**INCIDENT REPORT: TS-18961-Defensive: Malware Analysis**

**Date: 06/13/24**

**Executive summary:**

This User Story involves a laptop which is infected with multiple types of malware, which was presented by the complainant “Jack”. ProsperSec was able to recover hardware logs to assist in the identification of the malware and their sources.

**Narrative:**

Using Wireshark, I was able to identify the Victim Details and IOCs while examining the included packets. Potential IOC’s were exported at HTTP Objects and uploaded to VirusTotal for analysis.

**Conclusion:**

Under the Windows User Account ‘’bill.cook”, the victim queried http://tonmatdonanminh.com, where the TrojanDropper malware was downloaded. As a “dropper”, this likely facilitated the download of the Cobalt/Cobalt Strike Trojan and FickerStealer Trojans, which are commonly used to steal sensitive information, and in the case of Cobalt Strike, may allow for remote access by threat actors.

**Victim Details:**

* **Hostname:**  DESKTOP-MGVG60Z
* **IP Address:** 10.2.8.101
* **MAC Address:** 00:12:79:41:c2:aa
* **Windows User Account Name:** bill.cook

**Indicators of compromise (IOCs):**

* **Malware Name/Type:** FickerStealer Trojan, file: 6lhjgfdghj.exe
  + **IP Address:** 8.208.10.147
  + **Domain/URL:** http://roanokemortgages.com/6lhjgfdghj.exe
  + **SHA256 Hash:** 94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1
* **Malware Name/Type:** Cobalt or Cobalt Strike Trojan Shellcode, file: 6aov
  + **IP Address:** 198.211.10.238
  + **Domain/URL:** http://198.211.10.238:8080/6Aov
  + **SHA256 Hash:** e519c1e99f21fbc6754e2ed9ef38a12684d506617229b4ca87fcff86f6838250
* **Malware Name/Type:** TrojanDropper, files: uninviting.php; forum.php
  + **IP Address:** 45.124.85.55; 213.5.229.12
  + **Domain/URL:**  http://tonmatdoanminh.com; http://satursed.com
  + **SHA256 Hash:** 858aac988e85075348f32e4750f17bf5c16e579fff258d3def9f23563e89372d