**INCIDENT REPORT: BN-19004-Malicious-Email**

**Date:** June 25, 2024

**Executive Summary:**

On June 11, 2015, at approximately 10:22 PM UTC, an employee's computer was infected with multiple malware strains after opening a phishing email titled "You have received a new fax, document 000497762" from Interfax Service (incoming@interfax.net). The email contained a malicious attachment that triggered the download of the malware.

**Victim Details:**

* IP address: 10.3.66.103
* MAC address: Dell\_2d:90:81 (00:24:e8:2d:90:81)

**Indicators of Compromise (IOCs):**

* **Email:**
  + Sender: Interfax Service (incoming@interfax.net)
  + Subject: You have received a new fax, document 000497762
* **Malicious Files:**
  + HTTP GET /counter/?id=5552505E160B0601161017241605070F17140507014A070B095E3C5E060A1E4A070B094A091D5E17555E555050525C50505555505E55&rnd=3090341 (Malicious executable disguised as an image)
    - SHA256: f195bc9c26e0819663a907f855f6cff1125812993b89ba9d7bc48272181e2c73
    - File Size: 323 kB
    - File Type: Win32 EXE
    - File Location:kennedy.sitoserver.com
  + HTTP GET /counter/?id=5552505E160B0601161017241605070F17140507014A070B095E3C5E060A1E4A070B094A091D5E17555E555050525C50505555505E55&rnd=3090342 (Malicious executable disguised as an image)
    - SHA256: 24625e658cff6564bb37fcaf2d10784dc8b1632506c44bcdea943ead12df60bb
    - File Size: 153kB
    - File Type: Win32 EXE
    - File Location:kennedy.sitoserver.com
  + HTTP GET /counter/?id=5552505E160B0601161017241605070F17140507014A070B095E3C5E060A1E4A070B094A091D5E17555E555050525C50505555505E55&rnd=3090343 (Malicious executable disguised as an image)
    - SHA256: 47f4105cd981857f9eb1a039b60fe72b3189890abdb93798af9326c532c93c8d
    - File Size: 464kB
    - File Type: Win32 EXE
    - File Location:kennedy.sitoserver.com
  + HTTP GET /docs\_q50/318389448/Judgement\_04222020\_318389448.zip (Malicious ZIP file)
    - SHA256: 75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
    - File Size: 92.69KB
    - File Type: Win32 EXE
    - File Location:kennedy.sitoserver.com

**Malware Activity Observed on the Network:**

* **IP Address:** 174.121.246.162
* **Payloads:**
  + Final.exe (tagged as Trojan downloader, family labels: Kovter, Ursu, Uvpa)
  + pattern.exe (tagged as Trojan, family labels: Zbot, Boaxxe, Diple)
  + toolbox-cmd.exe (tagged as Trojan, ransomware, and downloader, family labels: Cerber, Hyteod, Ponmocup)

**Conclusion:**

The employee's computer was infected with multiple strains of malware, including a Trojan downloader and ransomware, after opening a phishing email from Interfax Service. The downloaded files subsequently communicated with a remote IP address, potentially exfiltrating data or downloading additional malware. This incident highlights the risk of email-based attacks and the importance of user education and robust email security measures.

**Recommendations:**

1. **Isolate Infected System:** Immediately quarantine the infected computer to prevent further spread.
2. **Forensic Analysis:** Conduct a thorough forensic analysis to assess the extent of the compromise and identify any data exfiltration.
3. **Restore from Backup:** If possible, restore the system from a known good backup taken before the infection.
4. **User Education:** Reinforce email security best practices, emphasizing the dangers of opening attachments from unknown sources.
5. **Email Security:** Review and strengthen email filtering solutions to block phishing emails and malicious attachments more effectively.