| 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 |
| --- |

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

| Impersonation of medical bodies, financial assistance and government stimulus packages, tailored attacks against employees working from home. |
| --- |

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

| Industrial and engineering sector |
| --- |

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

| A criminal adversary originating in China |
| --- |

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

| Outlaw Spider |
| --- |

1. What is an access broker?

| Threat actors that gain access to organizations or government entities and then sell that access. |
| --- |

1. Explain a credential-based attack.

| When an attacker(s) steal credentials to gain access or bypass security measures in order to steal critical data. |
| --- |

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

| Twisted Spider |
| --- |

1. What is a DLS?

| A dedicated leak site |
| --- |

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

| 79% |
| --- |

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

| Wizard Spider |
| --- |

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

| By deploying Linux versions of their respective ransomware families on ESXi hosts. Specifically targeting VM’s. |
| --- |

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

| Provides criminal actors with capabilities they may not have access to otherwise. i.e. Malware-as-a-service |
| --- |

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

| Services, Distribution, Monetization |
| --- |

1. 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 |
| --- |

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

| May 2020 |
| --- |

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

| 60% |
| --- |

1. What is credential stuffing?

| A method of cyberattack utilizing lists of compromised user credentials 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?

| More then half had been compromised, but only one-fifth were worried about it. |
| --- |

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

| Relies on users filling out a quiz in exchange for a prize. |
| --- |

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

| By redirecting network traffic through an Akamai scrubbing center and only forwarding clean traffic. |
| --- |

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

| August 17, 2020 |
| --- |

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

| July 11, 2020 |
| --- |

1. What 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 precursor to a breach. Could refer to any activity that compromises security. |
| --- |

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

| 70% External, 30% Internal |
| --- |

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

| 55% |
| --- |

1. What percentage of breaches were financially motivated?

| 71% |
| --- |

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

| **Denial of service**: An attack utilized to shutdown a machine or network, making it inaccessible  **Command control**: Used by attackers to retain communications with compromised systems within a target network.  **Backdoor**: Malware that allows access to a computer.  **Keylogger**: Activity monitoring software program that allows hackers to gain PII. |
| --- |

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

| Credentials |
| --- |

1. What was the percentage of breaches involving phishing?

| 25% |
| --- |

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