|  |
| --- |
| Cybersecurity Boot Camp |
| Security 101 Challenge |

## Cybersecurity Threat Landscape

## 

### Part I:

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.

|  |
| --- |
| 1. Exploitation of people looking for details on Covid disease 2. Actors pretending to be from WHO and CCD trying to get information. 3. Fake financial assistance and gov stimulus packages. |

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

|  |
| --- |
| In the Industrial and Engineering Sector. |

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

|  |
| --- |
| Wicked Panda is an adversary group from China that deals with espionage. They conduct wide range campaigns focused on citrix vulnerabilities (CVE-2019-19781) and Zoho remote code (CVE-2020-10189) they target Banking, healthcare and telecom. |

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

|  |
| --- |
| Outlaw spider |

1. What is an access broker?

|  |
| --- |
| Access brokers are actors that gain backend access and sell their access to criminal forums or through private channels. It eliminates time spent on gaining access. They can just focus on the monetary aspect. |

1. Explain a credential-based attack.

|  |
| --- |
| An actor will steal someone’s credentials to get into backoffice of business 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?

|  |
| --- |
| Dedicated Leak Sites are used by actors to publish stolen data |

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

|  |
| --- |
| eCrime intrusions made up of 79% of all intrusions uncovered by Overwatch 2020 (2021 Global Threat report-page 10) |

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

|  |
| --- |
| Wizard Spider |

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

|  |
| --- |
| They received leader capabilities to sign into the vCenter interface. Ransomware actors can then encode many structures within that machine. |

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

|  |
| --- |
| Enabler could be people working at the establishment and help the actors get into the network. They could be an organization as well. |

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

|  |
| --- |
| Wicked Panda Circuit Panda and Phantom panda |

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?

|  |
| --- |
| Its 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?

|  |
| --- |
| Credential stuffing is when people reuse their passwords and usernames and the criminals use bots to find those and use them to gain access. |

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 50% have had their accounts compromised, but only ⅕ of those care!! |

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

|  |
| --- |
| Its where the actors send out questions to have people answer in hopes to gain a prize. Actors will gain personal information. |

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

|  |
| --- |
| The tool helps to divert traffic to Akamai scrubbing centers, specialists in the SOC will stop assaults right away, before it happens. |

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

|  |
| --- |
| August 17 2020. Approx 365 Million |

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

|  |
| --- |
| Dec 24 2019 |

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

|  |
| --- |
| December 24 2019 |

### 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 an event that violates the company's security policies and puts the company's data at risk. Breach is when the CIA (confidentiality, INtegrity or Availability) of the data has been compromised. This requires the affected person to be notified. |

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

|  |
| --- |
| Roughly 69% outside and 34% internal |

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

|  |
| --- |
| 39% were perpetrated by organized crime. |

1. What percentage of breaches were financially motivated?

|  |
| --- |
| Roughly 71% |

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

|  |
| --- |
| **Denial of service**: It is a cyberattack where the perp seeks to make a machine or network unavailable by temporary or indefinitely disrupting service. They will flood the machine with requests.  **Command control**: is known as C2 and C&C, is very destructive as the perpetrator can go into systems unnoticed for espionage as they want to steal sensitive or secret information.  **Backdoor**:backdoor is a maleware that discredits verification techniques and allows actor access to assets. Backdoor is accomplished by exploiting weak parts in a web application.  **Keylogger**: a PC program recording every keystroke to obtain passwords and other sensitive data. |

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.