| 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 (specifically the TWISTED SPIDER with at least 20 infections (26 if we add Egregor)) followed by Conti (with their WIZARD SPIDER with 17 infections (25 if we add Ryuk)) |
| --- |

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

| Exploitation of individuals looking for details on disease tracking, testing and treatment  Impersonation of medical bodies, including the World Health Organization (WHO) and U.S.Centers for Disease Control and Prevention (CDC)  Financial assistance and government stimulus packages |
| --- |

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

| Industrials and Engineering |
| --- |
|  |
|  |

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

| WICKED PANDA is a cyber threat group from China that carries out state-sponsored espionage activities. However, they also have been known to do activities outside of state control for their own financial motivations. |
| --- |
|  |

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

| OUTLAW SPIDER first employed this tactic in May 2019. |
| --- |

1. What is an access broker?

| Access brokers are threat actors that gain backend access to various organizations and sell this access either on criminal forums or through private channels. |
| --- |

1. Explain a credential-based attack.

| A credential-based attack allows the threat to take on the personality of an individual who is authorized to access the system that the threat wants to access. |
| --- |

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

| TWISTED SPIDER |
| --- |
|  |

1. What is a DLS?

| Dedicated leak sites |
| --- |

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 infiltrating the systems which host the VM’s, they were able to gain access to and be able to encrypt the VM’s that are on those infrastructures.  As said in the article, “Encrypting one ESXi server inflicts the same amount of damage as individually deploying ransomware on each VM hosted on a given server. Consequently, targeting ESXi hosts can also improve the speed of BGH operations. Additionally, due to their lack of conventional operating systems, ESXi hosts lack endpoint protection software that could prevent or detect ransomware attacks.” |
| --- |

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

| They provide services and capabilities that others might not have access to, such as Malware-as-a-service, delivery mechanisms, or initial access information on exploited networks. |
| --- |

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?

| Players |
| --- |

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

| December 2019 |
| --- |

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

| More than 60% |
| --- |

1. What is credential stuffing?

| According to OWASP, credential stuffing is the automated injection of stolen username and password pairs into website login forms, in order to fraudulently gain access to user accounts. |
| --- |

1. 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 have had their accounts compromised, but only one fifth of them were worried about it. |
| --- |

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

| It is a quiz that offers a ‘prize’ after answering the questions, but in exchange results in stolen PII. |
| --- |

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

| Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, 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 with 365,181,101 logins |
| --- |

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

| July 11, 2020 with 14,631,618 gaming attacks |
| --- |

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

| August 20, 2020 with 5,150,760 media 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?

| Verizon describes an incident as a security event that compromises the integrity, confidentiality or availability of an information asset whereas a breach is the confirmed disclosure of data to an unauthorized party. |
| --- |

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

| 80ish% for external, 20ish% by internal |
| --- |

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

| 80ish% |
| --- |

1. What percentage of breaches were financially motivated?

| 95ish% |
| --- |

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

| **Denial of service**:According to Palo Alto, a Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.  **Command control**:If you mean Command and Control (C&C), then according to TrendMicro, a C&C server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.  **Backdoor**:This is a means by which someone (attacker, developer, user, etc) can gain access to a system without going through the proper security measures, typically with higher user level access.  **Keylogger**:This is a program that records every keystroke made by a user. |
| --- |

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

| Credentials |
| --- |

1. What was the percentage of breaches involving phishing?

| 36% |
| --- |

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