# 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?**  
     
   The Maze Ransomeware Family had the highest infection count in the healthcare industry in 2020. Followed closely by the Conti Family.
2. **Describe three different pandemic-related eCrime Phishing themes.**  
    1. Re-writing previously used phishing lure content to mention Covid-19  
    2. Impersonating medical bodies like The World Health Organization (W.H.O.) and the Center for Disease Control (C.D.C.)  
    3.Tailored atacks against employees working from home
3. **Which industry was targeted with the highest number of ransomware-associated data extortion operations?**The Industrial and Engineering sector had 229 incidents making it the most targeted industy, just slightly ahead of the Manufacturing sector which had 228 incidents.
4. **What is WICKED PANDA? Where do they originate from?**  
     
   "WICKED PANDA" are the top tracked named adversary from China.
5. **Which ransomware actor was the first observed using data extortion in a ransomware campaign?**  
     
   Outlaw Spider used this tactic in May 2019 and was the first observed organization to do so.
6. **What is an access broker?**  
   Access brokers are threat actors that sell access into a corporation or government organization.
7. **Explain a credential-based attack.**  
     
   An attack based on stolen credentials that bypasses an organizations security measures, allowing the hacker to carry out an attack (or theft) from within the organization.
8. **Who is credited for the heavy adoption of data extortion in ransomware campaigns?**TWISTED SPIDER
9. **What is a DLS?**  
     
   A Dedicated Leak Site
10. **According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?**   
      
    According to Overwatch eCrime Intrusions made up 79% of the intrusions they uncovered in 2020 up from 69% in 2019.
11. **Who was the most reported criminal adversary of 2020?**   
      
    WIZARD SPIDER
12. **Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.**  
      
    They were essentially top down infiltrations going after the hypervisor of the virtual systems in organizations. This approach allowed them to attack more systems with fewer malware deployments.
13. **What role does an Enabler play in an eCrime ecosystem?**  
      
    Very similar to access brokers; in that they do nefarious dealings in support of eCrime. Enablers focus on selling operations as a service. Specializing in malware, delivery mechanisms or network exploitations, they sell the code or software that is needed to pull off an attack.
14. **What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?**

1.Services

2.Distribution

3.Monetization

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

The malicious code was loaded into the SolarWinds software by the STELLARPARTICLE adversary in three stages

1."SunBurst" this was the backdoor into the system that allowed all the other code to work.

2."Sunspot" was a monitoring tool that also replaced source code with a modified version.

3. "Teardrop" was a custom in-memory loader