**INCIDENT REPORT: TS-18967-Defensive: Malicious Email**

**Date: 06/17/24**

**Executive summary:**

Due to a mail filter outage, the Turkey Mania company received a large amount of malicious email traffic. Employee Arthur Stoyt opened one of these malicious emails and caused an attachment to be executed. Turkey Mania needs to determine which email was accessed. They provided four emails that Stoyt received, as well as a PCAP file to assist.

**Narrative:**

Using Wireshark, I was able to identify the Victim Details. I reviewed the provided emails, and upon accessing the email attachments from each one, I was able to confirm that all four were malicious files when the files were uploaded to VirusTotal. VirusTotal identified associated URLs with the files, which were checked against the provided PCAP traffic in Wireshark. The results are outlined below.

**Conclusion:**

It was determined that the Interfax Service email, via [incoming@interfax.net](mailto:incoming@interfax.net), received Nov. 6, 2015, was the email that was accessed by Stoyt. The email contained a zipped version of the malicious file [fax000497762.doc.js](https://www.virustotal.com/gui/). VirusTotal indicated that this file is associated with the malware known as Nemucod, and https://kennedy.sitoserver.com is a common URL associated with the malicious file. PCAP traffic indicated that this site was accessed with Stoyt’s account on Nov. 6, 2015 at approx. 22:22:38 UTC.

**Victim Details:**

* **Hostname:** STROUT-PC
* **IP Address:** 10.3.66.103
* **MAC Address:** 00:24:e8:2d:90:81

**Indicators of compromise (IOCs):**

* **Malware Name/Type:** Nemucod Trojan, file: [fax000497762.doc.js](https://www.virustotal.com/gui/)
  + **IP Address:** 174.121.246.162
  + **Domain/URL:** https://kennedy.sitoserver.com
  + **SHA256 Hash:** c410086a1075dc1210aa7e2ff8f3040d860ca7c98e8805ff5e29b4c1617cbce4