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 was used by TWISTED SPIDER to attack the healthcare industry by targeting pharmaceutical and biomedical companies.

2. **Describe three different pandemic-related eCrime Phishing themes.**
   I. Scams that would involve either the sale or free distribution of medical protective equipment(Masks, face shields, gloves, sanitizer, etc.)

   II. Financial stimulus package scams which would often impersonate government officials asking the victim to input their credentials to receive their stimulus

   III. Cyber Criminals impersonating governmental medical entities such as WHO or CDC, where they may try and sell them a medical product or offer free vaccine doses, both of which would have the victim give out sensitive information

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

   The Healthcare industry

4. **What is WICKED PANDA? Where do they originate from?**

WICKED PANADA was a cyber criminal gang that started operating around the early 2010s in the People's Republic of China. In the late 2010s they gained enough reputation to be sponsored by the government. They often perform intrusions or disruptions that align with objectives of the PRC.

5. **Which ransomware actor was the first observed using data extortion in a ransomware campaign?**

In May 2019, OUTLAW SPIDER employed the usage of data extortion in their ransomware campaigns

6. **What is an access broker?**

An Access Broker is a hacker who finds a method into a particular software or system, and then sells that information to the highest bidder for oten thousands of dollars.

7. **Explain a credential-based attack.**

A Credentials-Based Attack is an attack that involves gaining administrative credentials with which they can then perform their attack. An example would be a cyber criminal phising a known system admin trying to get the credentials. Once they have the information they need, they can get into the main server and either take any and all sensitive information to perform a Data Extortion, or upload malicious code like ransomware or spyware.

8. **Who is credited for the heavy adoption of data extortion in ransomware campaigns?**

While OUTLAW SPIDER developed the technique of data extortion, TWISTED SPIDER is credited with the heavy usage and refinement of the attack.

9. **What is a DLS?**

A DLS is a Dedicated Leak Site. They are sites that, as the name suggests, are created for the sole purpose of dumping sensitive information often harvested by a Data Extortion Ransomware attack.

10. **According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?**

    79% of all intrusions were eCrime intrusions in 2020

11. **Who was the most reported criminal adversary of 2020?**

    WIZARD SPIDER used BGH techniques in order to form large criminal organization and become the most reported criminal adversary

12. **Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.**

Large organizations often use a version of linux called ESXi that runs multiple Virtual Machines in order to reduce the number of physical servers that are required. CARBON SPIDER and SPRITE SPIDER had the idea to instead of attacking all the individual VMs, to just infect the main host with Ransomware. This allowed their Big Game Hunting operations to be easier to pull off, while doing the same amount of damage as attacking all of the individual VMs.

13. **What role does an Enabler play in an eCrime ecosystem?**

Enablers provide Cyber Criminals with tools and information that they may not have access to. Enablers can develop more dangerous tools, run malware-as-a-service schemes or inform new cyber criminals safe means of operating while avoiding detection.

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

I. Ransomware Big Game Hunters
II. Access Brokers
III. Enablers

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

SUNSPOT is a monitoring virus that can track Orion packages. While monitoring the packages, SUNSPOT can be activated to infect a package with SUNBURSTS source code. SUNBURST then gains administrative permissions and can modify the system as the user pleases.