**INCIDENT REPORT: TS-18987-Defensive: Malware Deep Investigation**

**Date: 06/20/24**

**Executive summary:**

This User Story involves identifying how the victim computer was infected with malware based on the retrieved PCAP traffic. Upon infection, the victim’s bank account was hacked.

**Narrative:**

Using Wireshark, I was able to identify the Victim Details, which are listed below. This included conducting a Kerberos search to identify the Windows User Name. I then exported the HTTP Objects associated with the PCAP, but VirusTotal did not indicate any malware among the exported files.

In reviewing the traffic, I noticed that on 12/03/2019 at 22:50:25 UTC, URL w8.wensa.at was immediately visited following access to the URL mail.aol.com, where the victim’s email account resides. By 23:08:03 UTC, the victim’s computer connected with Bank of America.

**Conclusion:**

This incident appears to be caused by the victim clicking on a phishing email in her AOL email account. Although I was unable to export any malicious files from the PCAP, the wensa.at URL is identified in VirusTotal as being associated with the Ursnif Trojan which is commonly used in stealing banking credentials.

**Victim Details:**

* **IP Address:**  10.18.20.97
* **MAC Address:** 00.01.24.56.9b.cf; Acer
* **Operating System:** Windows 7
* **Hostname:** juanita-work-PC
* **Windows User Account:** momia.juanita

**Indicators of compromise (IOCs):**

* **Malware Name/Type/File:** Ursnif Trojan
* **Domain:**  wensa.at
* **IP Address:**  8.208.24.139