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 most dominant family that impacted the healthcare industry is known as Maze. An infection count of 20 shows how dangerous they truly are.

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

Scams offering Personal Protective equipment could include Covid related scams. The theme of Financial assistance could be used against those struggling due to the pandemic. Alongside passing the mention of Covid within previously used Phishing lure content.

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

The Industials and Engineering Industry was affected the most by ransomware-associated data extortion operations. At a very close second place is Manufacturing which was only off by a slight margin.

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

Wicked panda began in 2020 “conducting a wide-ranging campaign focused on exploiting multiple vulnerabilities”. They have a large portfolio of targets including but not limited to Academics, Manufacturing, Government, Technology, etc.

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

It’s stated that OUTLAW SPIDER was the first to employ data extortion back in May of 2019.

6. What is an access broker?

An access broker is a threat actor that has gained backend access through multiple organizations. They then go on to sell this information to private parties or forums.

7. Explain a credential-based attack.

Typically The information thiefs logs content would hold their login credentials. Attackers would use information to try and steal important information.

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

A group known as WIZARD SPIDER is credited as they were credited the most reported criminal adversary for the second year in a row.

9. What is a DLS?

A DLS is a Dedicated Leak Site associated with specific ransomware families. DLS is a rather newer method compared to the data extortion technique.

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

In quarter 1 of 2020 the percentage shot up over 300% and declined near the second quarter. During the beginning of the third and fourth quarters intrusions shot up over 400%.

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

The most reported criminal adversary in 2020 was TWISTED SPIDER with over 500 dedicated leak sites.

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

By deploying Linux versions of ransomware to ESXi hosts they can successfully damage multiple servers with a swift act. Leading to quicker operations.That alongside the fact that ESXi hosts are vulnerable to ransomware attacks.

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

They are in my opinion the brains behind things. They bring along with them resources that alongside a criminal actor could be used to deal irreversible damage.

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

The first part is called services, where one sells services or data. The second part is called Distribution, and it is the networking side where you send emails or “exploit kits”. The third part is monetization, which includes Money Laundering and Cryptocurrency.

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 code was Sunburst. The attack occurred on march 26th.

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 targeted element are the players due to more than half of them have had accounts compromised.

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

The Most daily web application attacks occurred on December 09, 2019. They came to a total of 46,961,855 attacks in just december.

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

It is stated that more than 60% of all phishing kits were active. Showing how fast they go through them.

4. What is credential stuffing?

Hackers will gain users' credentials and attempt to use the same credentials on different platforms. If you have the same password for multiple accounts then you risk becoming a victim to 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?

55 Million players experienced attacks on their accounts.Most players are worried as when new games come out they are at risk.

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

An attack on the user used to get credentials by using 3 questions related to the website.

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

Prolexic Routed uses Akamai scrubbing centers to allow only clean network traffic through. Experts in akamai also conduct live analysis of the traffic to make sure everything is running smoothly,

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

There were 365,181,101 Daily Credential Abuse Attempts on August 17th, 2020. That is the highest number I've seen in that area and I assume it will continue to increase.

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

On December 9th, 2019 there were 94,982,919 web applications attacks. That number has been the highest projected number of attacks in 12 months.

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 occurred on August 20th, 2020. 5,150,760 attacks towards media occured on that day.

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 while compromising the asset, still holds data. While a breach is the exposure and disclosure of an asset.

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

The percentage of breaches done by external actors in 2020 is just under 80%. Internal actors projections are dropping roughly under 30% nearing the 20% mark.

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

More than 80% of breaches were perpetrated by organized crime. I will assume projections will continue to stay at number 1 as organized crime is everywhere.

4. What percentage of breaches were financially motivated?

More than 75% of breaches were financially motivated in 2020. Increasing dramatically from 2018, I'd say that projections will continue to increase.

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

Denial of service: an attack with the motive of denying the user access to their machine.

Command control:A computer used by an attacker to send and receive compromised information to target networks.

Backdoor: access point where one can go undetected.

Keylogger: A program that tracks all of your keystrokes on your computer.

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

With over 40% betnet breaches i think that the information type data hackers are most sought after.

7. What was the percentage of breaches involving phishing?

```
The percentage of breaches that involve phishing is just under 40%. I’d
guess that it was around 35%.
```

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.