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?

Twisted Spider

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

One of the themes related to the pandemic is called “Labyrinth Chollima.” This focused on companies that were releasing Covid-19 vaccines and tried to enter U.S. based health care providers. The second theme originated in China and is called “Pirate Panda.” A China-nexus actor stole information about the Covid-19 vaccine. One of the last themes is “Ocean Buffalo” and came from Vietnam. The attack was focused on getting information regarding Covid-19 itself. Attacking was meant for Wuhan and was mainly spear phishing attacks.

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

Healthcare Industry

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

WICKED PANDA originated from China and focused on figuring out vulnerabilities and from that they were able to send out other attacks that further interacted with the victims

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 sell information regarding corporate and government agencies. This allows the attacker to spend less time gathering the data needed and they can just attack.

7. Explain a credential-based attack.

Credential-based attacks are brute force attacks or credential stuffing. These allow the attacker to easily input the stolen username or password or just keep guessing the information until they get it correct.

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

Twisted Spider

9. What is a DLS?

A DLS is a dedicated leak site which allows the attacker to have access to users personal information

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?

Wicked Spider

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

They were able to deploy an attack that didn’t require as much effort due to being able to attack multiple virtual machines with a single attack.

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

Enablers play a very important role because they give criminals easy access to servers and tools that they wouldn’t otherwise be able to get quickly.

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?

DDos Attacks

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?

60%

4. What is credential stuffing?

Automatically inputting a stolen username and password to gain access to a website

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 been compromised and only about 1/5th of them are worried

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

An attack that has the users answer three questions about a certain brand and allows the user to give out vital information

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

Redirects information through scrubbing centers and only allowing the clean data to go through the network

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?

A breach is gaining unautherized access to data and an incident is a violation to a companies security policy

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

About 70% of the breaches were done by outside actors and about 20% of breaches were done by internal actors.

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

About 80% of the breaches were done by organized crime

4. What percentage of breaches were financially motivated?

91% of the breaches were financially motivated

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

Denial of service: preventing users unauthorized access

Command control:allows hackers to remotely install malware using commands

Backdoor:goes against the normal way of accessing a system

Keylogger:recording every key pushed by a user to gain access to personal accounts

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

Credentials

7. What was the percentage of breaches involving phishing?

About 70%