# 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? Twisted Spider lead 2020 with ransomware attacks through their Maze and Egregor ransomware families with at least 26 infections.
2. Describe three different pandemic-related eCrime Phishing themes. Threat actors would use email attachments and hyperlinks for users to interact with or use online searches to attract traffic revolving around Covid 19 and stimulus packages.
3. Which industry was targeted with the highest number of ransomware-associated data extortion operations? Industrial and engineering sector had the highest number of ransomware-associated data extortion operations with 229 incidents.
4. What is WICKED PANDA? Where do they originate from? Wicked Panda is a threat actor originated from China.
5. Which ransomware actor was the first observed using data extortion in a ransomware campaign? Outlaw Spider was the first ransomware actor observed using data extortion in a ransomware campaign.
6. What is an access broker? Access Brokers are threat actors that get inside access and information and sell the access either on criminal forums or private channels.
7. Explain a credential-based attack. Credential-based attacks are when attackers steal credentials in order to break into a system and steal critical data.
8. Who is credited for the heavy adoption of data extortion in ransomware campaigns? Twisted Spider is credited for a heavy adoption of data extortion in ransomware campaigns and was the first actor to launch DLS(Dedicated Leak Site).
9. What is a DLS? DLS (Dedicated Leak Sites) are sites to leak sensitive data as part of data extortion techniques.
10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020? 79% of intrusions were eCrime intrusions in 2020 according to Crowdstrike Falcon OverWatch.
11. Who was the most reported criminal adversary of 2020? Wizard Spider was the most reported criminal adversary in 2020.
12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures. Virtual Machines have less endpoint protection software to detect ransomware. Thus by attacking VM and encrypting ESXi server, it can multiple systems the VM is attached to.
13. What role does an Enabler play in an eCrime ecosystem? Enablers are actors that run malware as a service operations and specialize in exploits in order for other actors to gain access to networks. They sell initial access to networks.
14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report? eCrime ecosystem is comprised of 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 is the name of the malicious code used to exploit SolarWinds Orion IT management software vulnerability.