**INCIDENT REPORT: TS-18970-Defensive: What’s the Payload?**

**Date: 06/18/24**

**Executive summary:**

This User Story involved a friend sending me a link to get a free premium membership to a subscription service. After clicking on the link, my system is no longer operating properly. I am tasked with examining the associated PCAP file to determine the exploit kit, the payload, and the compromised website that started the infection

**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 compromised website, likely payload, and exploit kit.

**Conclusion:**

My research identified the compromised website as “vitaminsthatrock.com”. VirusTotal identified the malware as likely being the Gameover Zeus Trojan. Internet research yielded the commonly-associated Exploit Kit as being BlackHole. The key preventative measure in this instance is to avoid clicking links in suspicious emails.

**Victim Details:**

* **Hostname:** GOOGENHEIM-PC
* **IP Address:**  192.168.137.239
* **MAC Address:** 00:02:a5:1c:d4:92

**Indicators of compromise (IOCs):**

* **Exploit Kit:** BlackHole
* **Payload:** Gameover Zeus Trojan
* **Compromised Website:**  vitaminsthatrock.com
* **IP Address:**  64.20.39.203
* **SHA256 Hash:** d982500af8fddce64c61fa397f4f8fe0f80e941cb0d203d12d5d340fccd16083