Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

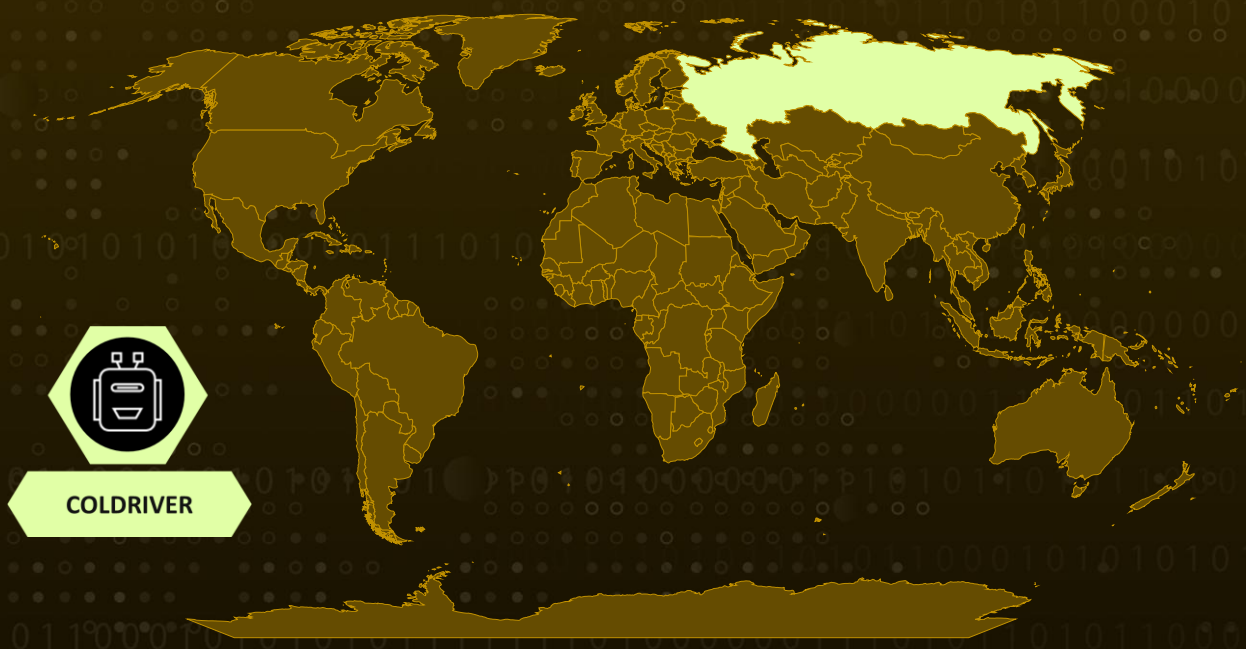
COLDRIVER's ClickFix Campaign Targets Civil Voices

Date of Publication	Admiralty Code	TA Number
September 26, 2025	A1	TA2025297

Summary

Attack Discovered: September 2025
Targeted Country: Russia
Targeted Industry: Civil Society
Actor: COLDRIVER (aka Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, Star Blizzard, UNC4057, IRON FRONTIER, Grey Pro, Mythic Ursa, Gossamer Bear)
Malware: BAITSWITCH, SIMPLEFIX
Attack: COLDRIVER has rolled out a crafty new ClickFix campaign that preys on trust and urgency to infiltrate Russia's civil society. Masquerading as support resources for activists and think tanks, the group lures victims into running malicious commands disguised as a simple "security check." This sleight of hand triggers BAITSWITCH, a downloader that quietly paves the way for the SIMPLEFIX backdoor, giving attackers remote control over compromised systems. While technically lightweight, the operation is carefully tailored to COLDRIVER's long-running mission of monitoring and undermining dissidents, showing how even modest tools, when paired with clever deception, can pose a serious threat.

Attack Regions



Attack Details

#1 In September 2025, a new ClickFix campaign targeting Russia's civil society was uncovered, linked to the threat actor COLDRIVER. Known for targeting NGOs, human rights defenders, and exiled activists, the group has expanded its arsenal with two new tools: an undocumented downloader dubbed BAITSWITCH, and a PowerShell backdoor named SIMPLEFIX. The campaign relies heavily on social engineering, with credential phishing serving as its main entry point. Attribution to **COLDRIVER** is made with medium confidence, based on overlaps in tactics, infrastructure, and victimology that strongly align with the group's past operations.

#2 The attack chain begins when a victim lands on a seemingly legitimate website disguised as a resource for Russian civil society and think tanks. Using the ClickFix method, the page deploys a clever trick: a fake Cloudflare Turnstile checkbox. When clicked, embedded JavaScript silently copies a malicious command to the victim's clipboard. The user is then nudged to paste and run this command in the Windows Run dialog, unknowingly launching BAITSWITCH through rundll32.exe. To maintain credibility, the site quickly redirects the user to a decoy Google Drive document.

#3 Once executed, BAITSWITCH sets up persistence and acts as a downloader for further payloads. It communicates with a threat actor–controlled domain using a hardcoded user-agent string, sending multiple HTTP requests to fetch instructions and eventually deliver the SIMPLEFIX backdoor. By leveraging CreateProcessA, BAITSWITCH executes commands directly on the endpoint, providing the attackers with an initial foothold.

#4 The next stage unfolds with a PowerShell stager that decodes and decrypts hidden payloads stored within obscure Windows registry keys. Using obfuscated Base64 and AES-encrypted data, the stager loads and executes SIMPLEFIX. This backdoor maintains persistence by running loops at regular three-minute intervals, dynamically generating user-agent strings, and sending periodic signals back to the command-and-control (C2) infrastructure.

#5 At its core, this campaign showcases COLDRIVER's steady evolution in combining social-engineering lures with lightweight custom malware. By exploiting trust and urgency, they manipulate victims into executing malicious commands themselves, bypassing many traditional defenses. While technically modest, tools like BAITSWITCH and SIMPLEFIX are effective in surveillance and espionage operations.

Recommendations

- **Be Cautious with Unexpected Prompts:** If a website asks you to copy and run a command in the Windows Run dialog, treat it as a red flag. Legitimate services will never require you to do this.
- **Restrict Unnecessary Privileges:** Ensure that users only have the permissions they truly need. Limiting administrator rights can stop malware from gaining a deeper foothold.
- **Isolate Risky Browsing Activities:** Browser isolation technologies, such as cloud-based browsing or secure sandboxes, help contain threats that originate from malicious websites.
- **Keep Systems and Defenses Updated:** Regularly patch operating systems, browsers, and security tools to reduce the risk of exploitation through old vulnerabilities.
- **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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1583** Acquire Infrastructure	**T1583.001** Domains	**T1583.006** Web Services
T1585 Establish Accounts	**T1585.002** Email Accounts	**T1585.003** Cloud Accounts	**T1587** Develop Capabilities
T1587.001 Malware	**T1608** Stage Capabilities	**T1608.001** Upload Malware	**T1608.003** Install Digital Certificate

T1608.005 Link Target	**T1204** User Execution	**T1204.004** Malicious Copy and Paste	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1059.003** Windows Command Shell	**T1037** Boot or Logon Initialization Scripts	**T1037.001** Logon Script (Windows)
T1112 Modify Registry	**T1140** Deobfuscate/Decode Files or Information	**T1564** Hide Artifacts	**T1564.003** Hidden Window
T1218 System Binary Proxy Execution	**T1218.011** Rundll32	**T1205** Traffic Signaling	**T1070** Indicator Removal
T1070.003 Clear Command History	**T1027** Obfuscated Files or Information	**T1027.011** Fileless Storage	**T1027.013** Encrypted/Encoded File
T1033 System Owner/User Discovery	**T1082** System Information Discovery	**T1135** Network Share Discovery	**T1016** System Network Configuration Discovery
T1016.001 Internet Connection Discovery	**T1087** Account Discovery	**T1087.001** Local Account	**T1083** File and Directory Discovery
T1049 System Network Connections Discovery	**T1057** Process Discovery	**T1018** Remote System Discovery	**T1046** Network Service Discovery
T1124 System Time Discovery	**T1005** Data from Local System	**T1530** Data from Cloud Storage	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1104** Multi-Stage Channels	**T1001** Data Obfuscation	**T1001.003** Protocol or Service Impersonation
T1105 Ingress Tool Transfer	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1573** Encrypted Channel
T1573.002 Asymmetric Cryptography	**T1566** Phishing	**T1036** Masquerading	**T1059.007** JavaScript
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	preentootmist[.]org, blintepeeste[.]org, captchanom[.]top, southprovesolutions[.]com
URLs	hxxps[:]//preentootmist[.]org/?uinfo_message=Resilient_Voices, hxxps[:]//blintepeeste[.]org/?u_storages=Resilient_Voices_concept, hxxps[:]//captchanom[.]top/check/machinerie[.]dll, hxxps[:]//captchanom[.]top/coup/premier, hxxps[:]//captchanom[.]top/coup/deuxieme, hxxps[:]//captchanom[.]top/coup/troisieme, hxxps[:]//captchanom[.]top/coup/quatre, hxxps[:]//southprovesolutions[.]com/FvFLcsr23, hxxps[:]//southprovesolutions[.]com/Zxdf, hxxps[:]//southprovesolutions[.]com/KZouoRc, hxxps[:]//southprovesolutions[.]com/EPAWl, hxxps[:]//southprovesolutions[.]com/VUkXugsYgu, hxxps[:]//drive[.]google[.]com/file/d/1UiiDBT33N7unppa4UMS4NY2oOJCM-96T/view
SHA256	87138f63974a8ccbbf5840c31165f1a4bf92a954bacccfbf1e7e5525d750aa48, 62ab5a28801d2d7d607e591b7b2a1e9ae0bfc83f9ceda8a998e5e397b58623a0, 16a79e36d9b371d1557310cb28d412207827db2759d795f4d8e27d5f5afaf63f
Email	narnobudaeva[@]gmail[.]com

References

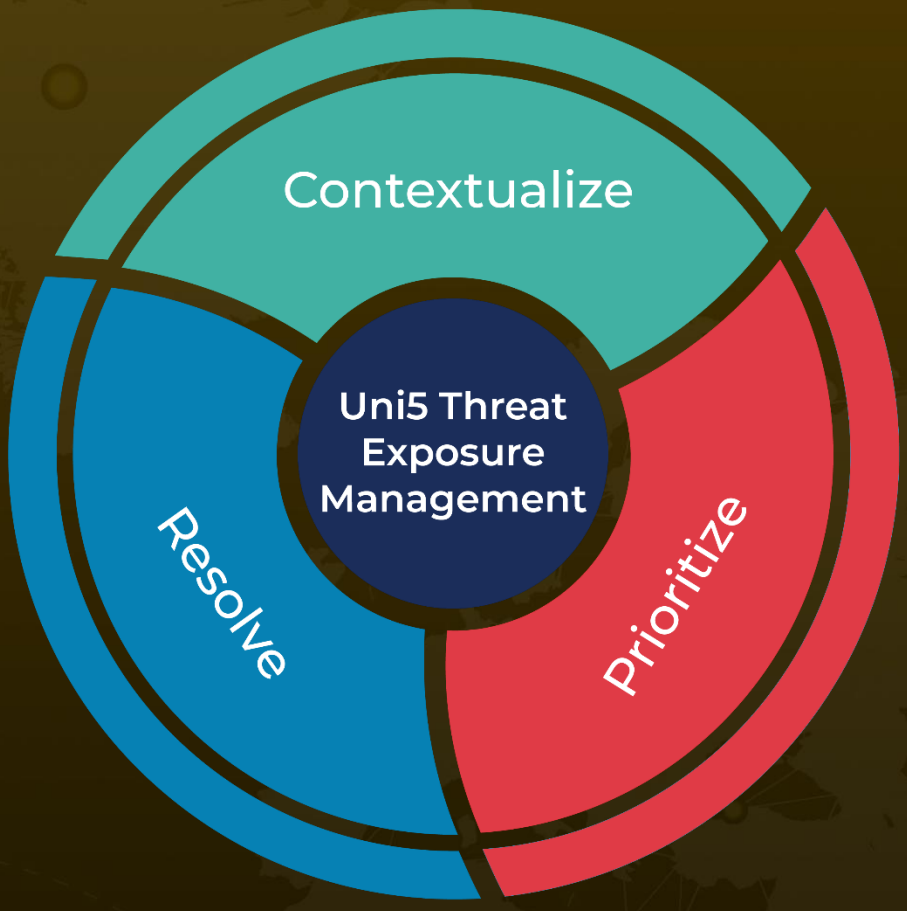
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix

https://hivepro.com/threat-advisory/coldriver-creeps-closer-with-lostkeys-malware/

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

September 26, 2025 . 8:30 AM

More at www.hivepro.com