Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

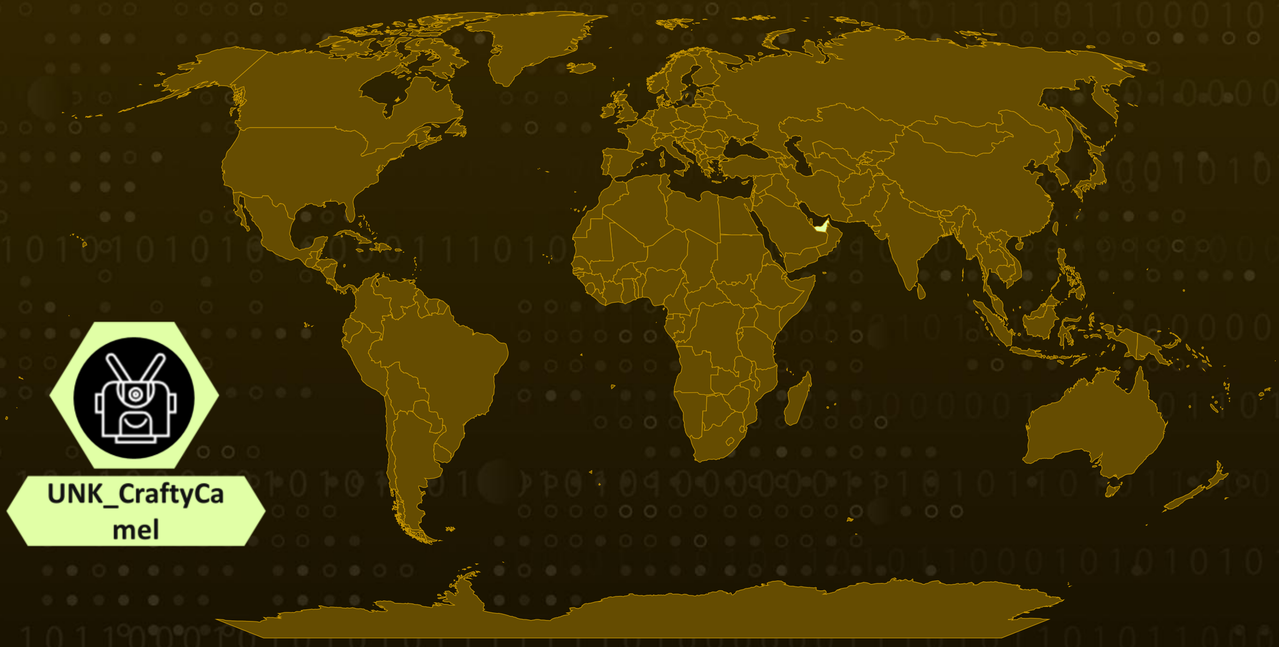
UNK_CraftyCamel: A New Cyber Threat Lurking in the Satellite Sector

Date of Publication	Admiralty Code	TA Number
March 6, 2025	A1	TA2025066

Summary

Attack Discovered: October 2024
Targeted Countries: United Arab Emirates
Actor: UNK_CraftyCamel
Malware: Sosano
Targeted Industries: Aviation and Satellite
Attack: A highly sophisticated cyber espionage campaign has been uncovered, targeting aviation and satellite communications firms in the United Arab Emirates. The operation, attributed to the threat actor UNK_CraftyCamel, exploited a compromised Indian electronics company to deliver tailored malware to its victims. This attack led to the discovery of a previously unknown backdoor, dubbed Sosano. The malware employs multiple layers of obfuscation, suggesting that its developers possess advanced technical expertise and significant resources.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 A newly emerging threat actor, UNK_CraftyCamel, has been identified targeting multiple organizations in the UAE, using polyglot files to deliver a custom Go-based backdoor named Sosano. The attackers employed malicious ZIP archives containing hidden LNK files masquerading as XLS documents, enabling the execution of malicious scripts and ensuring persistence within compromised systems. The UNK_ designation signifies an evolving cyber threat cluster currently under investigation.

#2 In October 2024, the attackers weaponized a compromised email account belonging to INDIC Electronics to distribute spear-phishing emails. These emails contained links to a fraudulent domain, which delivered a ZIP archive comprising two PDF files and an XLS file. However, the XLS file was actually an LNK file with a deceptive double extension, crafted to execute a PDF/HTA polyglot file. This HTA script acted as the attack's orchestrator, extracting an executable and a URL file from the second PDF. The payload then executed Hyper-Info[.]exe, which sought out the final malware component "sosano.jpg" embedded within the ZIP archive.

#3 The Sosano backdoor, built in Golang, is designed for stealth and persistence. While its core functionality appears limited, it features a bloated codebase packed with unnecessary Golang libraries to hinder analysis. The malware employs randomized sleep intervals to evade sandbox detection before establishing contact with its command-and-control (C2) server. Once active, it awaits specific commands, including "sosano," "yangom," "monday," "raian," and "lunna," which allow attackers to execute tasks and deploy additional payloads. Although the campaign's final-stage payload, "cc[.]exe," was unavailable at the time of analysis, the attack chain suggests sophisticated evasion techniques and long-term persistence capabilities.

#4 The tactics observed in this campaign closely align with methods previously attributed to Iranian state-sponsored groups TA451 and TA455, known for targeting aerospace organizations through HTA-based spear-phishing campaigns in the UAE. These adversaries frequently leverage business-themed lures to infiltrate high-value targets, particularly engineers and professionals with access to sensitive systems.

Recommendations

Enhance Email Security: Implement robust email filtering to block phishing emails impersonating trusted entities. Use email authentication mechanisms like DMARC, SPF, and DKIM to prevent spoofed emails. Educate employees on identifying phishing attempts.

Restrict Execution of Untrusted Files: Stop LNK and HTA files from running if they come from emails or unknown sources, as they are often used in malware attacks. Set up application whitelisting to ensure that only trusted scripts and programs can be executed on your systems.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Monitor and Restrict Unauthorized Activity: Monitor for LNK files running from newly unzipped folders, as this could signal an attack. Watch for URL files appearing in registry runkeys or attempting to connect to external servers. Flag any executables that interact with image files in user directories, as this is a known technique for hiding malware.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1036** Masquerading	**T1204** User Execution	**T1204.002** Malicious File
T1059 Command and Scripting Interpreter	**T1059.006** Python	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1083 File and Directory Discovery	**T1070** Indicator Removal	**T1586** Compromise Accounts	**T1586.002** Email Accounts

T1222 File and Directory Permissions Modification	**T1218** System Binary Proxy Execution	**T1218.005** Mshta	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	indicelectronics[.]net, bokhoreshonline[.]com
IPv4	46[.]30[.]190[.]96, 104[.]238[.]57[.]61
SHA256	336d9501129129b917b23c60b01b56608a444b0fbe1f2fdea5d5beb4070f1f14, 394d76104dc34c9b453b5adaf06c58de8f648343659c0e0512dd6e88def04de3, e692ff3b23bec757f967e3a612f8d26e45a87509a74f55de90833a0d04226626, 0c2ba2d13d1c0f3995fc5f6c59962cee2eb41eb7bdbba4f6b45cba315fd56327, 0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c

References

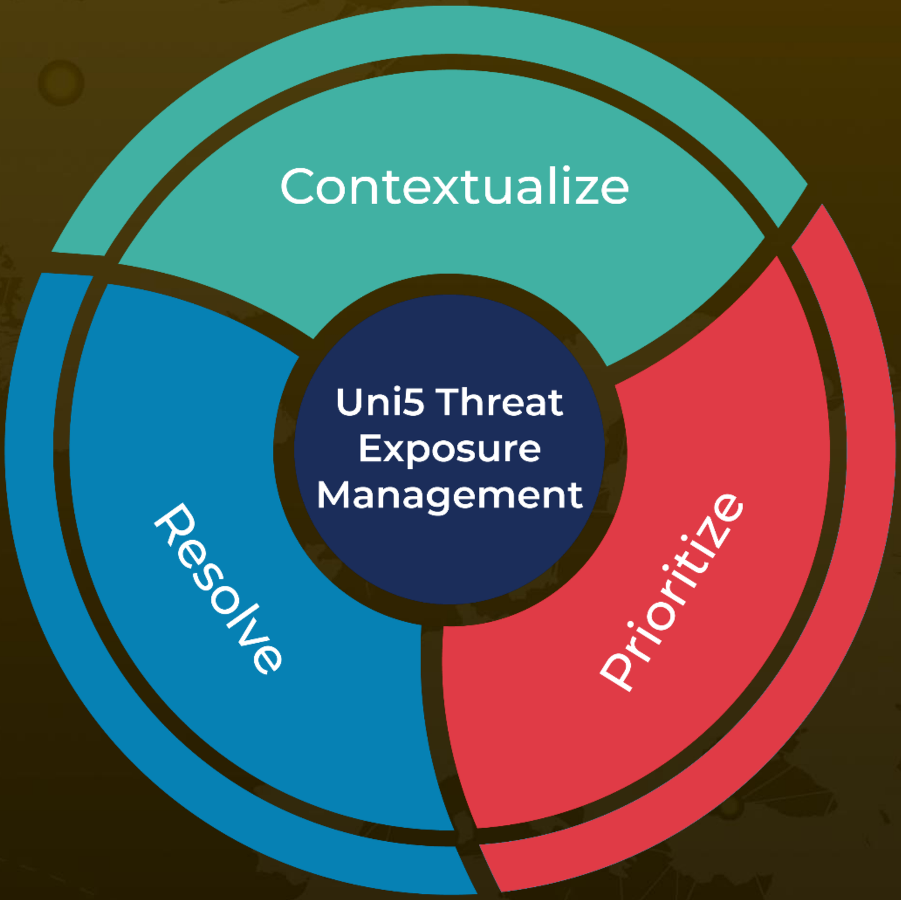
https://www.proofpoint.com/us/blog/threat-insight/call-it-what-you-want-threat-actor-delivers-highly-targeted-multistage-polyglot

https://www.hivepro.com/apt-33-uses-password-spray-campaigns-to-infiltrate-organizations/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 6, 2025 • 4:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com