**INCIDENT REPORT: TS-18955-Defensive: Malware Traffic**

**Date: 06/12/24**

**Executive summary:**

User Story indicated that the victim was visiting sites to download free movies. Victim’s computer is now encrypted as of 05/17/2015 at approx. 4:51 p.m.

**Narrative:**

After identifying three suspicious hostnames/domains involved(listed below) via HTTP filter on Wireshark, I then exported potentially suspicious HTTP Objects. These Objects were uploaded to VirusTotal, where the Macromedia Shockwave Flash file “%2f” was identified as a Trojan.

**Conclusion:**

This Trojan file resulted in the victim’s computer falling victim to a ransomware attack, and they have been directed to pay a fee of $700 USD to be provided access to the CryptoWall Decrypter program.

**Victim details:**

* **IP Address:** 192.168.138.158
* **MAC Address:** 00:00:00:00:00:00

**Indicators of compromise (IOCs):**

**SHA256 hash:** 81523163b298f2543d5f56a4c44ef8b07c6c9b3844b629b04fb870ca356c1437

* File Name: %2f
* File Size: 8.76 KB
* File Type: Flash
* File Location: http://ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in/
* File Description: Trojanytes)

**Malicious HTTP traffic:**

* 62.75.195.236, Port 80, http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in, GET /?285a4d4e4e5a4d4d4649584c5d43064b4745

**Suspicious domains using HTTP traffic:**

* http://runlove.us
* http://comarksecurity.com
* http://7oqnsnzwwnm6zb7y.gigapaysun.com