

## Cybersecurity Threat Landscape

### Part 1: 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 on):

1. What was the dominant ransomware family that impacted the healthcare industry in 2020?

| The most dominant ransomware family that impacted the healthcare industry in 2020 was the Spider family, with Wizard Spider and Twisted Spider using Conti and Maze. |
| --- |

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

| Three different pandemic-related eCrime Phishing themes include:   1. Financial assistance and government stimulus packages   -eCriminals could try to gain access to victims’ bank accounts and try to retrieve their stimulus money.   1. Tailored attacks against against employees working from home   -Phishers sent emails to employees working from home to try to catch someone being lazy and click links that they think they may need from work and do not have a superior around to readily ask for permission to click links.   1. Scams offering personal protective equipment   -They used fear as a tactic to possibly promote a sense of scarcity with these items. |
| --- |

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

| The industry with the highest number of ransomware-associated data extortion operations was the industrial and engineering industry. |
| --- |

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

| Wicked Panda is a cyber threat group that originates from China. |
| --- |

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

| The ransomware actor that was first observed using data extortion in a ransomware campaign was Outlaw Spider. |
| --- |

1. What is an access broker?

| Access brokers are the cyber threat actors that are able to act as a middleman for other criminals by accessing data and then selling that data to eCriminals for their benefit. |
| --- |

1. Explain a credential-based attack.

| A credential-based attack is a cyber attack in which a criminal can access the credentials to a user’s login, administrator logins, or information needed to login to a database, all while being able to avoid security. |
| --- |

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

| Twisted Spider is credited for the heavy adoption of data extortion in ransomware campaigns. |
| --- |

1. What is a DLS?

| D.L.S. stands for dedicated leak sites. These sites are the domains for criminals to share the sites that have been successfully hacked and confidential data that can be sold. |
| --- |

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

| Intrusions coming from eCrime intrusions in 2020 were at 400% at the end of the year, according to Crowdstrike Falcon Overwatch. |
| --- |

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

| Wizard Spider was the most reported criminal adversary in 2020. |
| --- |

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

| Sprite Spider and Carbon Spider impacted virtualization infrastructures by using ransomware on EXSI hosts that would enable them to gain access and infect numerous virtual machines at the same time. This made it easier for them to deploy one ransomware that could infect all of the VM’s instead of having to do it individually. By using administrator credentials, they were successful in gaining access. |
| --- |

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

| Enablers are the eCriminals that are using coding to assist the threat actors in gaining access into databases and networks that the actor may not have access to. They provide this service for profit. |
| --- |

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

| The three parts of the eCrime ecosystem that Crowdstrike highlights in their report include:   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?

| The name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software is 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 and September 2020?

| The most vulnerable and targeted element of the gaming industry between October 2019 and September 2020 was its players. |
| --- |

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

| From October 2019 to September 2020, December 2019 had the most daily web application attacks for the financial services industry. |
| --- |

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

| Phishing kits monitored by Akamai for only 20 days or less was at 60%. |
| --- |

1. What is credential stuffing?

| Credential stuffing is the practice of obtaining login credentials by means of a cyber attack to use for more than one service. Sometimes, users use the same login credentials for many different services and a cyber criminal may attempt to use those credentials for multiple logins. |
| --- |

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

| The majority of gaming industry frequent players have experienced their accounts being compromised. One fifth of players were actually worried about it. |
| --- |

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

| A three-question phishing attack is a tactic used by phishers by asking the user three simple questions within a pop-up for the website to trick them into clicking the link. These questions are often related to the current webpage to seem legitimate. |
| --- |

1. Explain how Prolexic Routed defends organizations against Distributed Denial of Service (DDoS) attacks.

| Prolexic Routed is a tool used to defend organizations against DDoS attacks by rerouting users through a network that only allows clean traffic to proceed and to stop bad traffic from entering into the network. |
| --- |

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

| August 17, 2020 had the highest Daily Logins associated with Daily Credential Abuse Attempts. |
| --- |

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

| July 11, 2020 had the highest gaming attacks associated with Daily Web Application Attacks. |
| --- |

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

| August 20, 2020 had the highest media attacks associated with Daily Web Application 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?

| An incident is when the confidentiality, availability, and integrity of an information asset has been endangered or threatened. A breach is a type of incident that results in the act of that information asset having been successfully obtained by the cyber criminal. |
| --- |

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

| Close to 80% Of breaches were perpetrated by outside actors. Close to 20% were perpetrated by internal actors. |
| --- |

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

| 80% of breaches were perpetrated by organized crime. |
| --- |

1. What percentage of breaches were financially motivated?

| About 70% of breaches were financially motivated. |
| --- |

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

| **Denial of service**: Attack designed to make a network unusable by shutting down the network or the machine that the network runs off of.  **Command control**: Attack that uses tools to access an infected network for a hacker to gain control over the network.  **Backdoor**: Tactic used by cyber criminals to gain access to networks without having to go through the main channel. The malware is linked to the network by a different mean that doesn’t need to be the main point of entry.  **Keylogger**: A tool used to monitor keystrokes and everything a user types into a computer. All of the activity is logged and can predict users’ tendencies. |
| --- |

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

| The most sought after data type for hackers are credentials. |
| --- |

1. What was the percentage of breaches that involved phishing?

| 36% of breaches involve phishing. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.