**INCIDENT REPORT: TS-18982-Defensive: Find the Culprit!**

**Date: 06/19/24**

**Executive summary:**

This User Story involves identifying how the victim computer was infected with malware based on the retrieved PCAP traffic.

**Narrative:**

Using Wireshark, I was able to identify the Victim Details, which are listed below. I then exported the HTTP Objects associated with the PCAP. After entering them into VirusTotal, I was able to identify the malware name and type, as well as confirm the malicious nature of the associated website http://classicalbitu.com

**Conclusion:**

On 09/22/2015 at approximately 22:41:15 UTC the victim computer accessed the

http://classicalbitu.com. This site is identified in VirusTotal as being malicious in nature, associated with spyware/malware. VirusTotal indicated that the site was created on 11/23/2020, registered in Scottsdale, AZ, via GoDaddy.com. PCAP traffic indicated that it was running on an Apache server.

At 22:41:16 UTC, the victim’s computer requested the malicious package, “config.jpg”, which was downloaded by 22:41:17 UTC. This malware is identified in VirusTotal as a ZBOT Trojan. According to the website TechMonitor *(https://techmonitor.ai/technology/cybersecurity/images-of-sunsets-or-cats-used-to-hack-into-bank-accounts-040314-4189283)*, the .jpg file incorporates steganography to monitor for any queries made to listed banks in order to capture credential information.

**Victim Details:**

* **IP Address:**  10.54.112.205
* **MAC Address:** 00:50:8b:01:db:2f
* **Operating System:** Windows 7
* **Hostname:** PENDJIEK-PC

**Indicators of compromise (IOCs):**

* **Malware Name/Type/File:** ZBOT Trojan, config.jpg
* **Domain:**  classicalbitu.com
* **IP Addresses:**  193.23.181.155; 10.54.112.205
* **SHA256 Hash:** 3359a8d15eb9de2e6a9d5a91182ae41f7dda053e78f5e9d3b715ab28afa57ea1