# 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 most prolific ransomware family that impacted the healthcare industry in 2020 was TWISTED SPIDER using the Maze, and WIZARD SPIDER using Conti. As shown in the Crowdstrike Report, TWISTED SPIDER realized 20 infections in the healthcare sectors victims with their Maze ransomware attacks.
2. Describe three different pandemic-related eCrime Phishing themes.

There were a number of eCrime phishing strategies that were prevalent during the pandemic, the themes of these eCrimes consisted of cybercriminals praying on the exploitation of individuals searching for information or updates on treatment, testing ,and disease tracking of COVID, impersonating individuals that could provide financial assistance and/or government assistance packages, and pretending to offer personal protective equipment. All these eCrime phishing schemes were attempts to encourage a human response to interact with a hyperlink or attachment within the email.

1. Which industry was targeted with the highest number of ransomware-associated data extortion operations?

The Crowdstrike Intelligence report recognized that the industry that recorded the highest number of ransomware-associated data extortion operations in the year was the industrial & engineering sector with 229 incidents

1. What is WICKED PANDA? Where do they originate from?

WICKED PANDA is a Chinese state-backed cyber espionage adversary that looks to target public and private sector organisations. One of the common trends in the types of attacks that WICKED PANDA employs are spear-phishing emails with malicious attachments/hyperlinks for the preliminary compromise of the attack

1. Which ransomware actor was the first observed using data extortion in a ransomware campaign?  
   OUTLAW SPIDER was the first observed to be utilizing data extortion in a ransomware campaign which was recorded as early as May 2019
2. What is an access broker?   
   Access brokers are threat actors that are able to access the backend of various organisations (e.g. corporations and government entities) and aim to sell the access they have obtained to criminal malware operators through criminal/private forums.
3. Explain a credential-based attack.

Credential-based attacks involve attackers aiming to steal credentials to gain access, bypass security measures setup by organisations, or look to steal critical data. Some of the more common measures utilized in this form of attack are Brute-Force attacks and phishing tactics.

1. Who is credited for the heavy adoption of data extortion in ransomware campaigns?TWISTED SPIDER has been credited for the heavy adoption of the data extortion in ransomware campaign through the operators of Maze and Egregor techniques
2. What is a DLS?  
   Dedicated Leak Site allows ransomware operators to publish leaked data from organisations so others are able to view this information Ransomware operators will often threaten to leak data on DLS platforms to pressure victim organisations to offer financial compensation.
3. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?   
   In 2020, the percentage of intrusions from eCrime was 79% according to Crowdstrike Falcon Overwatch
4. Who was the most reported criminal adversary of 2020?

WIZARD SPIDER for the second year in a row was the most report adversary in 2020. This was due to WIZARD SPIDER having a diverse and potent toolset that llows them to be one of the most formidable adversaries in the current eCrime landscape.

1. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.

SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures by being able to deploy Linux versions of their ransomware families on ESXI hosts. This is historical as operators have not generally targeted Linux based systems, and much less through the host of ESXI. This has allowed ransomware operators to be able to rapidly encrypt multiple systems with far less actual ransomware deployments.

1. What role does an Enabler play in an eCrime ecosystem?

Enabler’s performance a key role in the eCrime ecosystem as criminal actors are able to be provided with capabilities that without an enabler, they would not have access to. Enablers specialize in a number of activities such as the exploitation of networks in order to sell initial access on DLS platforms, delivery in mechanisms, and they run malware as a service operations

1. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

The three parts of the eCrime ecosystem consists of:   
1. Services (e.g. Ransomware, access brokers, DDoS attack tools)  
2. Distribution (e.g. Exploit kit development, spam email distribution, social network and IM spam)   
3. Monetization (e.g. Money laundering, cryptocurrency services, wirefraud)

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

In December 13 2020, there was public reports that identified a supply chain attack against the SolarWinds Orion IT management software. This vulnerability was successfully exploited through the adversary code dubbed SUNBURST.

**References**

Crowdstrike, 2021, *Global Threat Report*. Retrieved March 13th, 2022

Paloalto, 2022, *What is a Credential-Based Attack.* Retrieved March 14th, 2022,

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack#:~:text=Credential%20based%20attacks%20occur%20when,measures%2C%20and%20steal%20critical%20data.&text=Credential%20theft%2C%20the%20first%20stage,the%20process%20of%20stealing%20credentials>.