# 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 Ransomware Family.
2. Describe three different pandemic-related eCrime Phishing themes.  
    i) One of the methods used to phish individuals was to abuse the pandemic information available and exploit individuals attempting to search up information regarding the virus / pandemic.  
    ii) Another attack method was abusing the financial assistance and stimulus packages being awarded by the government and using this as a platform to manipulate vulnerable victims.  
    iii) Tailored attacks towards individuals and organizations who were operating remotely and/or working from home.
3. Which industry was targeted with the highest number of ransomware-associated data extortion operations?  
    Industrials and Engineering
4. What is WICKED PANDA? Where do they originate from?  
    Wicked Panda is a known and CrowdStrike tracked threat actor / adversary who originate from China and use methods such as spearphishing, malware, supply chain attack.
5. Which ransomware actor was the first observed using data extortion in a ransomware campaign?  
    Outlaw Spider in May 2019
6. What is an access broker?   
    Access brokers are individuals who have been able to quietly obtain access to networks and systems in which the user(s) are unauthorized who then offer their access to others for a fee.
7. Explain a credential-based attack.  
    A credential based attack is an attack in which the attacker steals credentials of the victim(s) and are then able to bypass security measures and other checks and then steal critical data.
8. Who is credited for the heavy adoption of data extortion in ransomware campaigns?  
    Twisted Spider has been credited with this adoption.
9. What is a DLS?  
    Dedicated Leak Site(s).
10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?   
     79% according to attributable intrusions uncovered by OverWatch.
11. Who was the most reported criminal adversary of 2020?   
     Wizard Spider.
12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.  
     These actors targeted ESXI, a hypervisor that manages multiple VMs on machines and systems, and were able to encrypt these systems with little ransomware deployment and were able to easily traverse these systems as there was little to no endpoint protection.
13. What role does an Enabler play in an eCrime ecosystem?  
     Enablers provide threat actors with malware as a service or allow initial access into systems and networks to be sold to other criminal threat actors.
14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

Services, Distributions, and Monetization

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

Sunburst.