

Earth Sirrush: A Russia-Aligned Intrusion Set With 4 Years of Evolving Espionage Tooling | TrendAI (US)

Archived: 2026-10-30 02:00:39 UTC

Since at least 2022, the Russia-aligned intrusion set tracked by TrendAI™ Research as Earth Sirrush — previously tracked as SHADOW-EARTH-065, overlapping with the [UAC-0099](#) designation by the Computer Emergency Response Team of Ukraine (CERT-UA) — has conducted sustained spear-phishing campaigns against Ukrainian government agencies, defense organizations, border guard units, and logistics operators. Our new report traces the group’s operations from 2022 through July 2026, revealing a threat actor who continually replaces its malware while retaining recognizable development, delivery, and infrastructure patterns.

For our full analysis, read our technical brief [here](#).

From PowerShell loaders to stealthier .NET implants

Earth Sirrush’s early campaigns relied on PowerShell- and Go-based tools, including the LONEPAGE, SEAGLOW, and OVERJAM families, as [documented by CERT-UA](#) and [Deep Instinct](#). These tools were delivered through malicious archives, HTA files, and exploitation of the CVE-2023-38831 WinRAR vulnerability. Early command-and-control (C&C) communications commonly used plain HTTP over high-numbered ports.

Between 2024 and 2025, the group shifted toward compiled C# malware. This phase introduced MATCHBOIL, MATCHWOK, and DRAGSTARE, [reported by CERT-UA](#) and, in the case of DRAGSTARE, also [analyzed by FortiGuard Labs](#). These are tools designed for loading payloads, executing encrypted tasking, stealing credentials, and performing system reconnaissance.

The group’s most notable development during this period was a previously undocumented .NET infostealer and remote access trojan (RAT) we named ASHVEIN, although its developers referred to the malware as “TelemetryBrowser.”

ASHVEIN targets Ukrainian government personnel and combines credential theft with surveillance and remote-control capabilities. Its functionality includes the following:

- Credential theft from Chrome and Firefox using DPAPI
- GDI-based screenshot capture
- File enumeration and retrieval
- PowerShell remote shell execution
- System fingerprinting through WMI queries
- Encrypted C&C communications
- Detection of security analysis tools such as Wireshark, IDA, OllyDbg, Fiddler, and Process Monitor

ASHVEIN also hides tasking inside invisible HTML elements. Some variants use a GitHub-based dead-drop resolver as a fallback mechanism, while delivery methods include DLL sideloading, VHD containers, and

dedicated .NET droppers.

One delivery component, AnswerFromPolice, displays a document impersonating the National Police of Ukraine while deploying the malware in the background. This combination of institutional impersonation and credible decoy content is designed to increase the likelihood that recipients will open and trust the file.

Steganography becomes a delivery mechanism

In 2026, Earth Sirrush expanded its use of image-based steganography. The CINDERBLOT campaign, also known as BadPaw and [first reported by ClearSky](#), used phishing lures impersonating the State Border Guard Service of Ukraine.

A later campaign impersonated a drone or unmanned aerial vehicle (UAV) parts company. Victims were directed to a professional-looking website displaying a fraudulent “Verified by antivirus” message before downloading weaponized ZIP files.

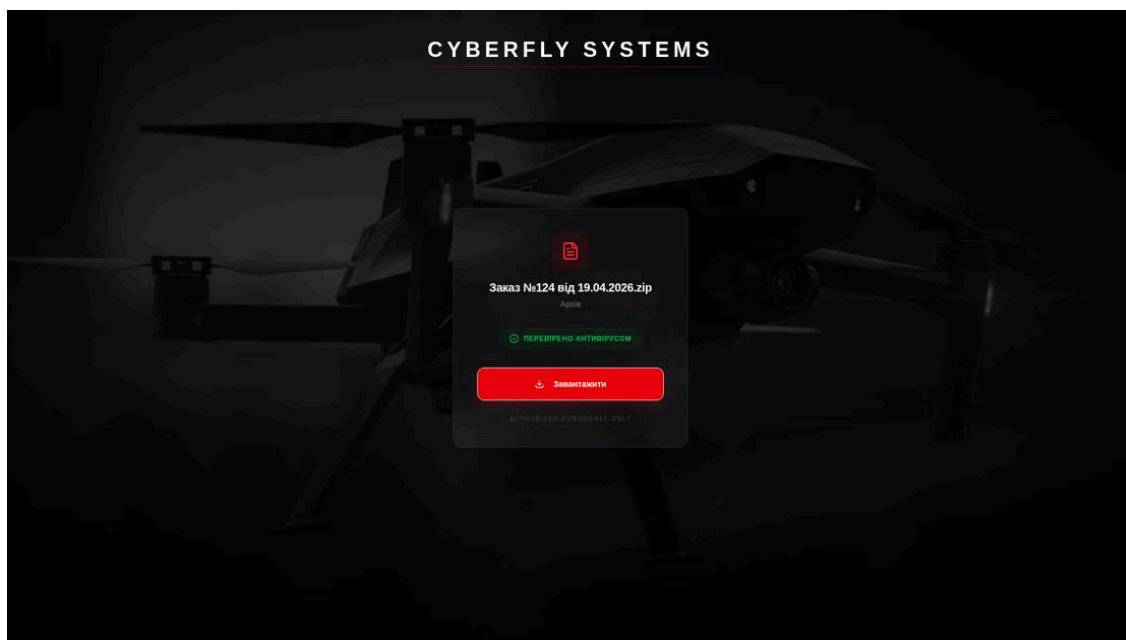


Figure 1. The order.cyberflysystems[.]com download page with a fake antivirus badge

The extracted payloads were hidden inside PNG images and deployed through scheduled tasks. In one case, the malware was stored in a file named KittyCat.png, continuing a naming convention observed in earlier campaigns.

The group also used multiple steganographic techniques. Some payloads were embedded after PNG image data, while others were extracted from pixel data by PowerShell scripts. This variation suggests that the operators maintain several delivery mechanisms in parallel to complicate detection and analysis.

A tactical shift in July 2026

In July 2026, [CERT-UA documented](#) a new delivery chain involving three tools. The campaign used LUNCHPOKE, a malicious Notepad++ plugin, to initiate the infection chain; BURNYBEAR, a .NET loader, to retrieve and execute payloads; and MATCHBOIL.V2, an updated loader with stronger encryption and revised

obfuscation. LUNCHPOKE uses DLL proxying to execute malicious code when the application starts. It then deploys BURNYBEAR and MATCHBOIL.V2, which are stored in randomized subdirectories under a user-writable location.

The campaign also abused renamed copies of schtasks.exe and created scheduled tasks that ran at short intervals. A parallel delivery chain used PowerShell scripts to extract payloads from PNG images and establish persistence through Registry Run keys.

These techniques demonstrate a consistent operational goal: Hide malware inside familiar software, legitimate-looking documents, and ordinary Windows locations.

Multiple clues point to one intrusion set

Although Earth Sirrush has repeatedly rebuilt its tooling, TrendAI™ Research identified several independent indicators connecting the campaigns:

- Reuse of the same PKCS #7 signature file as a social engineering prop
- Recurring developer account names and PDB path artifacts
- Russian-language indicators
- Structurally identical XOR-based string encryption across ASHVEIN, MATCHBOIL, and DRAGSTARE
- Identical WMI fingerprinting queries across ASHVEIN and CINDERBLOT
- Shared “TelemetryUP” branding in ASHVEIN metadata and related infrastructure
- Shared use of .library-ms files and the C:\Users\Public\Libraries\ directory
- Similar AES and RSA hybrid encryption schemes
- Repeated anti-debugging and TLS certificate-validation bypass techniques

Infrastructure analysis provides additional support. Many confirmed C&C domains were registered through the same registrar, Regery.com, and fronted by Cloudflare. Backend systems cluster in AS399629 (BL Networks). One backend IP directly links domains associated with both ASHVEIN and CINDERBLOT.

No single indicator is conclusive. However, the convergence of code similarities, reused artifacts, infrastructure relationships, and consistent targeting supports our high-confidence assessment that these operations belong to the same tracked intrusion set. ESET has [separately assessed](#) that UAC-0099 might conduct initial-access operations for Sandworm (APT44), an intrusion set linked to Russia’s military intelligence agency and known for destructive operations against Ukraine.

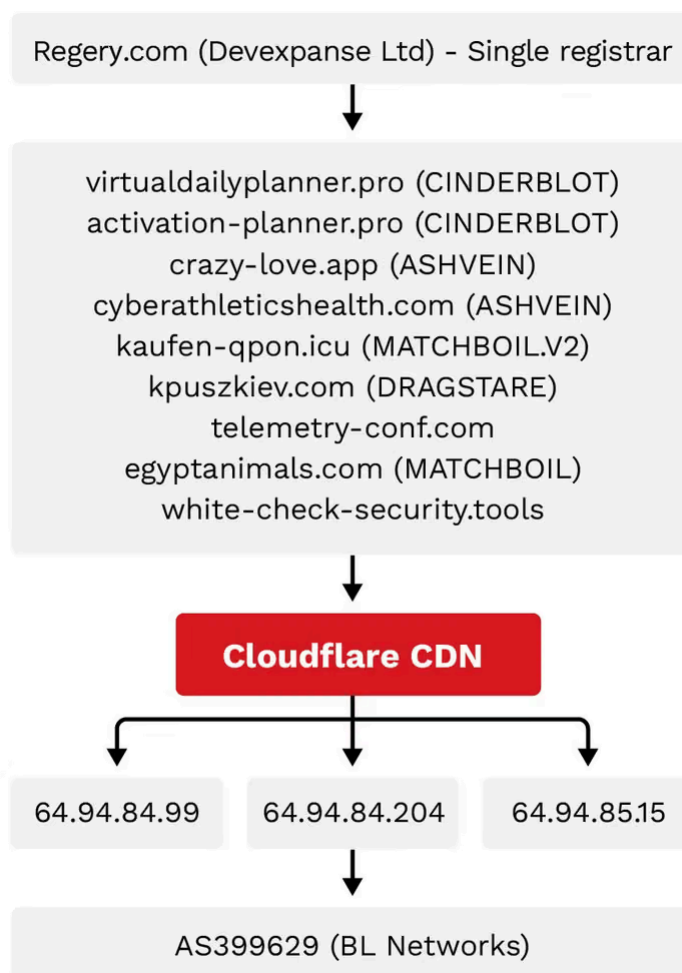


Figure 2. Earth SIRRUSH C&C infrastructure: single-registrar domain procurement, Cloudflare fronting, and backend IP clustering

Targeting expands beyond government

Earth SIRRUSH has targeted government ministries, defense forces, border guards, and organizations connected to Ukraine's logistics and defense supply chains. The threat actor's lures have impersonated the National Police, the State Border Guard Service, tax authorities, and the Ministry of Justice.

Our telemetry also shows activity against transport and logistics operators. In at least one case, scheduled-task persistence allowed the implant to maintain access through a month-long period without C&C communication.

This targeting suggests a long-term intelligence-collection mission rather than a short-lived smash-and-grab operation. As logistics and infrastructure become increasingly important to Ukraine's wartime resilience, they are also becoming more attractive targets for cyberespionage.

How organizations can mitigate risk

Because Earth Sirrush continually adapts its tooling and delivery methods, a layered defense can help organizations limit their exposure to potential attacks:

- Block confirmed C&C domains and IP addresses, while treating shared backend systems as supporting indicators, not standalone ones.
- Monitor executable creation under C:\Users\Public\Libraries\ and other user-writable staging directories.
- Detect renamed copies of schtasks.exe and Notepad++ loading DLLs from unusual plugin locations.
- Scan for PE files appended to PNG images and monitor suspicious VHD mounts.
- Alert on Unicode padding techniques used to disguise file extensions.
- Enable DPAPI auditing, PowerShell ScriptBlock logging, and Constrained Language Mode.
- Monitor unusual access to Chrome's Local State file and Firefox profile data.
- Train personnel in government, logistics, border security, and defense-adjacent organizations to recognize tailored spear-phishing lures.
- Validate digital signatures on incoming documents, particularly reused or mismatched PKCS #7 files.

Conclusion

Earth Sirrush has changed its tools repeatedly, from PowerShell scripts and Go binaries to compiled C# malware and protected .NET implants hidden inside images, yet its forensic traces remain visible. The group's evolution reinforces a central lesson for defenders: Malware families might change, but development habits, delivery patterns, infrastructure choices, and operational conventions can preserve the links between campaigns. Detecting those connections can help organizations identify the broader intrusion set before a single incident becomes a persistent compromise.

For our full analysis, read our technical brief [here](#).

Source: <https://www.trendaisecurity.com/en-us/resources-insights/trendai-security-blog/earth-sirrush-russia-aligned-intrusion-set-4-years-evolving-espionage-tooling>