

Security 101 Challeng

By Rishabh Gautam



March 23, 2023

**Cybersecurity Threat Landscape**

**Part I: 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 in.)

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

Answer: Crowd Strike

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

|  |
| --- |
| 1. Attack on Government employees working from home 2. Scams related to PPE 3. Impersonation of medical bodies including WHO and CDC |

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

|  |
| --- |
| Ans. Healthcare Sector |

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

|  |
| --- |
| Ans. Wicked panda can be described as Cyber threat group that carries Chines state sponsor espionage or Chinese based adversaries. Even though many occupational sectors were targeted such as Telecom, Government, Healthcare and Technology sector by this group but their main attentions was on telecommunication sector |

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

|  |
| --- |
| Twisted Spider |

1. What is an access broker?

|  |
| --- |
| Access Brokers can be defined as threat actors that are able to gain backend access for both public and private organisation; sell this access on private channels or criminal forum |

1. Explain a credential-based attack.

|  |
| --- |
| Some examples of credential-based attacks are:-   1. Brute force: Using (Guessing) different combination of passwords and user name in order to gain Unauthorized access 2. Password spraying: Using a single common password to gain unauthorized access for multiple account on single domain 3. Credential stuffing: When hacker or cyber criminals collect account information such as Password, username, email and etc; through a data breach |

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

|  |
| --- |
| Big game hunter are credited for the heavy adoption of extortion in ransomware campaigns |

1. What is a DLS?

|  |
| --- |
| Dedicated leak sites |

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.

|  |
| --- |
| Sprite spider and carbon spider were able to deploy Linux base ransomware base virus on ESXI host. ESXI host can be defined as type of hypervisor that only runs on dedicated hardware or virtual machines |

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

|  |
| --- |
| Enabler plays a major role in an ecrime ecosystem by providing cyber criminals capabilities to exploit which they might not have access to . these cyber criminals then run malware as as service operation and exploit networks so that they could sell access on private channels or criminal websites. |

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

|  |
| --- |
| 1. Trend and Techniques 2. Overwatch Feature: Wizard Spider Target Financials 3. eCrime Enablers |

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?

|  |
| --- |
| The Most vulnerable and target elements of the gaming industry was it’s “Players” . Many suspicious activities were reported by the player about their account being compromised. |

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

|  |
| --- |
| September 2020 saw a strong push in web based cyber attacks for about 33 million. Some of the common attack included SQL Injection, Local file inclusion and Cross site Scripting |

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?

|  |
| --- |
| When hacker or cyber criminals collect account information such as Password, username, email and etc; through a data breach |

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 said their account has been compromised however only one fifth of them were worried about it |

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

|  |
| --- |
| When a user fills out personal information in order to win the prize but end up with their personal information being stolen |

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

|  |
| --- |
| Prolexic routed defend organization against DDos attack by redirecting network traffic to a scrubbing centre and only clean traffic to go forward |

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

|  |
| --- |
| August 17,2020 Saw daily logins of 365,181,101 |

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

|  |
| --- |
| July 11th 2020 with 14,631,618 gaming attacks |

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

|  |
| --- |
| August 20th 2020 with 5,150,760 media 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?

|  |
| --- |
| Incident can be defined as a security event that compromises CIA triad (Confidentiality, integrity and Availability of a information asset. Whereas breach is when confirm disclosure of data to an unauthorized party. |

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

|  |
| --- |
| 80% of the breaches were perpetrated by outside actors whereas 20% were perpetrated by internal actors |

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

|  |
| --- |
| 80% |

1. What percentage of breaches were financially motivated?

|  |
| --- |
| 60% |

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

|  |
| --- |
| **Denial of service**: Cyber attack that compromises the availability of network and system.  **Command control**: When a hacker can compromise entire network and use a computer to send command to system through malware and is able to gather stolen data from a targeted network (John Bogna,2022)  **Backdoor**: It can defined as technique to again access for the computer network or encrypted data by creating a backdoor. Hacker can use the backdoor created by software developers and install themselves as a backdoor to exploit the system.  Lutkevich, B., & Posey, B. (2023, January 24).  **Keylogger**: It can be defined as a spyware that is able to record and monitor sensitive data when entered on the keyboard to gain authorized access. examples are entering sentive information like credit card details and password. Keylogger can be installed while visiting a webpage which records the sensitive information and then send the log file to a server where cyber criminals can use them.(SoPHOS,2019) |
|  |

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

|  |
| --- |
| Credentials |

1. What was the percentage of breaches involving phishing?

|  |
| --- |
| 25% |

**References**

Bogna, J. (n.d.). *What is a command and control cyberattack?* PCMAG. Retrieved March 23, 2023, from <https://www.pcmag.com/how-to/what-is-a-command-and-control-cyberattack>

Lutkevich, B., & Posey, B. (2023, January 24). *What is a backdoor attack? tips for detection and prevention: Definition from TechTarget*. Security. Retrieved March 23, 2023, from https://www.techtarget.com/searchsecurity/definition/back-door

*Demystifying a keylogger – how they monitor what you type and what you can do about it?* What is a Keylogger and How Can I Detect One on My Computer? | Sophos Home. (n.d.). Retrieved March 23, 2023, from https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger