# 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. **Maze**
2. Describe three different pandemic-related eCrime Phishing themes.
   1. **Financial assistance and government stimulus packages:**
      1. **This takes advantage of people's need for securing their financial situation during a turbulent time where many were losing jobs or having hours cut. People are looking for relief and are more vulnerable.**
   2. **Tailored attacks against employees working from home**
      1. **This takes advantage of the weaker networks found at the homes of individuals. Less/no network monitoring. Isolation from coworkers and lack of quick or easy support.**
   3. **Exploitation of individuals looking for details on disease tracking, testing, and treatment.**
      1. **Easy to spin up misinformation or clickbait to redirect to malicious sites. Testing sites required sign up and provision of PII which can be stolen or abused.**
3. Which industry was targeted with the highest number of ransomware-associated data extortion operations?
   1. **Industrial and Engineering sector**
4. What is WICKED PANDA? Where do they originate from?
   1. **Wicked Panda originates from China as a nation state actor (APT). They exploit multiple vulnerabilities against multiple sectors and geographic locations. Cobalt Strike is their continued tool of choice along with the use of several other loaders.**
5. Which ransomware actor was the first observed using data extortion in a ransomware campaign?
   1. **Outlaw Spider in May 2019.**
6. What is an access broker?
   1. **Access brokers are entities that initially compromise organizations and then sell that access to other criminal entities on forums or through private methods. This takes the initial identification and breach out of the hands of the buyer; allowing the buyer to deploy attacks against the breached organization quicker.**
7. Explain a credential-based attack.
   1. **Credential-based attacks use authentic credentials, often stolen or leaked, as part of larger attacks.** 
      1. **Brute forcing: Involves using generated lists and innumerous attempts to guess working sets of credentials.**
      2. **Password spraying: Brute forcing using the same credentials against multiple sites before moving on to the next set of credentials to try.**
      3. **Credential stuffing: Using known credentials or leaked credentials on multiple sites/services to see if a known credential set work will work for another site/service.**
8. Who is credited for the heavy adoption of data extortion in ransomware campaigns?
   1. **Twisted Spider**
9. What is a DLS?
   1. **A dedicated leak site. This is a website used to pressure victims into paying by threatening to leak data or actually leaking data if the threat actor is not paid.**
10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?
    1. **79%**
11. Who was the most reported criminal adversary of 2020?
    1. **Wizard Spider**
12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.
    1. **These two entities impacted virtualization infrastructures by shifting from single VM ransoming to attacking Linux ESXI hosts. Attacking this hypervisor system would allow the attackers to take out all of the VMs hosted on the servers at once. These targets were also weaker since they do not have a conventional operating system or endpoint protection software.**
13. What role does an Enabler play in an eCrime ecosystem?
    1. **These actors are like criminal contractors. They provide capabilities a criminal actor may not have in house; such as running malware-as-a-service operations, delivering malware, or gaining foothold access to sell to other criminal actors.**
14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?
    1. **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?
   1. **Sunburst**