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?

```
The Dominant ransomware was Maze.
```

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

```
Exploitation of individuals looking for details on disease tracking, testing
and treatment, by attracting visitor traffic via online searches.
Impersonation of medical bodies, (like WHO,CDC)
Tailored attacks against employees working from home, either to interact
with a hyperlink or attachment to an email.
Scams offering Personal Protective Equipment(PPE).Creating fake websites to
steal Personal Information.
```

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

```
Industrial Engineering sector
```

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

is a cyber threat group that carries out Chinese state-sponsored espionage activity. Originates 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?

threat actors that gain backend access to both corporations and government entities and sell this access on criminal
forums or through private channels.

7. Explain a credential-based attack.

They prey on vulnerabilities of user logins by exploiting Remote Service or Escalating privileges, using brute forcing, password spraying, credential stuffing to obtain users credentials.

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

Twisted Spider

9. What is a DLS?

Dedicated Leak Site. Used to pressure victims or companies into paying the ransom.Companies also used this to improve security practices that could negate encryption of their files by recovering from backups.

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.

```
By deploying linux versions of their ransomware families on ESXi hosts
during BGH operations.incidents, SPRITE SPIDER used administrator
credentials to log in through the vCenter web interface, this way targeting
multiple systems with relatively few actual ransomware deployments.
Carbon Spider shifted from narrow campaigns
focused entirely on companies operating POS devices to broad, indiscriminate
operations attempting to infect large numbers of victims across all
sectors.But later CARBON SPIDER's shift away from POS campaigns exemplifies
a broader
trend of targeted eCrime actors shifting targets to focus on BGH by using
their own ransomware, DarkSide.
```

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

```
They provide access to ransomware and phishing kits for a fee, without
Enablers many cyber criminals wouldnt have access to exploit networks. They
play a pivotal part in the e-crime ecosystem.
```

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 and September 2020?

The most Vulnerable and most targeted element was its 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?

a cyber attack in which an attacker uses a list of stolen usernames or email addresses and passwords to gain access to user accounts on various applications. (https://mojoauth.com/blog/what-is-credential-stuffing/)

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 they’ve had their accounts compromised, but only one-fifth of them were worried about such things.

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

These attacks rely on users filling out these quizzes in exchange for a “prize,” which often results in stolen personal information.

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

```
by redirecting network traffic through
Akamai 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?

```
August 17,2020. 365,181,101daily credential abuse attempts.
```

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?

```
A breach is an incident that results in
the confirmed disclosure—not just
potential exposure—of data to an
unauthorized party. An incident a security event that
compromises the integrity,
confidentiality or availability of
```

an information asset.

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

70% Outside actors, 30% Internal actors

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

80%

4. What percentage of breaches were financially motivated?

95%

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:a type of attack in which a malicious actor uses a malicious server to command and control already compromised machines over a network

Backdoor:is a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms.

Keylogger:a type of spyware that can record and steal consecutive keystrokes that the user enters on a device.

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

Credentials and Personal

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

80%