

Cybersecurity Boot Camp

Security 101 Challenge

## 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?

|  |
| --- |
| Maze |

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

|  |
| --- |
| The psychology behind social engineering techniques are tailored techniques that prey on human emotions and behaviour I.e. greed, curiosity, fear and the desire to help. Three eCrime phishing techniques designed to use lure content and social engineering techniques capable of targeting human emotions are:  Exploitation of individuals looking for details on disease tracking, testing and treatment  Financial assistance and government stimulus ackages  Tailored attacks against employees working from home |

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

|  |
| --- |
| Industrial and engineering sector (229 incidents). |

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

|  |
| --- |
| They originate from China. Wicked Panda consists of a superset of groups involving several contractors working in the interests of the Chinese state while still carrying out criminal, for-profit activities, likely with some form of tacit approval from CCP officials. |

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

|  |
| --- |
| Twisted Spider |

1. What is an access broker?

|  |
| --- |
| Threat actors that gain backend access to organisations, to sell either on criminal forums or through private channels. |

1. Explain a credential-based attack.

|  |
| --- |
| Brute force, password spraying and credential stuffing are examples of credential based attacks.  Brute force is explained as an approach that uses trial and error to crack passwords, login credentials, encryption keys etc. |

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

|  |
| --- |
| Twisted Spider |

1. What is a DLS?

|  |
| --- |
| Dedicated Leak Sites (DLSs) are websites where victims’ stolen data is released. |

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.

|  |
| --- |
| ESXi hosts run on hardware without the need for conventional operating systems, therefore lack endpoint protection software that could prevent or detect ransomware attacks. Targeting these hosts ransomware operators are quickly able to encrypt multiple virtualized systems with relatively few ransomware deployments. |

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

|  |
| --- |
| Provide criminal actors with capabilities they may otherwise not have access to. These actors run malware-as-a-service operations, specialise in delivery mechanisms or exploit networks in order to sell initial access to other criminal actors. |

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

|  |
| --- |
| Access Brokers, Ransomware operations, Malware Obfuscation. |

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 and September 2020?

|  |
| --- |
| The gaming players. |

1. From October 2019 to September 2020, in 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?

|  |
| --- |
| More than 60%. |

1. What is credential stuffing?

|  |
| --- |
| A kind of brute force attack that attempts to take over accounts using lists of compromised user credentials. |

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 halve of the frequent players, but only one-fifth were worried. |

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

|  |
| --- |
| An attack that requires users to answer three questions related to a short quiz in exchange for a prize, which often results in the theft of their personal information. |

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

|  |
| --- |
| It defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing the clean traffic forward. |

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

|  |
| --- |
| August 17, 2020. |

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

|  |
| --- |
| July 11, 2020. |

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

|  |
| --- |
| August 20, 2020. |

### 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: A security event that compromises the integrity, confidentiality or availability of an information asset  Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party. |

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

|  |
| --- |
| Figure 14 illustrates the trend of breaches perpetrated between 2016 and 2020 as a percentage, for external and internal actors.  It’s not clear what the exact percentages are from the vertical axis, therefore the percentages given are approximate.  Outside actors, approximately %:  2016 - 72  2017 - 72  2018 - 72  2019 - 72  2020 - 78  Internal actors, approximate %:  2016 - 28  2017 - 28  2018 - 32  2019 - 28  2020 - 22 |

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

|  |
| --- |
| 80% |

1. What percentage of breaches were financially motivated?

|  |
| --- |
| Fig 15 illustrates the trend for financially motivated breaches.  It’s not clear what the exact percentages are from the vertical axis, therefore the percentages given are approximate.  2016 – 67  2017 – 80  2018 - 75  2019 – 90  2020 - 97 |

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

|  |
| --- |
| **Denial of service**: A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.  Source: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>  **Command control**: Command and control is defined as a technique used by threat actors to communicate with compromised devices over a network.  Source: <https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained>  **Backdoor**: A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.  Source: <https://www.malwarebytes.com/backdoor>  **Keylogger**: A [keylogger](https://en.wikipedia.org/wiki/Keystroke_logging) is a type of surveillance software or hardware designed to record and monitor keystrokes made by a user on a computer keyboard, tablet, or smartphone. Keyloggers can capture sensitive information, such as login credentials, credit card numbers, and confidential messages, without the user’s knowledge or consent.  Source: <https://www.sentinelone.com/cybersecurity-101/keylogger-2/?utm_source=google-paid&utm_medium=paid-display&utm_campaign=ukie-promo-cloud&gclid=Cj0KCQjwr82iBhCuARIsAO0EAZzDJx0BWfpB3S2Ack7dSrYiKj2H4tYMBMC6vnPuVFlOu5PSyGeGAggaAkpwEALw_wcB> |

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

|  |
| --- |
| Credentials |

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

|  |
| --- |
| 36% |

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