**INCIDENT REPORT: BN-18986-Malware-Analysis**

**Date: 6/21/2024**

**Executive Summary:**

Analysis of network traffic logs from a compromised laptop revealed infections by three distinct malware families: Tordal/Hancitor/Chanitor, Win32/Ficker Stealer, and Cobalt Strike Beacon. The malware was delivered through malicious websites and downloads, resulting in the compromise of sensitive information and potential further exploitation of the victim's system.

**Victim Details:**

* IP address: 10.2.8.101
* MAC address: 00:12:79:41:c2:aa
* Host name: DESKTOP-MGVG60Z
* User account name: bill.cook

**Indicators of Compromise (IOCs):**

* **File Name:** uninviting.php
  + SHA256 hash: 858aac988e85075348f32e4750f17bf5c16e579fff258d3def9f23563e89372d
  + File Size: 1.05MB
  + File Type: HTML/TXT
  + File Location: tonmatdoanminh.com
  + IP Location: Vietnam (Latitude: 16.1667, Longitude: 107.8333)
  + File Description: The file utilizes obfuscation techniques (Base64 encoding) and a deceptive file name (.doc) to conceal its malicious nature. Upon execution, it downloads a binary file, potentially malware, through a hidden download link.
* **File Name:** 6lhjgfdghj.exe
  + SHA256 hash:N/A
  + File Size: 267.01 KB
  + File Type: win32.exe (Executable)
  + File Location: roanokemortgages.com
  + IP Location: United Kingdom (Latitude: 51.4964, Longitude: -0.1224)
  + File Description: This file is associated with Win32/Ficker Stealer, a malware known for its information-stealing capabilities.
* **File Name:** 6Aov
  + SHA256 hash: N/A
  + File Size: 203.56KB
  + File Type: Unknown
  + File Location: 198.211.10.238
  + IP Location: Canyon Country, US (Latitude: 34.413, Longitude -118.4269)
  + File Description: This file appears to be related to Cobalt Strike Beacon, a post-exploitation tool often used by attackers for further compromise and lateral movement within a network.

**Malicious HTTP traffic:**

**Tordal/Hancitor/Chanitor:**

* 45.124.85.55 (tonmatdoanminh.com): HTTP GET /uninviting.php (malicious script download)
* 54.235.147.252 (api.ipify.org): HTTP GET (likely IP address checking)
* 213.5.229.12 (satursed.com): HTTP POST /8/forum.php (potential C2 communication)

**Win32/Ficker Stealer:**

* 8.208.10.147 (roanokemortgages.com): HTTP GET /6lhjgfdghj.exe (malware download)
* 185.100.65.29 ([invalid URL removed]): TCP communication (unknown purpose)
* 54.235.147.252 (api.ipify.org): HTTP GET /?format=xml (likely IP address checking)

**Cobalt Strike Beacon:**

* 8.208.10.147 (roanokemortgages.com): HTTP GET /0801.bin, HTTP GET /0801s.bin (Cobalt Strike payloads)
* 198.211.10.238 (undefined.hostname.localhost):
  + HTTP GET /6Aov, HTTP GET /ca (potential Cobalt Strike staging)
  + HTTP POST /submit.php/id=3275377518 (potential C2 communication)
  + HTTPS traffic (encrypted, further analysis needed)

**Conclusion:**

The analysis of the network traffic paints a clear picture of a targeted, multi-stage attack. It began with a deceptive website luring the victim into downloading a malicious file through obfuscated JavaScript code. This initial foothold was then leveraged to deploy additional malware, including the information-stealing Win32/Ficker Stealer and the powerful post-exploitation framework Cobalt Strike Beacon.

This attack chain demonstrates the sophistication of modern cyber threats and the importance of proactive defense strategies.

**Recommendations:**

* **Immediate Actions:**
  + Isolate the infected laptop from the network to prevent further spread.
  + Reformat the hard drive and reinstall the operating system from a known good source.
  + Change passwords for all online accounts that may have been compromised.
* **Preventive Measures:**
  + Educate users about the risks of downloading files from untrusted sources.
  + Implement robust antivirus and anti-malware solutions.
  + Keep all software up-to-date with the latest security patches.