Unmasking UNK_CraftyCamel: A Threat Intelligence Perspective



.By Mario Rojas, Senior Security Researcher

Executive Summary

A recent Proofpoint investigation uncovered a highly sophisticated, multistage cyber espionage operation targeting key sectors in the **United Arab Emirates**. The actor, tracked by Proofpoint as **UNK_CraftyCamel**, executed a meticulously-crafted campaign against a limited number of high-value organsations with interests in **aviation, satellite .communications, and transportation infrastructure**

This operation underscores the growing complexity of targeted attacks leveraging .advanced social engineering and multi-format obfuscation techniques

This report provides an **intelligence-driven analysis** of the campaign, its implications for **enterprise security leaders and intelligence teams**, and key defensive strategies to .mitigate the risks posed by this emerging threat

Threat Actor Profile and Strategic Context

The operational footprint of UNK_CraftyCamel aligns with espionage-motivated activity. The use of a **compromised** Indian electronics company **email account** to distribute malicious payloads indicates a deliberate effort to exploit trusted relationships within targeted industries. The highly selective targeting and tailored malware development suggest an .actor with significant **technical capability and intelligence objectives**

The geopolitical context further strengthens this hypothesis. The UAE's strategic position in **global aviation, critical infrastructure, and defence alliances** makes it an attractive target for state-sponsored cyber espionage operations. This campaign signals an intent to infiltrate and establish persistent access within organisations handling sensitive geopolitical .or defence-related information

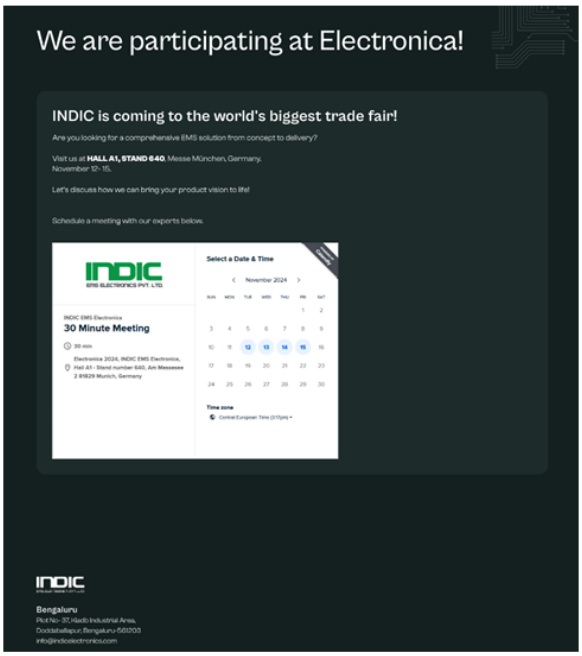
Technical Analysis of the Attack Chain

Delivery and Infection Chain Analysis

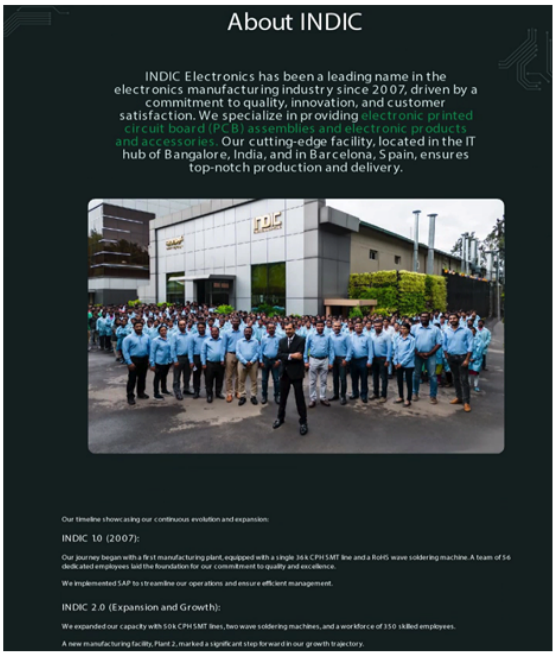
In late October 2024, UNK_CraftyCamel actor leveraged access to a **compromised email account, belonging to the Indian electronics company INDIC Electronics,** to send malicious email messages. These emails contained URLs pointing to an actor-controlled domain, **indicelectronics[.]net**, designed to mimic the legitimate INDIC Electronics .domain

The URLs linked to **https://indicelectronics[.]net/or/1/OrderList.zip**, which downloaded a ZIP archive. At first glance, the archive contained an **XLS file and two PDF files**, but :Proofpoint's analysis revealed

- .The **XLS file was actually an LNK file** using a double extension
- The **PDF files were polyglots:** one had a PDF file appended with an HTA script, and .the other contained an embedded ZIP archive



electronica-2024.pdf



about-indic.pdf

Polyglot Files and Execution Techniques

Polyglot files are crafted to be interpreted as multiple different formats depending on the application reading them. This technique exploits **format-specific quirks and overlapping headers**, making detection more challenging. The LNK file launched .**cmd[.]exe**, which in turn used **mshta[.]exe** to execute the **PDF/HTA polyglot file**

Target path	My Computer (Computer) : C:\Windows\system32\cmd.exe
Icon location	%PROGRAMFILES%\Microsoft Office\root\vfs\Windows\Installer\{90160000-000F-0000-1000-0000000FF1CE}\xlicons.exe
Command line arguments	/c mshta.exe "%cd%\electronica-2024.pdf" &&' C:\Windows\System32\cmd.exe '

Source: VirusTotal

:Execution Chain

- **LNK file execution** → Launches cmd.exe
- **cmd.exe triggers mshta.exe** → Executes **HTA script** inside the polyglot PDF
- (**HTA script writes a URL file** to the Windows Registry (persistence
- **The URL file is launched,** downloading and executing Hyper-Info[.]exe
- (**Hyper-Info[.]exe** searches for sosano.jpg (embedded in the ZIP polyglot
- (**sosano.jpg** is XOR-decoded into Sosano backdoor (DLL

:Mitigation Strategy

- .Monitor execution of LNK files from unzipped directories
- .Detect unusual mshta.exe behaviour triggering external script execution
- Deploy behavioural analytics to identify execution anomalies in Registry .modifications
- Leverage digital risk protection solutions like Discovery to monitor for compromised .credentials, which were key in enabling this attack

Sosano Backdoor

According to Proofpoint, the Sosano backdoor is a DLL written in Golang and designed to evade analysis through excessive code bloating. Despite being 12MB in size, it contains only a limited set of malicious functions, while embedding unnecessary Golang packages to .complicate reverse engineering

Sosano's Key Capabilities

:Upon execution, Sosano

- .(**Sleeps for a random time** using system time as a seed (evades sandbox analysis
- .**(Attempts to connect to its C2 server (bokhoreshonline[.]com**
- .**Sends periodic HTTP GET requests to await commands**
- :**Executes attacker-provided commands,** including
  - .sosano → Get current directory/change working directory ◦

- .yangom → List contents of current directory
- .monday → Download and load additional payload
- .raian → Delete/remove a directory
- .lunna → Execute a shell command

:Mitigation Strategy

- **.Monitor** outbound HTTP traffic for periodic **C2 beaconing patterns**
- .Implement SSL/TLS decryption and anomaly detection
- Deploy DNS security solutions like DNS Firewall to detect and block C2 communications.

(Indicators of Compromise (IoCs

Malicious Domains and C2 Infrastructure

Indicator	Type
indicelectronics[.]net	Domain
bokhoreshonline[.]com	Domain
96[.]46.30.190	IPv4
61[.]104.238.57	IPv4

File Hashes

Indicator	Hash
OrderList.zip	336d9501129129b917b23c60b01b56608a444b0fbe1f2fdea5d5beb4070f1f14
OrderList.xlsx.lnk	394d76104dc34c9b453b5adaf06c58de8f648343659c0e0512dd6e88def04de3
electronica-2024.pdf	e692ff3b23bec757f967e3a612f8d26e45a87509a74f55de90833a0d04226626
Hyper-Info[.]exe	0c2ba2d13d1c0f3995fc5f6c59962cee2eb41eb7bdbba4f6b45cba315fd56327
Sosano DLL	0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c

Recommendations for Mitigation and Risk Reduction

- Proactive Threat Hunting and Intelligence Integration
  - Monitor LNK files executing from unzipped directories.
  - Analyse HTA execution via mshta.exe for abnormal process behaviours.
  - Implement digital risk protection solutions like Discovery to continuously monitor for compromised credentials that may be used in similar targeted attacks
- Strengthening Email Security Posture
  - Deploy advanced email filtering solutions capable of detecting polyglot file anomalies.
  - Enforce Multi-Factor Authentication (MFA) for all email accounts to prevent credential-based takeover attempts.
  - Leverage Discovery to monitor email security posture by analysing DMARC, DKIM, and SPF records, ensuring proper authentication configurations to prevent spoofing and unauthorised email use.
- Enhancing Network Security Controls
  - Implement zero-trust architecture (ZTA) with strict access segmentation.
  - Deploy network anomaly detection for encrypted outbound traffic to flag suspicious HTTPS C2 channels.
  - Utilise DNS security solutions like DNS Firewall to detect and block connections to malicious domains used in C2 communication.

Conclusion:

The emergence of **UNK_CraftyCamel** represents a clear shift towards highly customised, multistage attacks leveraging file format manipulation, LOLBins, and covert C2 channels. This campaign is not just a technical challenge but a strategic risk that necessitates cross-disciplinary intelligence collaboration.

For **CISOs, Directors, and Security Decision-Makers,** this underscores the importance of:

- **Proactive intelligence sharing** between industry peers and government bodies.
- **Investing in adversary emulation exercises** to validate detection and response capabilities.
- **Aligning cybersecurity priorities with business risk mitigation**, ensuring that executive teams understand the impact of targeted cyber espionage.

In an era where **attack sophistication outpaces traditional defences,** organisations must evolve towards **intelligence-led security strategies** to stay ahead.

Remember, there’s always more intelligence to uncover.