Cybersecurity Boot Camp

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 was the dominant ransomware family, with conti right behind.
```

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

```
1) Exploitation of individuals looking for details on disease tracking,
   testing and treatment.
2) Tailored attacks against employees working from home.
3) Scams offering PPE
```

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

```
Industrials & Engineering, followed closely by Manufacturing
```

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

```
Wicked Panda is an adversary group that originates from China.
```

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

```
Outlaw Spider - May 2019.
```

6. What is an access broker?

```
Access brokers gain backend access to various organizations and sell this
access on either criminal forums or through private channels.
```

7. Explain a credential-based attack.

```
Credential based attack uses stolen credentials to gain access to domains
they would not otherwise be able to infiltrate. They can also use this
access to increase privilege within a domain to admin, which effectively
takes over the domain. This would allow the attacker to potentially obtain
more user credentials, and repeat the process again.
```

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, for the second year in a row.
```

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

```
They exploited an efficient tactic which allows the operator to encrypt one server, but yielded the work of encrypting multiple servers.The Spiders targeted ESXi servers and could encrypt the various legacy systems that were being managed from that hypervisor.
```

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

```
Enablers provide criminals with various services. These services include: malware, delivery mechanisms and network exploitation to sell initial access. Sounds like a one stop shop for script kitties looking to evolve.
```

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 to September 2020?

```
The gaming industry players.
```

2. From October 2019 to September 2020, 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?

```
“More than 60% . . .”
```

4. What is credential stuffing?

```
Credential stuffing is using login information from a breach in an 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 have had their accounts compromised. Only ⅕ were worried.
```

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

```
It is a phishing attack that asks questions that would be similar to password reset (e.g Mother’s Maiden Name) in exchange for a prize. This info could be used to log into accounts if an attacker had email login access, and wanted to reset passwords for various accounts.
```

7. Explain how Prolexic Routed defends organizations against DDoS attacks.

```
Prolexic Routed defends DDoS attacks by redirecting network traffic through Akami scrubbing centers, and then only allowing clean traffic through.
```

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

```
From Figure 4 it seems like it was August 15,2020. This was right before the darknet marketplace Empire went offline.
```

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

```
July 11, 2020
```

10. What 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?

```
An incident is an event that compromises one aspect of CIA. A breach is a
confirmed event of data being accessed by a 3rd party.
```

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

```
From Figure 14, it looks like approximately 80% were perpetrated by outside
attackers, and approximately 20% by internal actors.
```

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

```
From Figure 16's strange bar graph, it looks like approximately 80% of
breaches were perpetrated by organized crime.
```

4. What percentage of breaches were financially motivated?

```
Figure 15's Y axis seems to indicate that virtually all (appx 95%) of
breaches are financially motivated.
```

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. Pg 34 of Verizon Report

Command control:Technique used by threat actors to communicate with compromised devices over a network. After a foothold is established, it is common that the threat actor will upload additional Malware or Ransomware depending on their motivation.
https://www.paloaltonetworks.com/cyberpedia/what-is-command-and-control

Backdoor: Is a method that allows unauthorized access without the admin's knowledge. A backdoor can be installed via Malware, software exploits or a direct install into the device's hardware/firmware.
https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/

Keylogger: A type of spyware. It is a software that logs what you type into the keyboard. Keyloggers aren't necessarily nefarious, as corporations can have keyloggers installed to help end users troubleshoot technical problems with the help of IT staff. They generally infect a host via malware download unknowingly performed by the victim.
https://www.malwarebytes.com/keylogger

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

Credentials. Personal data is second.

7. What was the percentage of breaches involving phishing?

From Figure 20, it seems that approximately 35% of breaches involve phishing.