Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

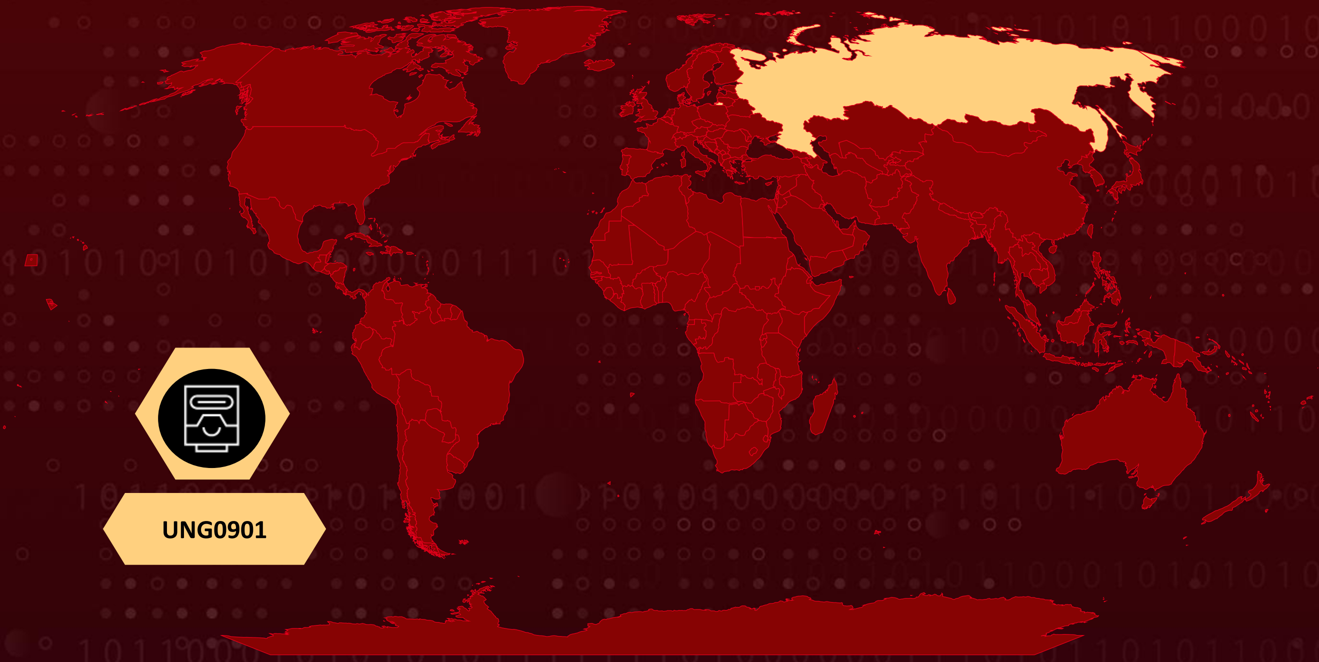
Operation CargoTalon: Targeting Russian Aerospace & Defense Sector

Date of Publication	Admiralty Code	TA Number
July 25, 2025	A1	TA2025232

Summary

First Seen: June 27, 2025
Targeted Country: Russia
Malware: EAGLET
Targeted Platforms: Windows
Campaign: Operation CargoTalon
Threat Actor: UNG0901
Targeted Industries: Aerospace and Defense
Attack: Operation CargoTalon is a targeted cyber-espionage campaign by threat group UNG0901, aimed at Russia's aerospace and defense sector. It uses malicious .LNK files to deliver the lightweight EAGLET implant, enabling stealthy data exfiltration and persistent access. The campaign highlights advanced social engineering and malware evasion tactics.

Attack Regions



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

Attack Details

#1

Operation CargoTalon is a recent cyber-espionage campaign, targeting organizations within the Russian aerospace and defense sector. Identified as UNG0901, the campaign employs a specialized malware implant named EAGLET, which is designed for stealthy surveillance and long-term persistence. The attackers rely on social engineering tactics to deliver malicious Windows shortcut (.LNK) files, which act as the initial entry point for infection.

#2

The attack chain begins with a phishing email that contains a crafted LNK file posing as a legitimate document. When executed, the file triggers a decoy document to distract the user while silently deploying the EAGLET implant in the background. This implant establishes communication with a remote command-and-control server, enabling the attacker to conduct reconnaissance, exfiltrate data, and maintain ongoing access to the victim's systems.

#3

What sets this operation apart is the lightweight and stealthy nature of the EAGLET implant. Its minimal footprint helps it evade detection by traditional security tools, making it an ideal tool for covert intelligence gathering. The targeting of Russia's defense and aerospace sectors indicates a highly strategic intent, likely aimed at acquiring sensitive military or technological data.

#4

Operation CargoTalon also draws parallels to an earlier campaign known as Operation HollowQuill, which targeted Russian research institutions using weaponized PDFs and Cobalt Strike beacons. While the two operations differ in malware tooling, both suggest a pattern of coordinated cyber-espionage aimed at weakening Russia’s defense R&D capabilities. In response to such campaigns, organizations, especially those in critical infrastructure, should enhance phishing defenses, monitor shortcut file activity, and implement advanced endpoint detection systems.

Recommendations

Enhance Email and Attachment Security: Deploy advanced email filtering to detect and block spear-phishing attempts, specifically those containing malicious attachments disguising as logistics or business documents (such as disguised DLL or LNK files). Actively monitor for suspicious file types and file extensions within inbound emails, and quarantine messages that contain executable content masquerading as archives.

User Awareness and Training: Conduct regular security awareness programs for staff, focusing on the identification of spear-phishing, social engineering lures, and suspicious attachments. Educate users about the risks associated with opening files from untrusted sources, and promote extra scrutiny for files related to logistics or supply chain themes.

Endpoint Detection and Response (EDR): Deploy modern EDR solutions with behavioral analysis capable of detecting malicious execution patterns associated with LNK scripts, PowerShell abuse, and DLL side-loading (such as EAGLET implant deployment). Monitor for the creation of suspicious directories such as C:\ProgramData\MicrosoftAppStore\, and the use of unusual GUIDs, which are part of the EAGLET implant persistence techniques.

Network Monitoring: Monitor network traffic for anomalous outbound connections, particularly those aimed at known C2 infrastructure or hosting providers in regions linked to the threat, such as Romania and Russia.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0002 Execution	TA0003 Persistence	TA0040 Impact
TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control	TA0001 Initial Access
TA0010 Exfiltration	T1041 Exfiltration Over C2 Channel	T1537 Transfer Data to Cloud Account	T1059 Command and Scripting Interpreter

T1566.001 Spearphishing Attachment	**T1059.001** PowerShell	**T1218.011** Rundll32	**T1059** Command and Scripting Interpreter
T1218 System Binary Proxy Execution	**T1566** Phishing	**T1574.002** DLL	**T1036** Masquerading
T1082 System Information Discovery	**T1482** Domain Trust Discovery	**T1071.001** Web Protocols	**T1071** Application Layer Protocol
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	01f12bb3f4359fae1138a194237914f4fcdbf9e472804e428a765ad820f399be, 02098f872d00cffabb21bd2a9aa3888d994a0003d3aa1c80adcfb43023809786, 204544fc8a8cac64bb07825a7bd58c54cb3e605707e2d72206ac23a1657bfe1e, 3e93c6cd9d31e0428085e620fdba017400e534f9b549d4041a5b0baaee4f7aff, 413c9e2963b8cca256d3960285854614e2f2e78dba023713b3dd67af369d5d08, 44ada9c8629d69dd3cf9662c521ee251876706ca3a169ca94c5421eb89e0d652, 4d4304d7ad1a8d0dacb300739d4dcaade299b28f8be3f171628a7358720ca6c5, a8fdc27234b141a6bd7a6791aa9cb332654e47a57517142b3140ecf5b0683401, a9324a1fa529e5c115232cbbc60330d37cef5c20860bafc63b11e14d1e75697c, ae736c2b4886d75d5bbb86339fb034d37532c1fee2252193ea4acc4d75d8bfd7, b683235791e3106971269259026e05fdc2a4008f703ff2a4d32642877e57429a,

TYPE	VALUE
SHA256	c3caa439c255b5ccd87a336b7e3a90697832f548305c967c0c40d2dc40e2032e, e12f7ef9df1c42bc581a5f29105268f3759abea12c76f9cb4d145a8551064204, f6baa2b5e77e940fe54628f086926d08cc83c550cd2b4b34b4aab38fd79d2a0d
MD5	08a92ba1d1d9e5c498dcaf53af7cd071, 65967d019076e700deb20dcbc989c99c, 7e52be17fd33a281c70fec14805113a8, 88453eb954669b5c7ac712ecf1e0179c, b49a7ef89cfb317a540996c3425fcdc2, be990a49fa1e3789ebc5c55961038029, d424a2d0a7481138ad219c98942cf628
SHA1	2a14a9dd1032479ab5bf8ed945ef9a22ebd4999d, 49a18dc1d8f84394d3373481dbac89d11e373dbd, 6942e07e7d08781cba571211a08e779838e72e9a, 851157c01da6e85ffa94ded7f42cab19aa8528d6, c52d70b92e41db70d4ca342c8dc32eff7883c861, c61a8f68a58461d386f443fb99346534ea7023d4, d9a4fd39a55cd20d55e00d3cace3f637b8888213
IPv4	185[.]225[.]17[.]104, 188[.]127[.]254[.]44

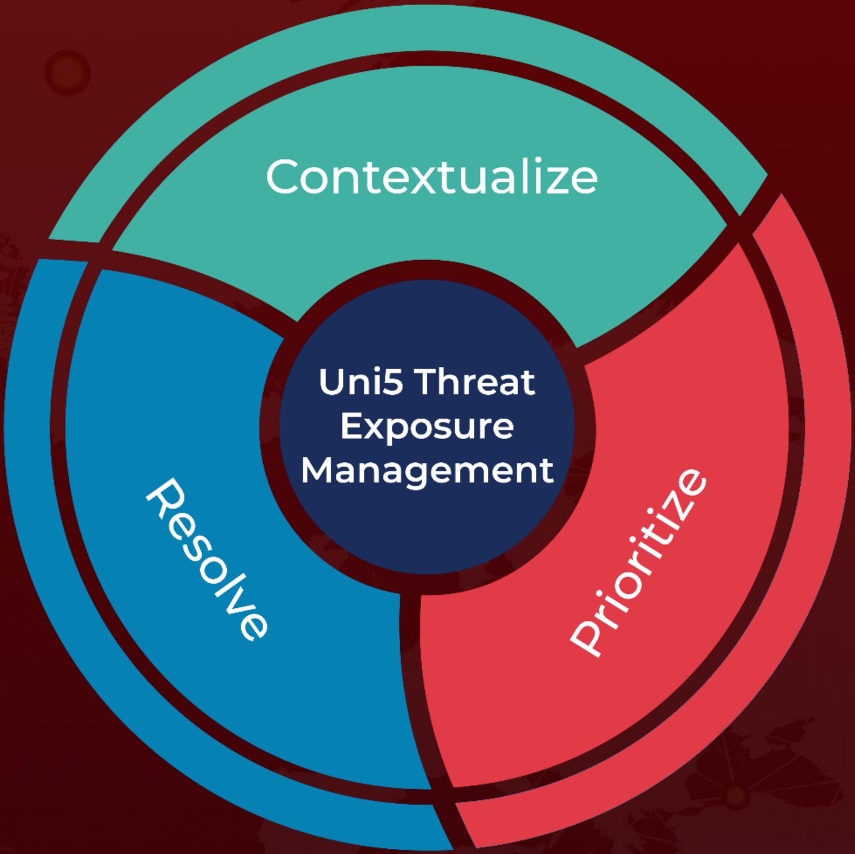
References

https://www.seqrite.com/blog/operation-cargotalon-ung0901-targets-russian-aerospace-defense-sector-using-eaglet-implant/

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

July 25, 2025 • 8:30 AM

More at www.hivepro.com