Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

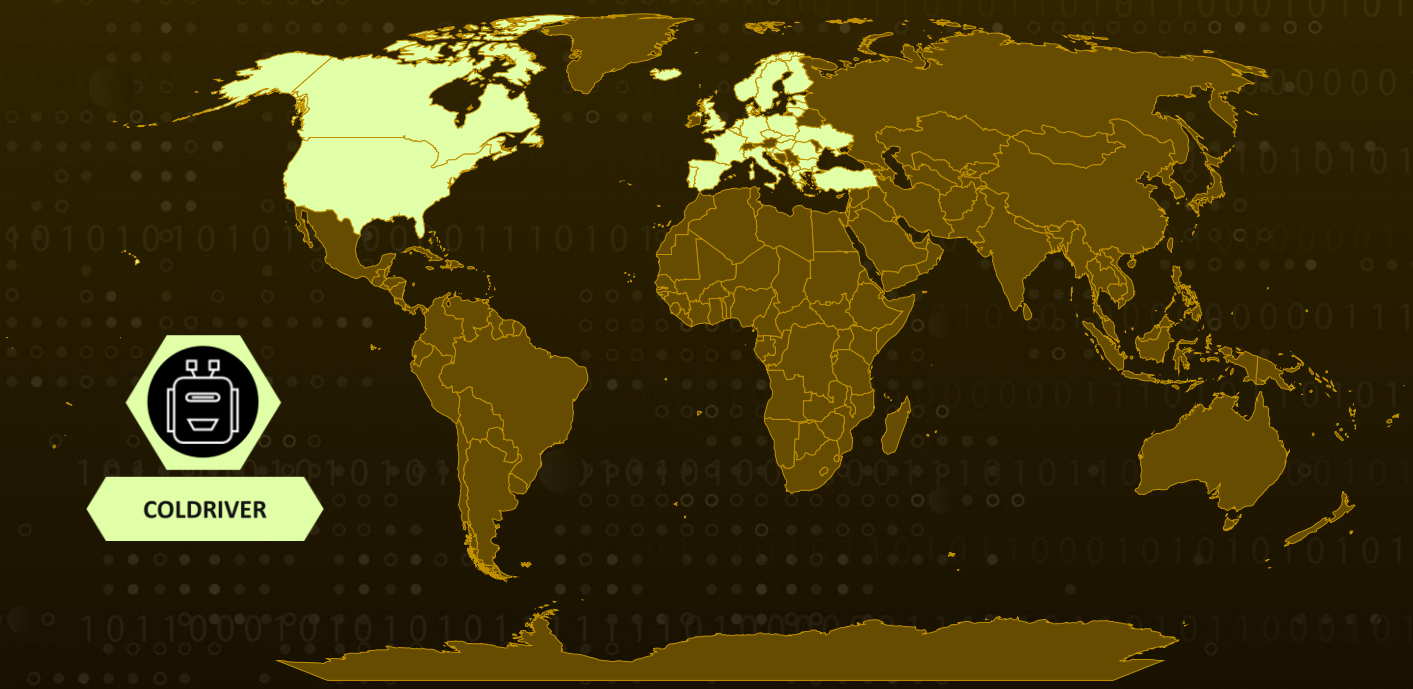
COLDRIVER Creeps Closer with LOSTKEYS Malware

Date of Publication	Admiralty Code	TA Number
May 19, 2025	A1	TA2025155

Summary

Attack Commenced: January 2025
Threat Actor: COLDRIVER (aka Star Blizzard, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, UNC4057)
Malware: LOSTKEYS
Targeted Regions: Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine, United Kingdom, United States
Targeted Industries: Governments, Militaries, Journalists, Think Tanks, NGOs
Attack: Russia-backed hacking group COLDRIVER, also known as Star Blizzard, has upped its espionage game with a new malware called LOSTKEYS. Discovered active in early 2025, this stealthy tool uses clever social engineering tricks to breach high-value targets, steal sensitive files, and evade detection. The campaign signals a sharp escalation in COLDRIVER's tactics, reinforcing the rising cyber threat from state-sponsored actors in today's volatile geopolitical climate.

Attack Regions



Attack Details

#1 The Russian state-sponsored threat group known as **COLDRIVER**, also tracked as UNC4057, Star Blizzard, and Callisto, has expanded its cyber-espionage arsenal with a newly identified malware strain dubbed LOSTKEYS. Active throughout January, March, and April 2025, LOSTKEYS represents a notable evolution following the deployment of SPICA malware in 2024.

#2 COLDRIVER's operations have traditionally revolved around credential phishing campaigns targeting high-value individuals such as intelligence officers, diplomats, NGOs, and advisors to NATO governments. These campaigns have typically served Moscow's strategic intelligence-gathering objectives.

#3 In this latest campaign, COLDRIVER has adopted a multi-stage infection process that cleverly blends social engineering with technical subterfuge. The attack begins with a phishing email leading to a malicious lure website posing as a legitimate service page. Victims are asked to complete a fake CAPTCHA as a means of "verification."

#4 Once completed, the site copies a PowerShell command directly to the user's clipboard and brazenly instructs them to paste it into the Windows Run prompt, a technique informally known as "ClickFix", employed by various threat actors to bypass email security controls and endpoint protections.

#5 If the victim complies, this PowerShell command initiates a chain of malicious actions culminating in the installation of LOSTKEYS. The malware is designed to exfiltrate files from a predefined list of file extensions and directories, capture detailed system information, and report active processes back to its operators.

#6 Adding to its sophistication, LOSTKEYS incorporates basic sandbox evasion techniques. Before proceeding to its final payload delivery, it checks the system’s display resolution hash and halts execution if it detects a known virtual machine environment.

#7 The concluding payload is a Visual Basic Script (VBS) file, decoded through a custom two-key substitution cipher, with each infection chain assigned a unique pair of keys. Once executed, this script harvests sensitive documents, collects comprehensive system diagnostics, and discreetly transmits the stolen data to remote servers under COLDRIVER’s control.

Recommendations

Enforce User Awareness and Security Training: Regularly train employees, especially those in sensitive roles, to recognize phishing, social engineering, and fake CAPTCHA scams. Conduct simulated phishing campaigns using realistic attack scenarios.

Strengthen Email and Web Security: Deploy advanced phishing filters with sandboxing for attachments and URLs. Block known malicious domains and typo-squatted URLs linked to phishing sites.

Signature and Heuristic Analysis: Ensure that the IDPS can analyze not only known malware signatures but also heuristic patterns, including dynamic runtime decryption, to flag potentially malicious behavior in real-time.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1566** Phishing
T1566.002 Spearphishing Link	**T1204** User Execution	**T1204.001** Malicious Link	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1059.005** Visual Basic	**T1027** Obfuscated Files or Information	**T1497.001** System Checks

T1497 Virtualization/Sandbox Evasion	T1082 System Information Discovery	T1057 Process Discovery	T1005 Data from Local System
T1119 Automated Collection	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	165[.]227[.]148[.]68, 80[.]66[.]88[.]67
Domains	njala[.]dev, cloudmediaportal[.]com
SHA256	13f7599c94b9d4b028ce02397717a1282a46f07b9d3e2f8f2b3213fa8884b029, 4c7accba35edd646584bb5a40ab78f963de45e5fc816e62022cd7ab1b01dae9c, 6b85d707c23d68f9518e757cc97adb20adc8accb33d0d68faf1d8d56d7840816, 3233668d2e4a80b17e6357177b53539df659e55e06ba49777d0d5171f27565dd, 6bc411d562456079a8f1e38f3473c33ade73b08c7518861699e9863540b64f9a, 28a0596b9c62b7b7aca9cac2a07b067109f27d327581a60e8cb4fab92f8f4fa9, b55cdce773bc77ee46b503dbd9430828cc0f518b94289fbfa70b5fbb02ab1847, 02ce477a07681ee1671c7164c9cc847b01c2e1cd50e709f7e861eaab89c69b6f, 8af28bb7e8e2f663d4b797bf3ddbee7f0a33f637a33df9b31fbb4c1ce71b2fee

References

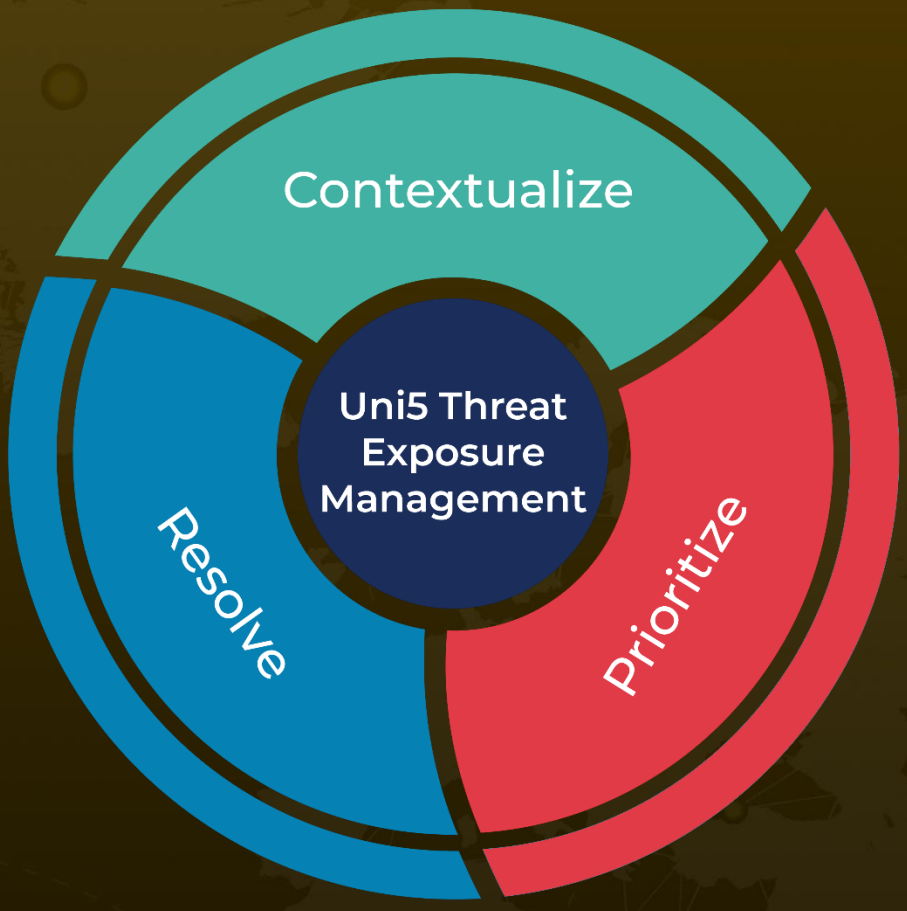
https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos

https://hivepro.com/threat-advisory/star-blizzard-continues-to-refine-their-tradecraft-for-evasion-and-stealth/

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

May 19, 2025 • 9:00 AM

More at www.hivepro.com