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.

Financial assistance and government stimulus packages; Tailored attacks against employees working from home; & Scams offering PPE.

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

Industrial and Engineering

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

WICKED PANDA is one of the adversaries tracked by CrowdStrike who targets multiple industries and vulnerabilities. According to crowdstrike.com, they

```
have shifted from criminally focused operations to state sponsored attacks
aligned with the CCP. They originate from China.
```

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 are threat actors that gain backend access and sell that
access.
```

7. Explain a credential-based attack.

```
A credential-based attack is when someone steals credentials to gain access
to an organization. Credentials can be used in multiple ways, to obtain
sensitive info, or to initiate additional attacks.
```

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. Most stagger the release of stolen data in
differing methods. Each release can trigger renewed reporting which can
increase pressure on the victim to pay ransom as well as create negative
publicity.
```

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.

Both SPRITE SPIDER and CARBON SPIDER deployed Linux versions of their ransomware families on ESKi hosts during BGH (Big Game Hunter) operations. Historically, Linux (ESXi specifically) systems have not been targeted by these. This has identified an exploit that could be used to encrypt multiple systems w/ relatively few actual deployments. Because they are not conventional operating systems, ESXi hosts lack endpoint protection software that could prevent/detect ransomware attacks.

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

Enablers run malware-as-a-service operations, specialize in delivery mechanisms or exploit networks in order to sell initial access to other criminal actors.

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?

SUNSPOT - A monitoring tool that detects the beginning of an Orion package build and replaces one of the source code files w/ a backdoored version.

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?

Its players

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

December 2019

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

60%

4. What is credential stuffing?

Credential stuffing is using compromised credentials to gain access to a protected account. It is based on people reusing usernames and passwords across different platforms.

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 of the players have reported having their accounts compromised. One fifth of players were worried about it.

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

A three-question quiz phishing attack is when an attacker uses a survey with three questions related to the alleged represented brand and the target “wins” a prize based on their answers and then enter their information.

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

```
Prolexic Routed defends organizations against DDos attacks by redirecting
network traffic through Akamai scrubbing centers and only allowing the clean
traffic forward.
```

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

```
August 17, 2020
```

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

```
July 11, 2020
```

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

```
August 20, 2020
```

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 a security event that compromises the integrity,
confidentiality, or availability of an information asset. A breach is an
incident that results in confirmed disclosure (not just potential exposure)
of data to an unauthorized party.
```

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

Approximately 80% of breaches were perpetrated by outside actors. Approximately 20% of breaches were perpetrated by internal actors. (Figure 14)

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

Approximately 80% (Figure 16)

4. What percentage of breaches were financially motivated?

Approximately 70-75% (Figure 18)

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. The most common pattern across incidents, but one of the easiest threats to mitigate.

Command control: A type of attack that uses a tool/program to communicate and control a compromised system or network.

Backdoor: Malware that goes around usual authentication in order to access a system or network.

Keylogger: A program that records all keystrokes typed into a machine. Usually used to obtain passwords or other access credentials.

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

Credentials (Figure 35)

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

36%