**Incident Report:** CH-15099-Defensive-Malicious-Email

**Date:** 10-24-2022

**Executive Summary:**

During a mail filter outage on 11-06-2015, an employee at Turkey Mania opened an email attachment containing a malicious file, subsequently infecting his computer.

**Date and Time of Infection:** 11-06-2015 at approximately 22:22 UTC

**Victim Details:**

* IP Address: 10.3.66.103
* MAC Address: 00:24:e8:2d:90:81 (Dell\_2d:90:81)
* Host name: Strout-PC

**Incident Summary:**

* At approximately 22:22 UTC on 11-06-2015, host Strout-PC on computer Dell\_2d:90:81 at 10.3.66.103 opened an email containing a zip folder and subsequently unzipped the file fax000497762.doc.js.
* The details of the email that was opened are as follows:
  + Subject: You have received a new fax, document 000497762
  + From: [incoming@interfax.net](mailto:incoming@interfax.net)
  + To: [arthur.stoyt@turkey-mania.co](mailto:arthur.stoyt@turkey-mania.co)
  + Received: 11-06-2015 @ 16:05
* An analysis of the suspect file using <https://beautifier.io/> and <https://playcode.io/javascript> yields the following information:
  + The malicious JavaScript contains three domain names:
    - kennedy.sitoserver.com
    - nzvincent.com
    - abama.org
  + Connecting to one of these sites causes the following on the infected device:
    - A shellcode object is created (“WScript.shell”)
    - A .exe file is saved (saveToFile(fn + n + “.exe”,2))
    - A .exe file is executed (Run((fn + n + “.exe”,2))
  + Checking against the VirusTotal database (<https://www.virustotal.com/gui/home/upload>) provided additional information regarding this file:
    - MD5: b0891ad5d08b7d59615d8f67eacd52da
    - SHA-1: bff576d43e5f94988ef05f6bec384fcdb590ed1f
    - SHA-256: c410086a1075dc1210aa7e2ff8f3040d860ca7c98e8805ff5e29b4c1617cbce4
* The PCAP of this device revealed the following suspicious traffic:
  + At 22:22:38 - communication between 10.3.66.103 and 174.121.246.162 (kennedy.sitoserver.com) through port 80 begins:
    - HTTP GET /counter/?id=5552505E160B0601161017241605070F17140507014A070B095E3C5E060A1E4A070B094A091D5E17555E555050525C50505555505E55&rnd=3090341
      * This is a DOS .exe file disguised as a .gif file
  + At 22:22:41 - two additional HTTP GET requests to the malicious host are captured
    - Both contain requests for .exe files disguised as .gif
  + Using Statistics → Conversations → TCP in Wireshark shows a large number of packets were exchanged between the infected host and the IP address 109.68.191.31
    - A check on that IP address in reveals the hostname colocation5714.tel.ru
    - At 22:23:00 - an HTTP GET request is made from the infected machine to download a suspicious file from the IP address 109.68.191.31
      * PCAP traffic associated with this host suggests this is post-infection traffic

**Conclusion:**

Based on the information provided through the relevant PCAP and aforementioned resources, the malware associated with this infection is as follows:

* File Name: fax-exec1.exe
  + File Size: 316KB
  + SHA256: f195bc9c26e0819663a907f855f6cff1125812993b89ba9d7bc48272181e2c73
  + VirusTotal details: <https://www.virustotal.com/gui/file/f195bc9c26e0819663a907f855f6cff1125812993b89ba9d7bc48272181e2c73/detection>
* File Name: fax-exec2.exe
  + File Size: 149KB
  + SHA256: 24625e658cff6564bb37fcaf2d10784dc8b1632506c44bcdea943ead12df60bb
  + VirusTotal details: <https://www.virustotal.com/gui/file/24625e658cff6564bb37fcaf2d10784dc8b1632506c44bcdea943ead12df60bb/detection>
* File Name: fax-exec3.exe
  + File Size: 454KB
  + SHA256: 47f4105cd981857f9eb1a039b60fe72b3189890abdb93798af9326c532c93c8d
  + VirusTotal details: <https://www.virustotal.com/gui/file/47f4105cd981857f9eb1a039b60fe72b3189890abdb93798af9326c532c93c8d/detection>

This infection can be traced back to an email from [incoming@interfax.net](mailto:incoming@interfax.net) received by an employee logged into 10.3.66.103 on 11-06-2015 containing the malicious file fax000497762.doc.js. Downloading this file enabled the attack host kennedy.sitoserver.com to infiltrate the victim’s device and execute further malware, creating an abundance of suspicious network traffic between the compromised client and the malicious domain server.