|  |
| --- |
| 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, followed closely by Conti |
|  |

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

|  |
| --- |
| Disease Tracking, Testing & Treatment  Impersonation of medical bodies (WHO, CDC etc)  Financial assistance or government stimulus measures |

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

|  |
| --- |
| Industrials & Engineering / Manufacturing |

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

|  |
| --- |
| Wicked Panda has been one of the most prolific and effective hacking groups since the mid 2010’s, based out of China.  They shift between criminally focused operations to state-sponsored targeted intrusions that align with Chinese communist party objectives. |

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

|  |
| --- |
| OUTLAW SPIDER was first observed using data extortion in ransomware as early as 2019, though more commonly seen in 2020 by Twisted Spider. |

1. **What is an access broker?**

|  |
| --- |
| An Inital Access Broker (IAB) is a threat actor that sells a suite of associated access credentials that are bundled up with an appropriate VPS/VPN and usually include RPC credentials. |

1. **Explain a credential-based attack.**

|  |
| --- |
| Credential stuffing, an example of credential-based attacks, involves using lists of credentials typically found from data leaks – and brute-forcing access to any account – note: the difference between normal brute-forcing and standard credential stuffing, is that the attacker is not attempting to brute-force access to a particular account, but rather access to any account in general. |

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

|  |
| --- |
| TWISTED SPIDER — operators of Maze and Egregor ransomware — has been credited with being the catalyst for the heavy adoption of this technique in 2020. |

1. **What is a DLS?**

|  |
| --- |
| A DLS is a dedicated leak site – a site exclusively used for the purpose of data leaks. The most well-known was and still is undoubtedly WikiLeaks. |

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

|  |
| --- |
| According to CrowdStrike – in 2020 eCrime accounted for 79% of all intrusions detected, with 21% from targeted intrusions occurring. |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

1. **What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?**

|  |
| --- |
| [Enter answer here] |

### 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?**

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

1. **What is credential stuffing?**

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

### 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?**

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| [Enter answer here] |

1. **What percentage of breaches were financially motivated?**

|  |
| --- |
| [Enter answer here] |

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

|  |
| --- |
| **Denial of service**:  **Command control**:  **Backdoor**:  **Keylogger**: |

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

|  |
| --- |
| [Enter answer here] |

1. **What was the percentage of breaches involving phishing?**

|  |
| --- |
| [Enter answer here] |

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