**Incident Report:** CH-15144-Defensive-Erik’s-Coffee-Packet-Analysis

**Date:** 10-26-2022

**Executive Summary:**

On Thurs 2020-04-23 at approximately 23:17:42 GMT, Steel Coffee employee Elmer O’Brien opened a malicious .zip file while logged into his Windows DESKTOP-GRIONXA device, infecting the local system with Qbot malware.

**Victim Details:**

* Host name: DESKTOP-GRIONXA
* IP Address: 10.0.0.167
* MAC Address: ac:16:2d:f5:37:e5
* Windows user account name: elmer.obrien

**Additional Host Information:**

There are two additional clients on this network:

* Windows host: DESKTOP-C10SKPY
  + IP Address: 10.0.0.149
  + MAC Address: c6:c2:17:f7:80:b6
  + User account name: alyssa.fitzgerald
* Ubuntu host:
  + IP Address: 10.0.0.202
  + MAC Address: c0:98:79:4a:5b:ad

**Indicators of Compromise (IOCs):**

* File name: judgement\_04222020\_318389448.vbs
  + SHA256 hash: 1c8a60fbe35465eeb3bbbc1cbe38202f01d2799caf0c452328c290110cf16beb
  + File size: 92.69 KB (94916 bytes)
  + File type: .vbs
  + File location: 158.69.28.93:80 (play.astrite.ga)
  + File description: enters system via .zip attachment containing a .vbs file that generates the malicious Windows executable wscript.exe
* File name: CMSTP.EXE (8888.png%3fuid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA==)
  + SHA256 hash: F6210DA7865E00351C0E79464A1BA14A8ECC59DD79F650F2FF76F1697F6807B1
  + File size: 1.86 MB (1950208 bytes)
  + File type: PE32 executable
  + File location: 119.31.234.40 (alphapioneer.com)
  + File description: Qbot payload file disguised as an image/png

**Network Analysis**:

* DNS Requests:
  + Domain: bg142.caliphs.my | Address: 220.158.200.181
  + Domain: afsholdings.com.my | Address: 220.158.200.181
  + Domain: alphapioneer.com | Address: 119.31.234.40
* HTTP Traffic:
  + Request to 220.158.200.181:80 (bg142.caliphs.my):
    - Request URL: /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA==
  + Request to 220.158.200.181:80 (afsholdings.com.my):
    - Request URL: /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA==
  + Request to 119.31.234.40:80 (alphapioneer.com):
    - Request URL: /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA==