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.

```
*Financial assistance and government stimulus packages.
*Impersonation of medical bodies, including WHO and U.S Center for disease
Control and Prevention.
*Scam 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?

```
The WICKED PANDA adversary began 2020 by conducting a wide-ranging
campaign focused on exploiting multiple vulnerabilities (CVE-2019-19781 and
CVE-2020-10189) that cut across verticals and geographies. Upon successful
exploitation,they deployed Cobalt Strike and Meterpreter payloads to further
interact with victims.They originate 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?

```
Access brokers are threat actors that gain backend access to various
organizations
(both corporations and government entities) and sell this access either on
criminal
forums or through private channels.
```

7. Explain a credential-based attack.

```
CrowdStrike Intelligence assesses that remote service and privilege
escalation
vulnerabilities enable the viability of credential-based attacks (e.g.,
brute forcing,
password spraying, credential stuffing). This assessment is made with
moderate
confidence based on in-the-wild attacks and other reporting pertaining to
access brokers.
```

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.

```
   ● In 2020, CrowdStrike Intelligence observed both SPRITE SPIDER (the
     operators
of Defray777) and CARBON SPIDER (the operators of DarkSide) deploy Linux
versions of their respective ransomware families on ESXi hosts during BGH
Operations.
   ● With more organizations migrating to virtualization solutions to
     consolidate legacy IT systems, this is a natural target for ransomware
     operators looking to increase the impact against a victim.
   ● CARBON SPIDER deepened their commitment to BGH in August 2020 by using
     their own ransomware,DarkSide. In November 2020, the adversary took
     another step into the world of BGH by establishing a RaaS-a!liate
     program for DarkSide, allowing other actors to use the ransomware
     while paying CARBON SPIDER a cut.
```

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

```
Enablers are a pivotal part of the eCrime ecosystem, providing criminal
actors with capabilities they may otherwise not have access to. These
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?

```
- Endpoints and cloud workloads
- Identity and data
- Provides a valuable research for organizations looking to bolster their security strategy.
```

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?

```
Its players.
```

2. From October 2019 to September 2020, 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%
```

4. What is credential stuffing?

```
Credential Stuffing is a cyberattack in which the attacker collects stolen
credentials consisting of username and password then uses it to gain access
to the unauthorized accounts.
```

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 player's accounts are compromised and only
one fifth of them were worried about it.
```

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

```
The three-question quiz phishing 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 DDoS attacks.

```
Prolexic Routed defends organizations against
DDoS attacks by redirecting network traffic through
Akamai scrubbing centers, and only allowing the
clean traffic forward. Experts in the Akamai security
operations center (SOC) tailor proactive mitigation
controls to detect and stop attacks instantly, and
conduct live analysis of the remaining traffic to
determine further mitigation as needed.
```

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

```
August 17th
```

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

```
July 11th
```

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

```
August 20th
```

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 is a security event that compromises the integrity, confidentiality or availability of an information asset whereas 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 87% and internal actors 17%
```

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

```
80%
```

4. What percentage of breaches were financially motivated?

```
71%
```

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

Denial of service:A Denial of service attack is an attack meant to shut down a machine or a network, making it inaccessible to its, or intended users. Dos attack accomplish this flooding the target with traffic or sending it information that triggers a crash.

Command control:A Command and control server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

Backdoor:A backdoor is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

Keylogger:A Keylogger is an insidious form of spyware. You enter sensitive form of data believing that nobody is watching.In fact, keylogging software is hard at work logging everything that you type. Keyloggers are activity-monitoring software programs that give hackers access to your personal data.

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

Credentials remains one of the most sought data types for hackers.

7. What was the percentage of breaches involving phishing?

36%