**Incident Report:** CH-15079-Defensive-Malware-Analysis

**Date:** 10-22-2022

**Executive Summary:**

On 08-02-2021 at approximately 14:00 UCT, a Windows 10 desktop used by ASCO Limited employee Bill Cook was infected with Hancitor, Ficker Stealer, and Cobalt Strike malware, resulting in the exfiltration of network shared files accessed through the compromised device.

**Victim Details:**

* Host name: 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):**

* File name: uninviting.pho
  + SHA256 hash: 3a5648f7de99c4f87331c36983fc8adcd667743569a19c8dafdd5e8 a33de154d
  + File size: 1097kB
  + File type: text/html
  + File location: 45.124.85.55 (tonmatdoanminh.com)
  + File description: Malware is encoded as base64 text in web page containing script that executes a saveAs function for the Word document file 0208\_54741869750132.doc
* File name: 6lhjgfdghj.exe
  + File size: 273 kB
  + File type: application
  + File location: 8.208.10.147 (roanokemortgages.com)
  + File description: Ficker Stealer executable malware
* File name: 6Aov
  + File size: 208 kB
  + File type: application
  + File location: 198.211.10.238
  + File description: Cobalt Strike payload (used in AD environments)

**Malicious HTTP Traffic**:

* Hancitor:
  + 45.124.85.55 port 80 (tonmatdoanminh.com) - HTTP GET /uninviting.php
  + 54.235.147.252 port 80 (api.ipify.org) - HTTP GET
  + 213.5.229.12 port 80 (satursed.com) - HTTP POST /8/forum.php
* Ficker Stealer:
  + 8.208.10.147 port 80 (roanokemortgages.com) - HTTP GET /6lhjgfdghj.exe
  + 54.235.147.252 port 80 (api.ipify.org) - HTTP GET /?format=xml
  + 185.100.65.29 port 80 (sweyblidian.com) - TCP traffic
* Cobalt Strike:
  + 8.208.10.147 port 80 (roanokemortgages.com) - HTTP GET /0801.bin
  + 8.208.10.147 port 80 (roanokemortgages.com) - HTTP GET /0801s.bin
  + 198.211.10.238 port 8080 - HTTP GET /6Aov
  + 198.211.10.238 port 443 - HTTPS traffic
  + 198.211.10.238 port 8080- HTTP GET /ca
  + 198.211.10.238 port 8080 - HTTP POST /submit.php?id=3275377518