# 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?
   1. According to CrowdStrike, “BIG GAME HUNTING (BGH) ransomeware campaigns aimed at high-value targets… dominated the ecosystem of eCrime enablers in 2020” (pg. 6).
2. Describe three different pandemic-related eCrime Phishing themes.
   1. Some of the different pandemic-related eCrime Phising themes are:
      1. “Scams offering personal protective equipment (PPE)” (CrowdStrike, pg. 15). This phishing scam relies heavily on fear. During the beginning months of the Pandemic, people were scrambling for groceries, cleaning supplies, and PPE - especially masks and gloves. In the midst of the heightened emotions, it is easy to understand why these crimes were successful.
      2. “Financial assistance and government stimulus packages” (CrowdStrike, pg. 15). The U.S. Government began expanding government assistance programs, such as EBT and Unemployment, as well has providing Stimulus Checks to certain groups of citizens. There was a lot of confusion among Americans when the stimulus checks began being dispersed. Besides the unsureness of whether you were getting one or not, there were also multiple checks being sent out as well as many cases of theft and fraud. All of these create an environment for phishing attacks to thrive one.
      3. “Tailored attacks against employees working from home” (CrowdStrike, pg. 15). COVID-19 forced many companies to have their employees work from home, which is something that was new for not only the employees, but also for the companies themselves. There was no time to prepare and train employees on safety protocols, and it is nearly impossible for a company to ensure that their employees are using safe online practices, WiFi connections, using their work technology solely for work purposes, etc.
3. Which industry was targeted with the highest number of ransomware-associated data extortion operations?
   1. CrowdStrike reports that the industry that was targeted with the highest number of ransomeware-associated data extortion operations was the “industrial and engineering sector” (CrowdStrike, pg. 21).
4. What is WICKED PANDA? Where do they originate from?
   1. WICKED PANDA is a targeted intrusion actor/adversary which targeted “telecommunications organizations in 2020” (CrowdStrike, pg. 35). WICKED PANDA operated “illicit for-profit cyber operations against video game firms for years… while also supporting state-directed intelligence requirements” (CrowdStrike, pg. 36).
5. Which ransomware actor was the first observed using data extortion in a ransomware campaign?
   1. According to CrowdStrike, “OUTLAW SPIDER” was the first to be observed using data extortion in a ransomware campaign” (pg. 23).
6. What is an access broker?
   1. Access brokers are “threat actors that gain backened access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels” (CrowdStrike, pg. 25).
7. Explain a credential-based attack.
   1. A credential-based attack is when a threat actor is trying to obtain credential information, such as usernames and passwords. Credential-based attacks lead to “exploitation and credential theft activities” which are difficult to control because “even after patching, threat actors can often use these stolen credentials to reacquire access to the same targets” (CrowdStrike, pg. 48-49).
8. Who is credited for the heavy adoption of data extortion in ransomware campaigns?
   1. “TWISTED SPIDER… has been credited with being the catalyst for the heavy adoption of this technique in 2020. TWISTED SPIDER was the first ransomeware actor to launch a DLS” (dedicated leak site) (CrowdStrike, pg. 23).
9. What is a DLS?
   1. A DLS is a dedicated leak site, which is associated with specific ransomware families and which was “adopted by at least 23 ransomware operators in 2020” (CrowdStrike, pg. 19).
10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?
    1. According to CrowdStrike Falcon OverWatch, “eCrime intrusions made up 79% of all attributable instructions… in 2020” (CrowdStrike, pg. 10).
11. Who was the most reported criminal adversary of 2020?
    1. “WIZARD SPIDER” was the most reported criminal adversary for the second year in a row” (CrowdStrike, pg. 27).
12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.
    1. SPRITE SPIDER and CARBON SPIDER “deploy Linux versions of their respective ransomware families on ESXi hosts during BGH operations… (and) with more organizations migrating to virtualization solutions… this is a natural target for ransomware operatoes looking to increase the impact against a victim” (CrowdStrike, pg. 26). According to CrowdStrike, all of the identified incidents of this occurring “were enabled by the acquisition of valid credentials,” allowing the ransomware operators to use less ransomware deployments to encrypt multiple systems (CrowdStrike, pg. 26).
13. What role does an Enabler play in an eCrime ecosystem?
    1. Enablers provide “criminal actors with capabilities they may otherwise not have access to,” and may “run malware-as-a-service operations, specialize in delivery mechanisms or exploit networks in order to sell” teh access to other malicious actors (CrowdStrike, pg. 30).
14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?
    1. The three parts of the eCrime ecosystem according to CrowdStrike’s report are: 1. Services, 2. Distribution, and 3. Monetization (CrowdStrike, pg. 31).

1. What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?
   1. The code used in the “sophisticated supply chain hack against… SolarWinds Orion IT management software” is called SUNBURST (CrowdStrike, pg. 16).