AL2025_17 Emerging Polyglot Malware Targets Aviation and Satellite Communication Sectors (18th March 2025)

Description

A new and previously undocumented polyglot malware is being deployed against aviation, satellite communication, and critical transportation firms in the United Arab Emirates. The malware, named Sosano, is designed to establish persistence on infected systems and allow remote command execution. Discovered by Proofpoint in October 2024, this attack campaign is linked to a threat actor known as 'UNK_CraftyCamel.' While still limited in scope, the campaign is considered advanced and dangerous, posing a serious cyber-espionage threat.

Attack Details

The polyglot malware exploits multiple file formats within a single file, allowing different applications to interpret them in various ways. This method helps attackers bypass security software that typically scans files for a single known format.

In this attack, adversaries use a spear-phishing technique, sending highly targeted emails from a compromised Indian electronics company (INDIC Electronics). The emails contain malicious URLs directing victims to a spoofed domain (indicelectronics[.]net), where they are prompted to download a ZIP archive named "OrderList.zip."

The ZIP archive includes:

- A Windows LNK (shortcut) file disguised as an Excel spreadsheet (XLS).
- Two polyglot PDF files (“about-indic.pdf” and “electronica-2024.pdf”).
  - One PDF contains HTA (HTML Application) code.
  - The second PDF includes a hidden ZIP archive.

When executed, the LNK file launches a chain of processes:

1. The LNK file triggers cmd.exe, which launches mshta.exe to execute the HTA script embedded in the first PDF.
2. The second PDF extracts a hidden ZIP archive, writing a URL file to the Windows Registry for persistence.
3. A disguised XOR-encoded JPEG file decodes and executes the Sosano backdoor (yourdllfinal.dll).

Once activated, Sosano establishes a connection with its command-and-control (C2) server (bokhoreshonline[.]com) and awaits instructions. The malware allows attackers to:

- Perform file operations.

- Execute shell commands.
- Fetch and launch additional payloads.

Indicators of Compromise (IoCs)

1. **Malicious Domains:**
   - indicelectronics[.]net
   - bokhoreshonline[.]com
2. **Malicious File Names:**
   - OrderList.zip
   - about-indic.pdf
   - electronica-2024.pdf
   - yourdllfinal.dll
3. **Processes and Techniques:**
   - Execution of mshta.exe via cmd.exe
   - Use of polyglot PDFs containing HTA scripts and hidden ZIP files
   - URL persistence mechanism in the Windows Registry

Remediation

To defend against polyglot malware threats, organizations should implement the following measures:

1. **Email Security Measures:**
   - Deploy advanced email scanning tools that inspect multiple file formats within a single file.
   - Block dangerous file types such as LNKs, HTAs, and ZIPs if they are not required in daily operations.
2. **Endpoint Protection:**
   - Use endpoint security solutions capable of detecting multi-format malicious files.
   - Monitor system activity for unusual processes involving mshta.exe and cmd.exe executions.
3. **User Awareness and Training:**
   - Educate employees about spear-phishing tactics and suspicious email indicators.
   - Encourage users to report unexpected file downloads and email attachments.
4. **Network Security:**
   - Block known malicious domains and IP addresses associated with this attack.
   - Monitor outbound network traffic for unexpected C2 communications.
5. **Regular System Audits:**
   - Conduct frequent security assessments to identify and remove unauthorized registry modifications.
   - Keep software, including security solutions, updated to prevent exploitation of vulnerabilities.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- FadilpaŠI, S. (2025, March 5). Aviaton firms hit by devious new polyglot malware. Retrieved from TechRadar. https://www.techradar.com/pro/security/aviaton-firms-hit-by-devious-new-polyglot-malware
- Toulas, B. (2025, March 4). New polyglot malware hits aviation, satellite communication firms. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-polyglot-malware-hits-aviation-satellite-communication-firms/