## **Cybersecurity Threat Landscape**

### **Part I: Crowdstrike 2021 Global Threat Report**

[CrowdStrike Global Threat Report (2021)Links to an external site.](https://drive.google.com/file/d/1t3cl2fU3Pp6I4_mwGX4W6D4qslFjdVSp/view?usp=sharing)

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 individuals looking for details on disease tracking, testing and treatment.” There was a lot of fraud and rumors around Covid 19. This gave hackers an opportunity to manipulate the information on websites that can fool the public or sway opinions.  2.”Impersonation of medical bodies, including the World Health Organization (WHO) and U.S.Centers for Disease Control and Prevention (CDC)” Scammers could impersonate these organizations giving the public false information on what is happening and how they should respond to the Pandemic.  3.”Financial assistance and government stimulus packages” There were several rounds of checks given by the government to the American people to help them with finances during the pandemic. This was perfect for hackers to step in to intercept the money. |

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?

|  |
| --- |
| WICKED PANDA is a the “most prolific adversaries trakced by CrowdStrike Intelligence.” It originated from China. |

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 threat actors that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels.” In other words, they are hackers that get into private systems to collect private data and sell it on the dark web. |

1. Explain a credential-based attack.

|  |
| --- |
| It is an attack to try to achieve a user’s login information by using brute force, password spraying, etc. |

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

|  |
| --- |
| TWISTED SPIDER |

1. What is a DLS?

|  |
| --- |
| DLS or Dedicated Leak Sites are sites dedicated to exposing login information to criminals. |

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.

|  |
| --- |
| They targeted Linux, specifically ESXi which was very unusual. SPRITE SPIDER was able to use login credentials and access the information using the vCenter web interface. |

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

|  |
| --- |
| Enablers run malware-as-a-service so they can share/sell other criminals different hacking methods. |

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

|  |
| --- |
| 1. Services 2. Distribution 3. 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**

[Akamai Security Year in Review (2020)Links to an external site.](https://drive.google.com/file/d/1HefXRqMudz5elB_seBDfXaoPhau1mdg5/view?usp=sharing)

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 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?

|  |
| --- |
| 60% |

1. What is credential stuffing?

|  |
| --- |
| Hackers use lists of user credentials bought on the dark web or stolen to break into a system. It is an example of a brute force attack. |

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

|  |
| --- |
| Half of the accounts were compromised but only a fifth were worried. |

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

|  |
| --- |
| They are fake quizzes or surveys that supposedly come with a reward for filling it out but usually just ends up stealing your information. |

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 |

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?

|  |
| --- |
| Aug 20, 2020 |

### **Part 3: Verizon Data Breaches Investigation Report**

[Verizon 2021 Data Breach Investigations ReportLinks to an external site.](https://drive.google.com/file/d/1t0dFuDqnta0YcJy3c95o5rXyVBFmBRqa/view?usp=sharing)

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 compromises any of the CIA Triad of an asset. A breach is an incident but it is confirmed that the data has been tampered with. |

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

|  |
| --- |
| Outside factors:about 85%  Internal Factors: about 15% |

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

|  |
| --- |
| 80% |

1. What percentage of breaches were financially motivated?

|  |
| --- |
| About 90% |

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

|  |
| --- |
| **Denial of service**: users cannot access their accounts on devices, websites, or any network  **Command control**:an attacker controlling your system and collecting info, compromising data, etc.  **Backdoor**: using technology to gain unauthorized access to a system  **Keylogger**: a form of spyware that tracks your keystrokes and clicks |

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

|  |
| --- |
| Credentials |

1. What was the percentage of breaches involving phishing?

|  |
| --- |
| 25% to 36% |