**INCIDENT REPORT: BN-18986-Eriks-Coffee**

**Date: 6/24/2024**

**Executive Summary:**

Analysis of network traffic logs from Erik's Coffee Shop revealed that the system belonging to "elmer.o'brien" was infected with Qakbot malware. This infection poses a significant risk of data theft, particularly financial information, and the potential for further malware propagation within the network.

**Victim Details:**

* **Infected:**
  + **User account name: elmer.obrien (**Elmer O'Brien)
  + **Host name:** DESKTOP-GRIONXA.steelcoffee.net
  + **MAC address:** ac:16:2d:f5:37:e5
  + **IP address:** 10.0.0.167
* **Not Infected:**
  + **User account name: alyssa.fitzgerald** (Alyssa Fitzgerald)
  + **Host name:** DESKTOP-C10SKPY.steelcoffee.net
  + **MAC address:** 6c:c2:17:f7:80:b6
  + **IP address:** 10.0.0.149
  + **User account name:** Ubuntu User
  + **MAC address:** c0:98:79:4a:5b:ad
  + **IP address:** 10.0.0.202

**Indicators of Compromise (IOCs):**

**File Name:** 8888.png%3fuid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA==

* **SHA256 hash:** f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
* **File Size:** 1.86MB
* **File Type:** Win32 EXE
* **File Location(s):** alphapioneer.com, afsholdings.com.my (bg142.caliphs.my), atn24live.com
* **IP Location(s):** Singapore **(Latitude:** 1.3673**, Longitude:** 103.8014**)**
* **File Description:** This file is a common delivery mechanism for Qakbot, disguised as an image with an obfuscated query string.

**File Name:** Judgement\_04222020\_318389448.zip

* **SHA256 hash:** 75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
* **File Size:** 92.69KB
* **File Type:** ZIP
* **File Location:** play.astrite.ga
* **IP Location:** Chicago, USA **(Latitude:** 41.8486**, Longitude:** -87.6288**)**
* **File Description:** This file scans as another Qakbot file possibly relating to other malware file

**Malicious HTTP Traffic:**

* **Trojan/Qakbot:**
  + **220.158.200.181 (afsholdings.com.my, aka bg142.caliphs.my):** HTTP GET /spool/8888.png (Initial download of Qakbot malware)
  + **119.31.234.40 (alphapioneer.com):** HTTP GET /spool/8888.png (Additional download of Qakbot malware)
  + **104.24.111.29 (atn24live.com):**
    - HTTP GET /spool/8888.png (Additional download of Qakbot malware)
    - HTTP GET /cgi-sys/suspendedpage.cgi?... (Possible C2 communication)
  + **158.69.28.93 (play.astrite.ga):** HTTP GET /docs\_q50/318389448/Judgement\_04222020\_318389448.zip (Download of additional payload)

**Conclusion:**

The presence of Qakbot on the victim's system indicates a serious security breach. This malware is known for stealing banking credentials, installing additional malware, and participating in botnet activities. It is crucial to take immediate action to contain the damage, eradicate the malware, and prevent further compromise of the network.

**Recommendations:**

1. Isolate and Analyze: Immediately disconnect the infected system (DESKTOP-GRIONXA.steelcoffee.net) from the network. Conduct a thorough forensic analysis to assess the extent of the compromise and identify any stolen data.
2. Scan and Clean: Use updated antivirus and anti-malware software to scan and clean the infected system and all other systems on the network.
3. Change Passwords: Change all passwords, especially those related to online banking and sensitive accounts, as Qakbot is known to steal credentials.
4. Educate Users: Conduct security awareness training for all employees, emphasizing the risks of phishing emails and how to identify and avoid malicious attachments.
5. Patch Systems: Ensure that all systems and software are up-to-date with the latest security patches to prevent future exploitation of vulnerabilities.