| 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?

| Maze was the dominant ransomware family that impacted the healthcare industry in 2020. |
| --- |

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

| Exploitation of individuals looking for details on disease tracking, testing and treatments.  The attack takes advantage of the victims' fears and emotions. They can then trick the victims into clicking or subscribing to a false website to gather personal data.  Financial assistance and government stimulus package.  Scams victims into giving away personal information in hopes to receive money from governments. Once the attacker has the information, they will then perform a spear phishing attack to get more information to cause more damage.  Tailor attacks against employees working from home.  Scams victims into giving away business sensitive information. This allows the attackers to have access to the business. |
| --- |

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

| The industrial and engineering sector was targeted with the highest number of ransomware and data extortion operations. |
| --- |

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

| WICKED PANDA is a China based hacker group. |
| --- |

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

| Viking Spider were the first to be identified in December of 2019. |
| --- |

1. What is an access broker?

| Criminal groups that sell illegitimate access to corporate networks. |
| --- |

1. Explain a credential-based attack.

| A credential-based attack happens when an attacker steals information that allows them to bypass an organization's security measures and steals data from the server. |
| --- |

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

| Twisted Spider was credited for the heavy adoption of data extortion and ransomware campaigns. The operator of Maze and Egregor ransomware. |
| --- |

1. What is a DLS?

| DLS stands for dedicated leak site. |
| --- |

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

| ECrime intrusions made up 79% of all attributable intrusion uncovered by OverWatch in 2020. |
| --- |

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

| Wizard Spider was the most reported criminal adversary of 2020. |
| --- |

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

| They deployed Linux versions of their ransomware onto the ESXi host. ESXi is a hypervisor used to run virtual machines. Since this host ran multiple machines they were able to gather a large amount of data. |
| --- |

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

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

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

| The three part are listed as followed:   * Trends and Techniques * OverWatch Features: WIZARD SPIDER Targets Financial Institution * ECrime Enablers |
| --- |

1. 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 was dubbed 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 target element of the gaming industry are its gamers. |
| --- |

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

| December 09, 2019 was the month with the highest web application attacks on the financial services. |
| --- |

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

| 60% of all the phishing kits monitored by Akamai were active for only 20 days. |
| --- |

1. What is credential stuffing?

| Credential stuffing attack is a kind of brute force attack. The attacker will use a list of stolen credentials collected to breach a system. |
| --- |

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

| Approximately 50% of gaming industry players experienced accounts compromised but only 5% are worried about the issue. |
| --- |

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

| The three-question phishing attack scams the players into filling out quizzes which results in stolen credentials. |
| --- |

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

| The Prolexic Routed defends the organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing center, and only allowing the clean traffic forward. |
| --- |

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

| August 17, 2020 had the highest Daily Logins associated with Daily Credential Abuse Attempts. |
| --- |

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

| July 11, 2020 had the highest gaming attack associated with Daily Web Application Attacks. |
| --- |

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

| August 20, 2020 had the highest media attacks associated with Daily Web Application 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?

| A security incident is when an attacker tries to enter the systems using malware or other illegal methods. There could also be malware in the system already but it will still be considered an incident. A security breach is the moment the attacker successfully damages the system. |
| --- |

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

| The percentage of breaches perpetrated by outside attackers were 87%.  The percentage of breaches perpetrated internally were 17%. |
| --- |

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

| 80% of breaches were perpetrated by organized crime. |
| --- |

1. What percentage of breaches were financially motivated?

| Financially motivated attacks make up almost 86% - 100% of all breaches. |
| --- |

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

| **Denial of service**:  A cyber attack that caused a website or network to crash or make it unavailable to use. Two examples are flooding service and crashing services  **Command control**:  Controls infected machines from a malicious remote server. Once the victim’s machine is compromised the attacker has complete controls of the computer.  **Backdoor**:  An access point created in the system after an attack that allows the users continuous access.  **Keylogger**:  A malware that tracks the victims keystrokes and sends the data collected to the attacker’s server. |
| --- |

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

| Credentials remain one of the most sought-after data types. |
| --- |

1. What was the percentage of breaches involving phishing?

| Breaches involving phishing remained in the region of 25%. |
| --- |

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