

## 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 BGH ransomware family that impacted the healthcare industry in 2020 was “Maze”. In 2020 TWISTED SPIDER (Russian Adversary Group) infected 26 healthcare sector victims. TWISTED SPIDER announced their intentions to avoid frontline healthcare groups, such as hospitals, however, instead focused on targeting Pharmaceutical and Biomedical companies. |
| --- |

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

| There are numerous pandemic-related eCrime Phishing themes. Three examples of these themes include; Impersonation of medical entities, such as the World Health Organisation (WHO), Disease COntrol Prevention Agencies, and U.S Government Bodies. Additional themes of eCrime Phishing Themes include specific attacks for remote employment, and luring emails featuring financial support and government stimulus packages. |
| --- |

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

| The most targeted industry of ransomware-associated data extortion operation identified by CrowdStrike was the Industrial and Engineering sector with approximately 229 recorded incidents. The Manufacturing industry shortly followed with 228 incidents. Manufacturing and Engineering are affected most as their core businesses are dependent on the day-to-day operations and meeting the production demands. |
| --- |

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

| WICKED PANDA is a Chinese adversary group that used the Citrix Application Delivery Controller (CVE-2019-19781) and Netclear and Nextitem functions buffer overflow (CVE-2020-10189) vulnerabilities, to deploy CobaltStrike and Meterpreter exploits onto victims machines. |
| --- |

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

| Data extortion is the kidnapping of a user or system’s sensitive data until the actor's demands are met. OUTLAW SPIDER was the first observed actor that used data extortion in a ransomware campaign. |
| --- |

1. What is an access broker?

| Access Brokers are threat actors which gain unauthorized access to the backend of Enterprises and Government Entities, enabling them to sell their access on criminal platforms. |
| --- |

1. Explain a credential-based attack.

| A Credential-Based Attack, is a threat actor that targets credential vulnerabilities of a user allowing a threat to gain unauthorized access into a user or admin account. Examples of credential-based attacks include; Bruteforcing (Automation and scripting to guess password & usernames), Password Spraying (Spraying an authentication server with common username and password combinations), and Credential Stuffing (using data breached user credentials from one service on another unrelated service). |
| --- |

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

| TWISTED SPIDER has been credited with launching the technique in 2020 after infecting 26 Healthcare sector victims. |
| --- |

1. What is a DLS?

| A Dedicated Leak Site (DLS) is a unique website where adversaries data dump illicitly retrieved sensitive data of companies who fail to meet the demands of the attacker. |
| --- |

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

| In 2020, CrowdStrike Falcon OverWatch identified 79% of all intrusions came from eCrime intrusions. |
| --- |

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

| WIZARD SPIDER, for the 2nd year in a row, became the most reported eCrime adversary in 2020. |
| --- |

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

| SPRITE SPIDER and CARBON SPIDER deployed Linux versions of their BGH ransomware families on ESXi hosts. ESXi is a hypervisor that allows Virtual Machines (VMs) to be a natural target for ransomware operators. More organizations are opting for virtualization solutions in efforts to consolidate old IT systems. |
| --- |

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

| ECrime enablers is the party that provides criminal actors with the opportunity to pose a risk to a system. Enablers provide the opportunity to threats that threats normally would not have access to. These Enablers run malware-as-a-service operations or exploit vulnerabilities on the system in an effort to sell access to criminal actors. |
| --- |

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

| The three parts of the eCrime ecosystem as described by CrowdStrike are Services, Distribution, and Monetization. |
| --- |

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

| The malicious code dubbed ‘SUNBURST’ was used to exploit a vulnerability in the SolarWinds Orion IT management software. |
| --- |

### 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 gamers were the most vulnerable and targeted entity. The human element was the hardest to control as people are prone to making mistakes in keeping themselves secure. |
| --- |

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

| The month with the most web application attacks in the financial services industry was December 2019 hitting approximately 46,961,855 attacks. |
| --- |

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

| More than 60% of all Phishing kits monitored by Akamai were active for 20 days or less. This therefore reinforces the rapid lifecycle of the kit. |
| --- |

1. What is credential stuffing?

| Credential Stuffing is the act of using illegitimately obtained login credentials from one service, and using the same combination of credentials to try to access an unrelated service. Attackers do this in bulk as the success rate can be quite high as users fail to update login credentials even after exposure. |
| --- |

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

| According to 2020: A YEar in Review: Volume 6, Issue 4, More than half of all gamers said they have experienced their gaming accounts being compromised, and only a fifth of the gamers are worried about their accounts. |
| --- |

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

| The three-question phishing attack was a malicious email that relied on targets to file out the three questions of a quiz, in an effort to win a prize. Revealing the prize will require the user to input their credentials opening the door to malicious attacks. |
| --- |

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

| Prolexic Routed defends against DDOS attacks by routing all network traffic through an Akamai scrubbing center, and only allowing filtered traffic inside the network. |
| --- |

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

| On August 17th 2020, the number of daily logins hit it’s peak at 365,181,101 credential abuse attempts. |
| --- |

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

| July 11th was the date that held the highest gaming attacks associated with Daily Web Applications. |
| --- |

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

| August 2020 was the date that held the media gaming attacks associated with Daily Web Applications. |
| --- |

### 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?

| A cybersecurity incident is defined as a security event in which it compromises the CIA Triad of the asset, that is, the Integrity, Confidentiality, and Availability. Whereas a breach is defined as an incident that results in the exposure and disclosure of sensitive data to an unauthorized actor. |
| --- |

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

| At the end of 2019, 44% of breaches were completed by Internal Actors, whereas, 56% of breaches were caused by External Actors. |
| --- |

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

| Approximately 80% of breaches reported in the Verizon Report were perpetrated by organized crime groups. |
| --- |

1. What percentage of breaches were financially motivated?

| Approximately 92% of breaches reported in the Verizon Report were financially motivated. |
| --- |

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

| **Denial of service**: An attack that aims to interrupt or render the systems of a business inaccessible, ultimately hindering the availability that company should offer.  **Command control**: An attack that allows malicious actors to gain unauthorized access to an infected machine or network. Common control is best described as the tools used to communicate machines to execute specific action inside a network.  **Backdoor**: A vulnerability allowing attackers the opportunity to gain unauthorized access into systems that are normally protected by security protocols.  **Keylogger**: An attacking tool that records every keystroke a victim may input into a machine allowing attackers to obtain potential passwords or credentials. |
| --- |

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

| A user’s credential login credentials are the most sought-after data type that attackers aim to acquire. This is because gaining access to a user’s account often reveals valuable sensitive information. |
| --- |

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

| In the Asian Pacific region 70% of all breaches were socially engineered targeted attacks. These attacks were primarily phishing, capturing 98% of affected victims' credentials. |
| --- |

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