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 ransomware families that impacted the healthcare industry in
2020 were Twisted Spider using Maze and Wizard Spider using Conti.
```

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

The Pandemic was a golden opportunity for the attackers to gain access by impersonating as a health care provider or sending COVID-19 related hyperlinks and many other schemes to trap an innocent victim.

Here are the three different Pandemic-related eCrime Phishing themes out of many.

1. **Financial assistance and government stimulus packages**
    - The scam came into action as many governments throughout the world declared several COVID-19 related Aid and Relief acts. The perpetrators taking advantage of this, started sending emails and text messages luring the citizens and tricking them in providing their personal information and bank details.

2. **Scams offering personal protective equipment (PPE)**
    - From the beginning there was a huge rising demand for medical equipment such as PPE kits, N95 masks, gloves etc, and with that the scam and phishing also continued to rise. This shortage lured many examples of selling fraudulent products, used products, scamming the customers and even charging an illegal price.
    - There were multiple instances where hospitals, companies and individual societies paid millions of dollars for all safety equipment which unfortunately ended up being a scam or receiving unsafe products to use.

3. **Impersonation of medical bodies, including the World Health Organization (WHO) and U.S.Centers for Disease Control and Prevention (CDC)**
    - Along with many tactics of exploiting the vulnerabilities of individuals during the COVID-19, the scammers and hackers also took advantage of different organization’s names such as WHO and CDC. The perpetrator impersonates an employee of such a prestigious organization and sends emails, text messages and makes phone calls asking for their personal information or making them click on malicious links which will eventually give

them the victim’s username and password of bank account logins and other sensitive information.

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

The highest number of ransomware-associated data extortion operations were recorded in the Industrial and Engineering sector with 229 incidents being reported.

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

Wicked Panda originated from China and is also known as Axiom, Winnti, APT41 and Bronze Atlas. It is known as one of the sophisticated cyber threat group which act in accordance with Chinese Ministry of State Security (MSS) and the People's Liberation Army (PLA)

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

The Outlaw Spider was first observed using data extortion in a ransomware campaign.

6. What is an access broker?

Access broker is a one of many threat actors that will obtain the backend access to different corporations and government entities, which will be then sold via criminal forums or through various private channels.After purchasing such access it becomes very easy for the hackers to gain access of the victim’s database as the requirement of spending time in aiming the target and compromising its securities will be eliminated.

7. Explain a credential-based attack.

A credential-based attack occurs when the attackers will successfully have the credentials to make an entrance, bypassing the security measures placed by an organization to get a hold of the critical data.

```
The credential-based attack will begin by exploiting the remote services. Once the attacker will be able to have the credentials, it will be sold for future Brute Force attacks, password spraying, credential stuffing and other similar attacks.
```

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

```
The Twisted Spider, operators of Maze and Egregor ransomware were credited for the heavy adoption of data extortion in ransomware campaigns.
```

9. What is a DLS?

```
DLS stands for Dedicated Leak Sites or Data Leak sites. The DLS usually are the pages on the dark web where the attackers will post the names of the victims and additional details. Often the attackers also disclose certain details regarding the attack that has either already taken place or is going to, in order to prove to the audience that they successfully harvested the data from the target’s platform. Additionally, if the victims refuse to pay the ransom, the hackers may also publish the whole stolen data on the same dark web.
```

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

```
As per Crowdstrike Falcon OverWatch, 79% of intrusions came from eCrime intrusions in 2020.
```

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.

```
The Defray777 operated SPRITE SPIDER and the DarkSide operated CARBON SPIDER,  deployed from their individual ransomware families Linux versions
```

```
on ESXi hosts. These versions were deployed during the BGH operations, which
never targeted Linux and especially ESXi.

The hypervisor ESXi runs on a firm hardware and governs collective Virtual
Machines. This became increasingly a very effective target against the
victims for ransomware operators as many organizations began to migrate to
virtualization solutions to synthesize legacy IT systems.
```

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

```
An Enabler plays a very crucial part in the eCrime ecosystem. An Enabler
provides capabilities to the criminal actors which they cannot access to
otherwise. They sell the initial access to different criminal actors  by
running malware-as-a-service operations in order to specialize in delivery
mechanisms or network exploitation.
```

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

```
The three parts of the eCrime ecosystem that CrowdStrike highlighted in
their report are 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?

```
The name of the malicious code used to exploit a vulnerability in the
solarWinds Orion IT management software was 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 most vulnerable and targeted element of the gaming industry between October 2019 to September 2020 were the players indeed.
```

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

```
The month of December in the year 2019, recorded the highest numbers of daily web application attacks that took place between October 2019 to September 2020.
```

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

```
Over 60% of all the phishing kits were active for only 20 days or less which was monitored by Akamai.
```

4. What is credential stuffing?

```
A credential stuffing is one of many types of cyber attack, where the hacker will attempt to log in on a service with the credentials obtained from a data leak of a totally different service.
```

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

```
Over 50% of the frequent players had their accounts taken over and only 20% of the players were worried about it.
```

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

```
The three-question quiz phishing attack will provide the users with a quiz to finish in exchange for a “prize”, which will eventually lead to the victim’s information being stolen.
```

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

```
The Prolexic Routed defends organizations against DDoS attacks by
redirecting the network traffic through Akamai scrubbing centers where the
proactive mitigation controls are established which will detect and halt the
attack immediately and will only allow the clean traffic to move forward.
```

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

```
The highest Daily Logins associated with Daily Credential Abuse Attempts
between October 2019 to September 2020 was recorded on August 17, 2020 with
365,181,101 number of logins.
```

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

```
The highest gaming attacks associated with Daily Web Application Attacks
between October 2019 to September 2020 was recorded on July 11, 2020 with
14,631,618 number of attacks.
```

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

```
The highest media attacks associated with Daily Web Application Attacks
between October 2019 to September 2020 was recorded on August 20, 2020 with
5,150,760 number of 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?

```
The difference between an incident and a breach is that an incident is a
warning to a potential breach and points towards any activity that
```

compromises one's security. While a breach is a confirmation of the protected data being leaked or stolen.

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

The outside actors perpetrated about 74% of the breaches and the internal actors perpetrated around 28% of the breaches.

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

The organized crimes perpetrated about 80% of the breaches.

4. What percentage of breaches were financially motivated?

About 81% of the breaches were financially motivated.

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

Denial of service: The main intention of this type of attack is to compromise the systems and network by sending traffic or information towards it, which will eventually crash and shut down, becoming inaccessible to the users.

Command control: A command-and-control is a type of server which the attacker will control via a computer to send commands to receive stolen data from a malware compromised system

Backdoor: A backdoor can also be called a potential security risk as a backdoor is a way of bypassing all the security products, algorithm, authentication etc and gaining access to a computer system.

Keylogger: It is a tool which records what an individual is typing on their device. There are many uses for this tool in a malicious way to conduct an attack where the Keylogger software will send the hacker all the recordings of the typing and keystroke of the victim’s keyboard.

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

```
Credentials remain one of the most sought-after data types for hackers.
```

7. What was the percentage of breaches involving phishing?

```
About 37% of the breaches involved phishing.
```