# 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 became the dominant ransomware in the healthcare industry in 2020.
2. **Describe three different pandemic-related eCrime Phishing themes.**1. Financial assistance and government stimulus packages - hit people that were curious about the different programs that were being announced by the government about aid that would help them in times of crisis.   
   2. Tailored attacks against employees working from home - since many Americans and employees had offices shut down, they were forced to transition to working from home, outside of work LANs and offices with proper network security measures in place for sensitive data. Many worked at home, or other locations outside the offices on home networks or SOHOs, even nearby public networks from ISPs or nearby businesses with fewer security measures put in place, exposing sensitive data such as personal banking information, proprietary business practices, and ransomware attacks on company-owned computers.   
   3. Scams offering personal protective equipment - with an immediate short supply of PPE due to mass need and hoarding amongst citizens and professionals to reduce spread, cybercriminals preyed on the fear and need for protection amongst society, possibly by tricking individuals with the availability of supply for financial gain.
3. **Which industry was targeted with the highest number of ransomware-associated data extortion operations?**The industrial and engineering sectors were targeted the highest with 229 incidents.
4. **What is WICKED PANDA? Where do they originate from?**WICKED PANDA is a Chinese, for profit state-sponsored and state-directed cyber attack group that originates from the PRC.
5. **Which ransomware actor was the first observed using data extortion in a ransomware campaign?**OUTLAW SPIDER
6. **What is an access broker?**They’re described as “threat actors that gain backend access to various organizations and sell this access either on criminal forums or through private channels.”
7. **Explain a credential-based attack.**A credential-based attack is one that attacks a system with such tools as brute force password crackers, password spraying, and credential stuffing in order to gain login to a system with a user’s cracked password or access code.
8. **Who is credited for the heavy adoption of data extortion in ransomware campaigns?**TWISTED SPIDER
9. **What is a DLS?**DLS is a dedicated leak site.
10. **According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?**400% of the intrusions in 2020 came from eCrime.  
    79% (Correction)
11. **Who was the most reported criminal adversary of 2020?**WIZARD SPIDER**,** a Big Game Hunting actor
12. **Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.**  
    SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures by targeting Linux systems as Big Game Hunting actors using ransomware in order to take hostage with multiple consolidated systems in one target vs having to target multiple systems separately. “By targeting these hosts, ransomware operators are able to quickly encrypt multiple systems with relatively few actual ransomware deployments.”
13. **What role does an Enabler play in an eCrime ecosystem?**They are in the Services portion of the ecosystem and run ransomware-as-a-service (RaaS) or malware-as-a-service (MaaS) operations for other criminal actors to use and implement into their tradecraft.
14. **What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?**1. Services  
    2. Distribution  
    3. Monetization (pg31)

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