Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

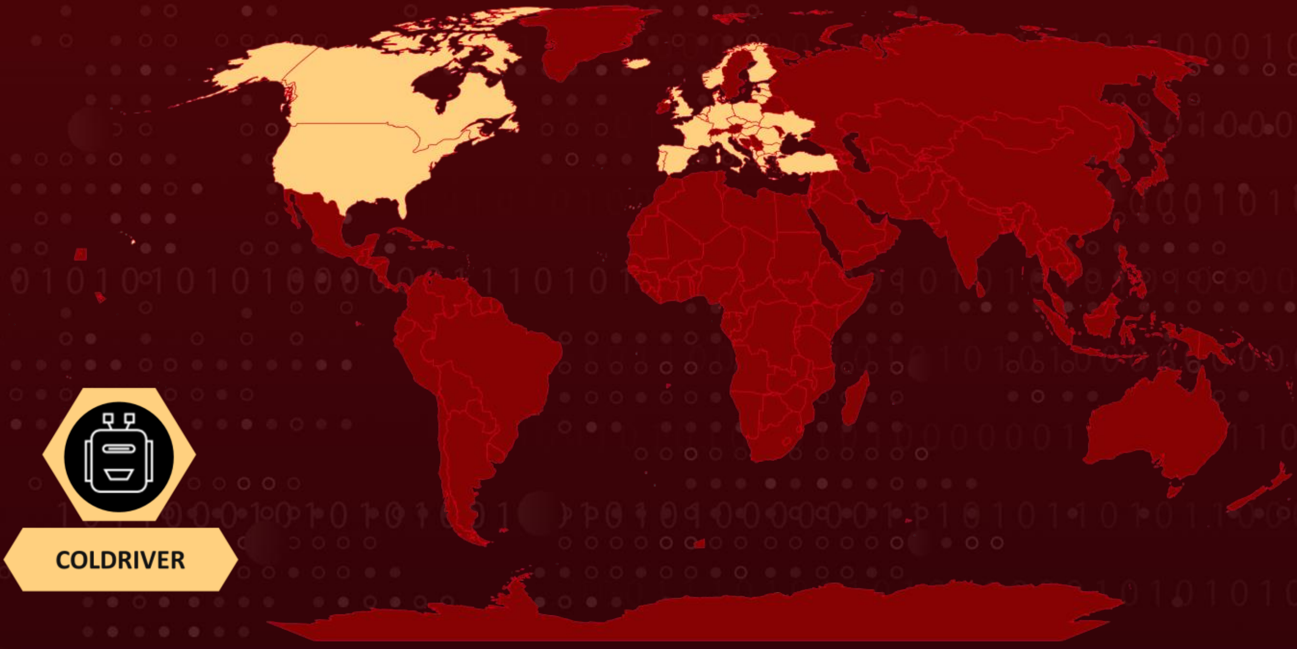
COLDRIVER Expands Beyond Phishing, Incorporating Custom SPICA Backdoor

Date of Publication	Admiralty Code	TA Number
January 19, 2024	A1	TA2024024

Summary

Attack Discovered: November 2022
Attack Region: Ukraine, NATO countries
Targeted Industries: High profile individuals in NGOs, former intelligence and military officers and NATO governments
Actor: COLDRIVER (aka Star Blizzard, Nahrelbared, NahrElbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto)
Malware: SPICA backdoor
Attack: The threat actor associated with Russia, known as COLDRIVER or Star Blizard, has expanded its tactics from mere credential harvesting. The group has initiated campaigns where PDFs are employed as lure documents to distribute malware. Notably, COLDRIVER has introduced its first custom malware, the SPICA backdoor, written in the Rust programming language.

Attack Regions



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

Attack Details

#1

COLDRIVER (aka Star Blizzard), known for targeting high-profile individuals in NGOs, former intelligence and military officials, and NATO governments, is transitioning beyond credential phishing. The group is evolving by moving from credential phishing activities to delivering malware SPICA backdoor through campaigns that utilize PDFs as lure documents.

#2

COLDRIVER has been engaging in activities where it sends seemingly harmless PDF documents to targets from impersonated accounts since November 2022. These documents are presented as encrypted, and if the target replies it is unable to read them, the impersonate account provides a link to a "decryption" utility. Tracked as SPICA, this utility serves as a means for COLDRIVER to gain access to the victim's machine. Notably, SPICA is the first custom malware developed and deployed by COLDRIVER, marking a significant evolution in their tactics.

#3

SPICA is a Rust-based script that employs JSON over websockets for command-and-control purposes. It is equipped with a range of commands, allowing actions such as shell execution, cookie theft, file uploading, and filesystem examination. SPICA undertakes the decoding of embedded PDFs, writing them to disk and opening them as decoys. Additionally, it establishes persistence in the background through a PowerShell command, creating a scheduled task named CalendarChecker.

#4

COLDRIVER is speculated to have utilized the backdoor as early as November 2022. Multiple variants of the initial PDF lure have been identified, with only one instance, "Proton-decrypter.exe," successfully retrieved. This variant was likely active between August and September 2023. It's worth noting that there might be multiple versions of the SPICA backdoor, each featuring a different embedded decoy document tailored to match the lure document sent to targets.

Recommendations

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1566.002** Spearphishing Link
T1539 Steal Web Session Cookie	**T1083** File and Directory Discovery	**T1053** Scheduled Task/Job	**T1027** Obfuscated Files or Information
T1027.010 Command Obfuscation	**T1059** Command and Scripting Interpreter	**T1204** User Execution	**T1204.001** Malicious Link
T1204.002 Malicious File	**T1560** Archive Collected Data	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0f6b9d2ada67cebc8c0f03786c442c61c05cef5b92641ec4c1bdd8f5baeb2ee1, A949ec428116489f5e77cefc67fea475017e0f50d2289e17c3eb053072adcf24, C97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d, Ac270310b5410e7430fe7e36a079525cd8724b002b38e13a6ee6e09b326f4847, 84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507, 37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9
Domain	https[:/]45.133.216[.]15:3000/ws

References

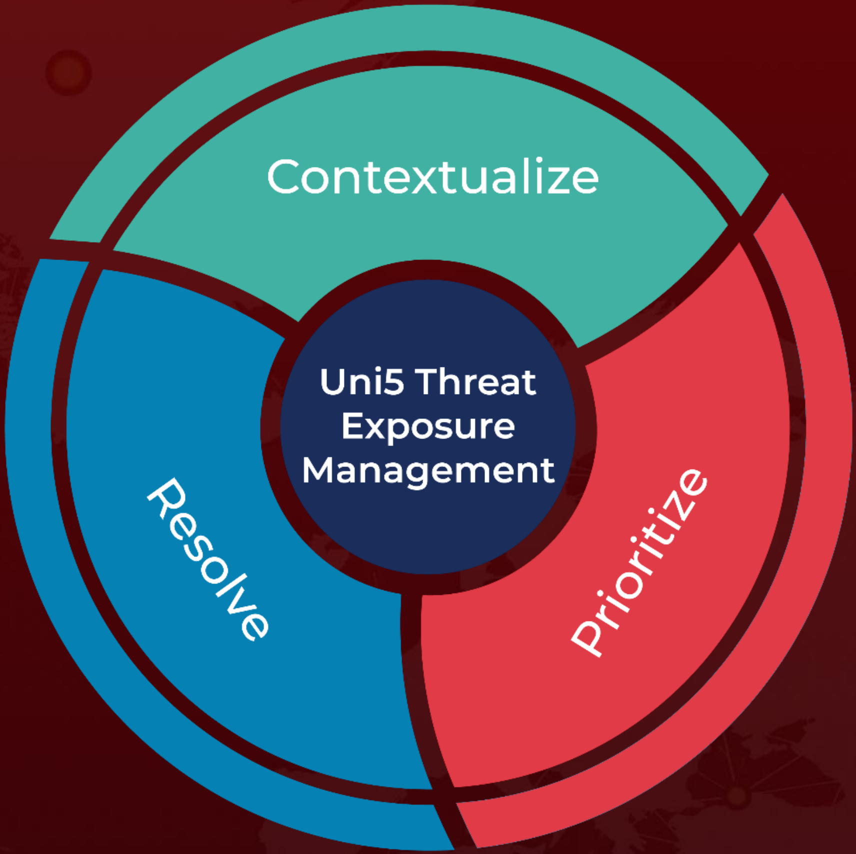
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

https://www.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

January 19, 2024 • 3:45 AM

More at www.hivepro.com