مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Sosano Backdoor Malware Used in UAE-Targeted Attacks

Tracking #:432316931

Date:05-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers have identified a highly targeted email-based campaign, tracked as UNK_CraftyCamel, targeting organizations in the United Arab Emirates (UAE) with a distinct focus on aviation, satellite communications, and critical transportation infrastructure.

TECHNICAL DETAILS:

Security researchers have identified a highly targeted cyber-espionage campaign by an emerging threat cluster designated UNK_CraftyCamel. The campaign specifically targeted organizations in the United Arab Emirates (UAE) within the aviation, satellite communications, and critical transportation infrastructure sectors. Attackers leveraged a compromised Indian electronics company to send spear-phishing emails containing malicious polyglot files, ultimately deploying a new Golang-based backdoor named "Sosano.

Technical Details:

Attack Delivery and Infection Chain

- **Initial Access:** Phishing emails were sent using a compromised account from "INDIC Electronics," a legitimate Indian electronics company. The emails contained URLs linking to a spoofed domain (indicelectronics[.]net) hosting a malicious ZIP file.
- **Payload Delivery:** The ZIP archive contained:
  - An XLS file that was actually an LNK file with a double extension.
  - Two PDF files, both of which were polyglot files with hidden malicious components.
- **Execution and Malware Deployment:**
  - The LNK file executed cmd.exe, which then launched mshta.exe to process the first PDF/HTA polyglot file.
  - The HTA script orchestrated the infection, extracting an executable (Hyper-Info[.]exe) and a disguised JPG file (sosano.jpg).
  - The JPG file was XOR-encrypted and contained a DLL payload (yourdllfinal.dll), which is the Sosano backdoor.

Sosano Backdoor Capabilities

- Developed in Golang and bloated with unused libraries for obfuscation.
- Executes delayed execution to evade sandbox detection.
- Establishes a connection to the C2 server (bokhoreshonline[.]com) and awaits commands.
- Supports commands including:
  - **sosano**: Retrieve/change the working directory.
  - **yangom**: List directory contents.
  - **monday**: Download and load additional payloads.
  - **raian**: Delete/remove a directory.
  - **lunna**: Execute a shell command.
- The backdoor attempts to download and execute a next-stage payload (cc[.]exe), though this file was not available for analysis.

Threat Actor Attribution and Targeting

- Proofpoint tracks this activity as UNK_CraftyCamel.
- Shares TTPs with Iranian-aligned threat actors TA451 and TA455.
- Demonstrates interest in aviation, satellite communications, and critical infrastructure in the UAE.

- Highly selective targeting suggests an advanced threat actor with significant operational security awareness.

Technical Detection Opportunities

- Monitor for LNK files executing from recently unzipped directories.
- Detect persistence mechanisms such as URL files in registry run keys.
- Flag executable files accessing JPG files in user directories.
- Analyze network activity for connections to known malicious infrastructure, including:
  - indicelectronics[.]net
  - bokhoreshonline[.]com

Indicators of Compromise:

Indicator	Type	Context
indicelectronics[.]net	Domain	Delivery
46.30.190[.]96	IP	Delivery
336d9501129129b917b23c60b01b56608a444b0fbe1f2fdea5d5beb4070f1f14	SHA256	OrderList.zip
394d76104dc34c9b453b5adaf06c58de8f648343659c0e0512dd6e88def04de3	SHA256	OrderList.xlsx.lnk
e692ff3b23bec757f967e3a612f8d26e45a87509a74f55de90833a0d04226626	SHA256	electronica-2024.pdf
0c2ba2d13d1c0f3995fc5f6c59962cee2eb41eb7bdbba4f6b45cba315fd56327	SHA256	Hyper-Info[.]exe
bokhoreshonline[.]com	Domain	C2
104.238.57[.]61	IP	C2
0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c	Hash	Sosano DLL

RECOMMENDATIONS:

1. **Email Security Enhancements**:
   - Deploy advanced email filtering solutions to detect and block spearphishing emails, including those with malicious URLs or attachments.
   - Monitor for domain impersonation and typosquatting, particularly in emails from trusted contacts.
2. **Endpoint Detection and Response (EDR)**:
   - Implement EDR solutions to detect suspicious activities such as LNK files executing from unzipped directories, URL files in registry run keys, or executables accessing JPG files in user directories.
   - Enable behavioral analysis to identify and block obfuscated payloads and polyglot file exploitation.
3. **User Awareness Training**:
   - Train employees to recognize and report suspicious emails, especially those containing unexpected attachments or links, even if they appear to come from trusted sources.

- Emphasize the risks of opening files with double extensions (e.g., .pdf.exe) or files from unknown origins.

4. **Network Monitoring**:
   - Block traffic to known malicious domains and IPs associated with this campaign.
   - Monitor for unusual outbound HTTP GET requests to unknown domains, which may indicate C2 communication.
5. **Supply Chain Risk Management**:
   - Assess and monitor third-party vendors and suppliers for potential security risks, particularly those with access to sensitive systems or data.
   - Implement strict access controls and segmentation to limit the impact of supply chain compromises.
6. **Threat Hunting**:
   - Proactively hunt for indicators of compromise (IOCs) associated with this campaign, including the Sosano backdoor, polyglot files, and related TTPs.
   - Leverage threat intelligence feeds to stay updated on emerging threats and adversary tactics.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot