote work-related phishing targets increased remote
work, using emails on tools, video conferencing, or IT support
```

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

```
Health care industry, as hospitals and other healthcare organizations became
prime targets, Critical infrastructure, including energy and transportation.
```

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

```
Wicked Panda is a Chinese state-sponsored cyber threat group that
specializes in espionage and financially motivated activity.
```

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

```
The first known malware extortion attack was the "Trojan"
```

6. What is an access broker?

```
Access Broker (IAB) is a threat actor specializing in infiltrating computer
systems and networks, then selling that unauthorized access to other
malicious actors
```

7. Explain a credential-based attack.

```
Credential-based attacks occur through stealing, brute force, or finding
passwords on the dark web. Harvesting exploits user unawareness, while
credential stuffing results from data breaches at other companies
```

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

```
Maze and Egregor ransomware – has been credited with being the catalyst for
the heavy adoption of this technique in 2020.
```

9. What is a DLS?

```
Dedicated Leak Sites (DLS) publish data that has been illicitly retrieved
from companies that refuse to pay a ransom.
```

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

```
79% of all attributable intrusions in 2020 were eCrime intrusions
```

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

```
Wizard Spider was the most reported criminal adversary of 2020.
```

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

```
Sprite Spider: Utilizes stolen credentials for web interface access.
Carbon Spider: Accesses with legitimate credentials, focusing on U.S.
retail, restaurant, and hospitality sectors.
```

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

```
Enablers in an eCrime ecosystem are individuals or organizations that
provide services to those who want to carry out cyberattacks
```

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

```
Service, 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?

```
Account Takeovers (ATO): Cybercriminals aimed to compromise gaming platform accounts through phishing, credential stuffing, and using stolen login credentials from prior data breaches.
```

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

```
December
```

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
```

4. What is credential stuffing?

```
Credential stuffing is a cyberattack where an attacker uses stolen or leaked credentials to gain unauthorized access to user accounts. The attacker uses automated tools to test large numbers of credentials against multiple websites or services.
```

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

```
The gaming industry experienced 20% attacks
```

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

```
Attackers mimic reputable sources, urging recipients to take a security quiz. The fake survey gradually collects personal data, posing risks like identity theft, unauthorized account access, and fraud.
```

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

```
Prolexic Routed, by Akamai, is a DDoS protection service shielding organizations from online service disruptions. It counters DDoS attacks by
```

```
filtering and diverting malicious traffic away, ensuring uninterrupted and
secure online operations.
```

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?

```
Incident: A security event that compromises the integrity, confidentiality
or availability of an information asset.
Breach: 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?

```
80% external 20% interna
```

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

```
80%
```

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

```
Financially motivated attacks ranged between 86 and 100%.
```

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

```
DDoS Attacks: Coordinated assaults by botnets overwhelm targets. Their
distributed nature heightens potency and poses challenges for effective
mitigation.
Command Control: Linked with malware, it connects compromised systems to
remote servers, serving as command centers for attackers to send
instructions and gather data.
Backdoor: In cybersecurity, it denotes potential security risks, prompting
vigilance against unauthorized access, emphasizing the need for protective
measures.
Keylogger: Records keystrokes on devices, capturing sensitive information.
Keyloggers, with dual-use potential, can serve legitimate purposes or be
exploited maliciously for unauthorized data collection.
```

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

```
One of the most sought-after data types for hackers is personally
identifiable information (PII). PII includes any information that can be
used to identify an individual, either on its own or in combination with
other available information.Hackers target PII because it can be used for
various malicious purposes, including identity theft, financial fraud, and
other forms of cybercrime.
```

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

```
35%
```