Cybersecurity Boot Camp

Security 101 Challenge

Cybersecurity Threat Landscape

Part 1: 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 on):

---

1. What was the dominant ransomware family that impacted the healthcare industry in 2020?

“Maze”

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

- “Exploitation” of those looking for “disease” healthcare information
    - Those wanting to find information on treatments, disease spread, and testing may happen upon a malicious source.
- “Financial assistance and government stimulus packages”
    - Those impacted financially may seek out official financial help, but may end up the target of a malicious phishing email. This may target less computer literate people.
- Reusing old phishing links, whilst rebranding them to include mentions of COVID-19 to entice clicks to malicious websites.

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

The “Industrial and Engineering sector” had the most attack, followed by “Manufacturing.”

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

A China-based hacking group that targeted multiple companies in the videogame industry.

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

“Outlaw Spider”

6. What is an access broker?

A person who sells access (there is a variety of access levels that they provide) to the “backend” of a corporation's data. They don’t exfiltrate the data, all they do is sell the access to someone who is interested in using/selling the data.

7. Explain a credential-based attack.

Gaining access to the backend of a system, and gaining login/credential information. This is a loop, where these credentials can be used to gain more credentials, if the system is not properly secured after the attack.

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

Twisted spider & Wizard spider

9. What is a DLS?

“Dedicated leak-site”

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

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

They started targeting the structure that manages the VMs, which allows them to encrypt more machines and data with less input. This type of attack is currently harder to detect than previous methods.

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

Selling access to tools, which *Enables* cybercriminals to better attack vulnerable targets

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

1.Trends and Techniques
2. WIZARD SPIDER Targets Financial Institution
3. eCrime Enablers

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 and September 2020?

Account stealing/credential abuse. It wasn’t very clear, but I had an educated guess.

2. From October 2019 to September 2020, in 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?

An automated, brute-force, attack that attempts to reuse compromised passwords on websites.

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

Of the players asked in the survey, 50% said their accounts were compromised, but only 20% were ever worried.

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

A quiz imitating an entity, which has a user answer 3 questions. It then gives them a “prize” (regardless of the answers given) then redirects the users to a website prompting for input of personal information.

7. Explain how Prolexic Routed defends organizations against Distributed Denial of Service (DDoS) attacks.

A third-party company that monitors the incoming traffic, which scrubs suspicious traffic based on IP addresses and other data.

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

August 17th

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

July 11th. The graph shown was not entirely clear on conveying the information from the chart.

10. Which 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?

An incident is an event that could compromise data within the CIA triad. A breach (is an incident) in which data has “confirmed disclosure” to a third party.

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

20-30%

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

80%

4. In 2020, what percent of breaches were financially motivated?

Greater than 90%

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

Denial of service:
Flooding an asset with bot traffic, preventing legitimate users from accessing a site.
Command control:
A chain reaction of malware that infects multiple devices. This allows an outside actor to remotely control actions on each device infected.
Backdoor:
An accidental, sometimes purposeful, entry which circumvents the security of a system. Backdoors are obfuscated to prevent widespread access, but this doesn't always work.
Keylogger:
Malware that logs the input from keyboards, or other user-input devices. This allows bad-actors to potentially see sensitive information, like passwords and logins.

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

Financial data

7. What was the percentage of breaches that involved phishing?

25% of breaches were from phishing.