

## 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 dominant ransomware family that impacted the healthcare industry in 2020 was Maze. (found on page 14 of Crowdstrike Report 2021) |
| --- |

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

| 1. Exploitation of individuals looking for details on disease tracking, testing, and treatment 2. Impersonation of medical bodies, including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC) 3. Financial assistance and government stimulus packages   (found on page 15 of Crowdstrike Report 2021) |
| --- |

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

| The industry targeted with the highest number of ransomware-associated data extortion operations was Industrials and Engineering.  (found on page 22 of Crowdstrike Report 2021) |
| --- |

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

| -”Chinese adversaries targeted telecommunications, with WICKED PANDA” (Found on Page 6 of Crowdstrike Report 2021)  -WICKED PANDA is from China and largely aligned with historic focuses on espionage, intellectual property theft, and surveillance in 2020. They focused on organizations in the telecommunications, government, healthcare and technology sectors (Found this on Page 35 of Crowdstrike Report 2021) |
| --- |

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

| OUTLAW SPIDER was the first observed ransomware actor that combined data extortion and ransomware tactics in May 2019. (Found this on Page 19 of Crowdstrike Report 2021) |
| --- |

1. What is an access broker?

| An access broker is a threat actor that gains backend access to organizations and government entities to sell this access either on criminal forums or through private channels. (Found this on Page 25 of Crowdstrike Report) |
| --- |

1. Explain a credential-based attack.

| A credential-based attack is brute forcing, password spraying, or credential stuffing.Credential-based attacks can be automated mechanisms and a self-sustaining process. (Found this on page 48 of Crowdstrike Report) |
| --- |

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

| TWISTED SPIDER has been credited with being the catalyst for the heavy adoption of data extortion in ransomware campaigns. They were the first ransomware actor to launch a DLS, which was created on Dec. 10, 2019.They would leak victim data in percentage increments. (Found this on Page 23 of Crowdstrike Report. |
| --- |

1. What is a DLS?

| DLS is a dedicated leak site, most commonly used by TWISTED SPIDER beginning in 2019.(Found this on Page 23 of Crowdstrike Report) |
| --- |

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

| According to Crowdstrike Falcon OverWatch, eCrime intrusions made up 79% of all attributable intrusions uncovered by OverWatch in 2020. (Found this on Page 10 of Crowdstrike Report) |
| --- |

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

| The most reported criminal adversary of 2020 was WIZARD SPIDER. “Their diverse and potent toolset makes this criminal group one of the most formidable adversaries in the current eCrime landscape” (Found this on Page 27 of Crowdstrike Report) |
| --- |

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

| SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures by deploying ransomware for linux in BGH operations targeting ESXi specifically which lack endpoint protection software that could prevent or detect ransomware attacks. (Found this on Page 26 of Crowdstrike Report) |
| --- |

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

| “Enablers are a pivotal part of the eCrime ecosystem, providing criminal actors with capabilities they may otherwise not have access to. These actors run malware-as-a-service operations.” (Found this on Page 30 of Crowdstrike Report) |
| --- |

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

| Three parts of the eCrime ecosystem in the Crowdstrike report that are highlighted are found in the table of contents: Trends and Techniques page 24, OverWatch Feature: WIZARD SPIDER Targets Financial Institution page 28, and eCrime Enablers page 30. (Found this on Table of Contents page of Crowdstrike Report) |
| --- |

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

| The malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software is known a SUNBURST (Found this on Page 16 of Crowdstrike Report) |
| --- |

### 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. The human element is always the hardest to control and secure.Through Web application attacks, credential abuse, and DDoS attacks. (Found on page 12, 15-16 of the Akamai Security Year in A Review) |
| --- |

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

| The majority of the attacks between October 2019 to September 2020 was in December of 2019 for Financial Services. (Found on page 5 of the Akamai Security Year in A Review) |
| --- |

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

| More than 60% of all the phishing kits monitored by akamai were active for only 20 days or less.(Found on page 3 of the Akamai Security Year in A Review |
| --- |

1. What is credential stuffing?

| Credential stuffing is the automated injection of stolen username and password pairs (“credentials”) into website login forms, in order to fraudulently gain access to user accounts. (found on this site: https://owasp.org/www-community/attacks/Credential\_stuffing) |
| --- |

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 of the frequent players said they’ve had their accounts compromised, but only one-fifth of them were worried about such things. (Found on page 12 of the Akamai Security Year in A Review) |
| --- |

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

| Three question quiz phishing attacks “rely on users filling out these quizzes in exchange for a prize which often results in stolen personal information.” (Found on page 11 of the Akamai Security Year in A Review) From experience, you would receive a popup or an email, etc. enticing you to click on their game, etc. and have you fill out your personal information for the purpose of stealing your information. |
| --- |

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

| “Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing the clean traffic forward” (Found on page 16 of the Akamai Security Year in A Review) |
| --- |

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

| Highest daily logins with daily credential abuse attempts was on August 17, 2020 with 365,1814,101 attempts (Found on page 18 of the Akamai Security Year in A Review) |
| --- |

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

| Highest gaming attacks associated with daily web application attacks was on July 11,2020 with 14,631,618 attacks (Found on page 19 of the Akamai Security Year in A Review) |
| --- |

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

| Highest media attacks associated with daily web application attacks was on August 20, 2020 with 5,150,760 attacks. (Found on page 19 of the Akamai Security Year in A Review) |
| --- |

### 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: A security event that compromises the integrity, confidentiality or availability of an information asset. A breach: an incident that results in the confirmed disclosure-not just potential exposure-of data to an unauthorized party. (Found this on Page 4 of Verizon Data Breach Report) |
| --- |

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

| Outside actors made up over 70% from 2016-2020, where in 2020 it was almost 80%. Internal actors were less than 40% from 2016-2020, where in 2020 the percentage dropped to nearly 20% (Found this on Page 12 of Verizon Data Breach Report) |
| --- |

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

| Organized crime made up nearly 80% of all breaches. (Found this on Page 12 of Verizon Data Breach Report) |
| --- |

1. In 2020, what percent of breaches were financially motivated?

| Nearly 100% of breaches were financially motivated in 2020.(Found this on Page 12 of Verizon Data Breach Report) |
| --- |

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

| **Denial of service**:The Denial of Service pattern consists  of attacks intended to compromise the availability of networks and systems.  This pattern includes both network and application layer attacks, and is the most common pattern across incidents. (Found this on Page 35 of Verizon Data Breach Report)  **Command control**:A command-and-control (C2) server is a main tool cyber threat actors have in their arsenal to launch and control cyber attacks. Threat actors use C2s to send commands to their malware and to distribute malicious programs, malicious scripts, and more. They also use them to receive stolen data that they exfiltrated from target servers, devices, websites, and forms. In short, C2s are the technical brain behind a threat actor’s malicious operations. (Found this on an external site: https://www.feroot.com/education-center/what-is-a-command-and-control-c2-server/#:~:text=A%20command%2Dand%2Dcontrol%20(C2)%20server%20is%20a,%2C%20malicious%20scripts%2C%20and%20more.)  **Backdoor**:A backdoor attack is a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms. A developer may create a backdoor so that an application, operating system (OS) or data can be accessed for troubleshooting or other purposes. Attackers make use of backdoors that software developers install, and they also install backdoors themselves as part of a computer exploit.(Found this on an external site: https://www.techtarget.com/searchsecurity/definition/back-door)  **Keylogger**:A keylogger or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a command-and-control (C&C) server. The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.(Found this on an external site: https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers) |
| --- |

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

| As we have pointed out in previous reports, Credentials remain one of the most sought-after data types (Found this on Page 22 of Verizon Data Breach Report) |
| --- |

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

| Phishing continues to walk hand-inhand with Use of stolen credentials  in breaches as it has in the past.Admittedly, we expected to see an increase here due to a larger remote workforce. However, the numbers have remained in the region of 25% of breaches, which is still a significant number. (Found this on Page 16 of Verizon Data Breach Report) |
| --- |

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