# Security 101 Homework: 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.

1. What was the dominant ransomware family that impacted the healthcare industry in 2020? - Maze
2. Describe three different pandemic-related eCrime Phishing themes. - a. Exploitation of individuals looking for details on disease tracking, testing and treatment

b. impersonation of medical bodies, including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC)

c. Financial assistance and government stimulus packages

1. Which industry was targeted with the highest number of ransomware-associated data extortion operations? - **industrial and engineering sector**
2. What is WICKED PANDA? - adversaries targeting telecommunications organizations Where do they originate from? - China

1. Which ransomware actor was the first observed using data extortion in a ransomware campaign? - Twisted Spider
2. What is an access broker?  **Access brokers are threat actors that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels. When criminal malware operators purchase access, it eliminates the need to spend time identifying targets and gaining access, allowing for increased and quicker deployments as well as higher potential for monetization. Some access brokers escalate privileges to the domain administrator level (often advertised as “full access”), while other access brokers just provide the credentials and endpoints necessary to gain access.**
3. Explain a credential-based attack. - credential-based attacks (e.g., brute forcing, password spraying, credential stuffing)
4. Who is credited for the heavy adoption of data extortion in ransomware campaigns? - **TWISTED SPIDER**
5. What is a DLS? - dedicated leak sites
6. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020? - 79%
7. Who was the most reported criminal adversary of 2020? - WICKED PANDA
8. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures. - drive innovation in the world of malware development. Over the year, CrowdStrike Intelligence noted trends in the use of open-source obfuscation software and the targeting of virtualization environments pioneered by these adversaries.

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, specialize in delivery mechanisms or exploit networks in order to sell initial access to other criminal actors.
2. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report? 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? - *SUNBURST*