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?

```
The dominant families were TWISTED SPIDER and WIZARD SPIDER.
```

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

```
1. Financial assistance and government stimulus packages. This Phishing
   scheme played on the vulnerable demographics that were struggling
   financially during the pandemic. Mimicking financial institutions as
   well as government entities.
2. Impersonating medical organizations. This theme targeted people trying
   to stay up to date on important information regarding the pandemic. A
   much broader theme to target more people during the pandemic.
3. Targeting employees working from home. With the mass transition of
   employees working from home this was an easy target. Many employees
   would not be well educated on the potential for Phishing.
```

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

```
CrowdStrike Intelligence identified that the industrial and engineering
sector was the most targeted industry with 229 incidents. Followed by the
manufacturing sector with 228 incidents.
```

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

```
WICKED PANDA is a cyber threat group that originates from the People's
Republic of China. They targeted telecommunications companies, the
government, as well as the technology and healthcare sectors.
```

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

```
The first actor observed extorting data from ransomware campaigns was BOSS
SPIDER in January 2016.
```

6. What is an access broker?

```
An access broker is a threat actor that has obtained access to the backend
of an organization. The broker will then take this information and sell it
through private channels or criminal forums. Access brokers can sell a
variety of services ranging from, escalating someone's privilege to give
them full access to a site; to selling logs, screenshots, or access point
information.
```

7. Explain a credential-based attack.

```
A credential-based attack is the use of stolen credentials to authenticate
applications and steal data. Once the credentials have been stolen and sold
the attacks against the company are very hard to identify since there can be
little done to validate who is actually using the credentials, making all
attacks insider attacks.
```

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

```
TWISTED SPIDER is credited with being a catalyst to the mass adoption of
data extortion using their Maze and Egregor ransomwares.
```

9. What is a DLS?

```
A DLS is a Dedicated Leak Site, which makes leaked information easily
accessible to the public. This information can be used by other threat
actors that can leverage the data to aid in other attacks.
```

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

```
eCrime accounted for 79% of all attributable intrusions in 2020.
```

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

```
WIZARD SPIDER was the most active reported adversary of 2020.
```

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

```
Both SPRITE and CARBON SPIDER targeted Linux systems running ESXi hosts.
Though uncommonly targeted, the ESXi system runs on dedicated hardware and
manages multiple VMs. So by attacking this vulnerable point they were able
to encrypt lots of systems with relatively little effort, having the same
effect as individually encrypting each VM. Due to the use of an
unconventional operating system the companies hosting ESXi lacked any
endpoint protection that could prevent the attack.
```

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

```
An Enabler provides criminal actors with capabilities that they might not
have access to. These actors sell delivery mechanisms, network exploits, and
malware-as-a-service operations. Many actors work with or purchase from
other actors to increase the success of their own campaigns.
```

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

```
1. Services. Many actors acquire access to tools and technology by
   establishing relationships within the eCrime ecosystem.
```

```
2. Distribution. The distribution of Phishing schemes, Malware, or other
   forms of spam messaging to mass targets.
3. Monetization. Turning a profit from the exploits used. Examples may
   include: money laundering, wire fraud, ransom payments and extortion.
```

15. What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?

```
The malicious code dubbed SUNBURST was used to collect information and
exploit SolarWinds Orion systems.
```

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?

```
According to the survey taken by Akamai in collaboration with DreamHack, the
most vulnerable and targeted element of the gaming industry was the players
themselves.
```

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

```
On May 14, 2020 the financial services industry encountered 47,698,955
attacks via web application attacks.
```

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

```
According to Akamai more than 60% of the Phishing kits monitored were only
active for 20 days or less.
```

4. What is credential stuffing?

```
Credential stuffing is the use of leaked login credentials from past data breaches to gain access to different sites that might use the same leaked credentials. Ex: If Website A’s data is leaked and sold on the darknet, then an attacker can use that data on Website B to attempt to gain access.
```

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

```
According to Akamai's State of the Internet Security Report 55% of frequent players say that they have had an account compromised. 20% of frequent players state that they are worried about having their accounts compromised.
```

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

```
The three-question quiz is a phishing scam that tricks a victim into sharing personal information by impersonating a reputable brand, company or government entity. They have you answer three basic questions while using scripts to steal your personal data and use it for other purposes. They also require users to share the quiz on social media platforms or through other outlets leading to the quizzes spreading rapidly.
```

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

```
Prolexic directs network traffic to scrubbing centers where they deploy proactive and custom mitigation controls to stop attacks. Clean traffic is then directed back to the origin, and DDoS traffic is scrubbed and stopped.
```

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

```
August 17, 2020 was the peak for Daily Credential Abuse Attempts with 365,181,101
```

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

```
On July 11, 2020 there was 14,631,618 attacks associated with daily web application attacks
```

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

```
On August 20, 2020 the media sector experienced 5,150,760 attacks via web application attacks.
```

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?

```
Verizon defined an incident as “A security event that compromises the integrity, confidentiality or availability of an information asset”
Verizon defined a breach as “An incident that results in the confirmed disclosure of data to an unauthorized party”
```

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

```
Verizon estimated that just under 80% of breaches occurred from outside actors, while just over 20% of breaches were perpetrated by internal actors.
```

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

```
Verizon gathered that roughly 80% of breaches were caused by organized crime groups.
```

4. What percentage of breaches were financially motivated?

```
Roughly 70% of breaches were 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. Includes both network and application layer attacks”

Command control: When an actor inflitrates a system and installs malware allowing them to remotely send commands from a server to infected devices.

Backdoor:A malware that negates the authentication procedures to access a system, resulting in remote access to the system.

Keylogger: A type of malware or hardware that records and stores the keystrokes of the infected device.

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

The most sought after data type for hackers was credentials at just under 60%.

7. What was the percentage of breaches involving phishing?

Verizon estimated that up to 36% of breaches involved phishing.