

GREYVIBE: A Russia-nexus group leveraging AI across state-aligned operations - WithSecure™

By Authors

Archived: 2026-06-04 02:00:48 UTC

Executive Summary

- WithSecure identified an ongoing and persistent set of activity targeting Ukraine and Ukraine-related entities since at least August 2025.
- Based on significant overlaps observed across both development and operational phases of the associated campaigns, WithSecure associates the activities with a threat group tracked as GREYVIBE. At the time of writing, WithSecure has not identified definitive links between GREYVIBE and any previously tracked threat group.
- The group has leveraged multiple attack vectors, including spear-phishing e-mails, fake captcha pages and fraudulent Ukrainian adult club websites, to deliver malware to a diverse set of victims. The observed victimology includes military, government, civilian, and business-related entities. Across these campaigns, the group has relied on custom developed obfuscators, loaders, and malware. WithSecure additionally identified several associated activity and related campaigns that shared varying degrees of overlap with the group's tooling, infrastructure, and tradecraft.
- The lures, targeting, and observed actions on objectives of the activities align with Russian state interests, particularly in support of intelligence-gathering objectives related to Ukraine in the context of the ongoing Russia-Ukraine war. WithSecure also identified multiple indicators suggesting that the associated developers and operators are Russian-speaking and operate broadly in Russian (Moscow) time zone.
- While the activities align with Russian state interests, several observed indicators suggest the group has ties to the broader cybercrime ecosystem, with the group potentially involving current or former cybercriminal actors.
- Moreover, WithSecure found strong evidence suggesting systematic use of generative AI (GenAI) and large language models (LLMs) by GREYVIBE throughout their operation.
- Taken together, WithSecure assesses GREYVIBE is a low-to-moderately sophisticated group, as reflected in repeated operational security failures, heavy reliance on LLMs, and overall observed tradecraft.
- Lastly, WithSecure identified design flaws in LegionRelay, a custom malware associated with GREYVIBE that WithSecure assesses was likely developed with LLM assistance. These flaws exposed a limited number of LegionRelay's backend functionality which provided WithSecure with research visibility into associated activity over an extended period. This visibility informed WithSecure's assessment of the group's victimology, actions on objectives, post-compromise tooling, and operational behaviour. Sensitive details pertaining to the observed victimology and actions on objectives as well as information that could aid the threat actor have been deliberately omitted from the report, but could be shared with relevant authorities where appropriate.

This blog post summarises key topics from WithSecure's [full report](#), which covers our investigation and findings in substantially greater depth.

A multi-vector activity set

GREYVIBE has used several delivery approaches. We grouped GREYVIBE's observed activity into a set of distinct campaigns linked by shared malware, infrastructure, and operational behaviours. Across these campaigns, the group has consistently used appropriate lures for deception and implemented a decoy-and-payload execution logic to reinforce the credibility of the lure while covertly gaining access to the victim's machine.

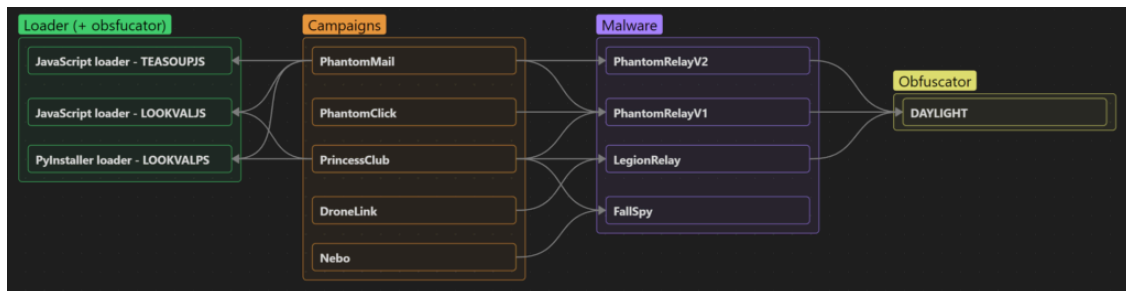


Figure 1. Overview of GREYVIBE-associated campaigns, malware, loaders, and obfuscators

PhantomMail – spear-phishing via email

Since August 2025, the group has conducted at least six distinct spear-phishing campaigns. Spear-phishing e-mails sent to targeted victims typically contained links to malicious ZIP or RAR archives hosted on third-party file-sharing services such as Google Drive and 4sync. The archives contained PyInstaller- or JavaScript-based loaders that launched a decoy (e.g. a PDF document or an error pop-up) while initiating the PhantomRelay infection chain in the background. Lures impersonated a range of Ukrainian entities, including a Kyiv City Council official, a Ukrainian energy company, the Main Directorate of the State Emergency Service of Ukraine, and the State Service of Special Communications and Information Protection of Ukraine.

АКЦІОНЕРНЕ ТОВАРИСТВО “УКРАЇНЬСЬКА ОБОРОННА ПРОМИСЛОВОСТЬ” вул. Дегтярівська, 36, м. Київ, 04119, Україна тел. +380(44)586-24-01, факс +380(44) 586-24-77 код ЄДРПОУ 37854297 e-mail: kanc@ukroboronprom.com		JOINT STOCK COMPANY “UKRAINIAN DEFENSE INDUSTRY” 36 Degtshirivska Str., Kyiv, 04119, Ukraine tel. +380(44)586-24-01, fax +380(44) 586-24-77 identification code 37854297 e-mail: kanc@ukroboronprom.com
--	---	---

15.05.2025 № UOP 4.2-4279

на № _____ від _____

АТ "УОП"



3433780

**Керівникам підприємств та
господарських товариств
(за списком)**

Щодо посилення захисту інформаційних систем

З метою посилення стану кібербезпеки Вашого підприємства/товариства та підвищення рівня кіберзахисту, направляємо узагальнені рекомендації Департаменту контррозвідки Служби безпеки України щодо першочергових заходів кібербезпеки з урахуванням виявлених форм протиправної діяльності іноземних розвідок, для опрацювання та використання в роботі відповідними фахівцями у сфері інформаційної безпеки.

За результатами вжитих заходів просимо інформувати Акціонерне товариство "Українська оборонна промисловість".

Додаток: за текстом на 10 (десяти) аркушах.

В.о. Генерального директора

Тарас ШИЙКО

Figure 2. Example of decoy PDF document dropped and launched

PhantomClick – ClickFix via fake CAPTCHA pages

In early October 2025, the group briefly experimented with ClickFix-style fake CAPTCHA pages for initial malware delivery. Associated domains masqueraded as Zoom conference and LAPAS (Latvian Platform for Development Cooperation) websites. Once landed on the site, victims were instructed, in Ukrainian, to run commands under the pretext of completing a Cloudflare-themed security verification process, while the executed command initiated a PhantomRelay infection chain in the background. The fake sites also implemented decoy redirection to legitimate destinations, likely to reinforce the appearance of a normal verification process.

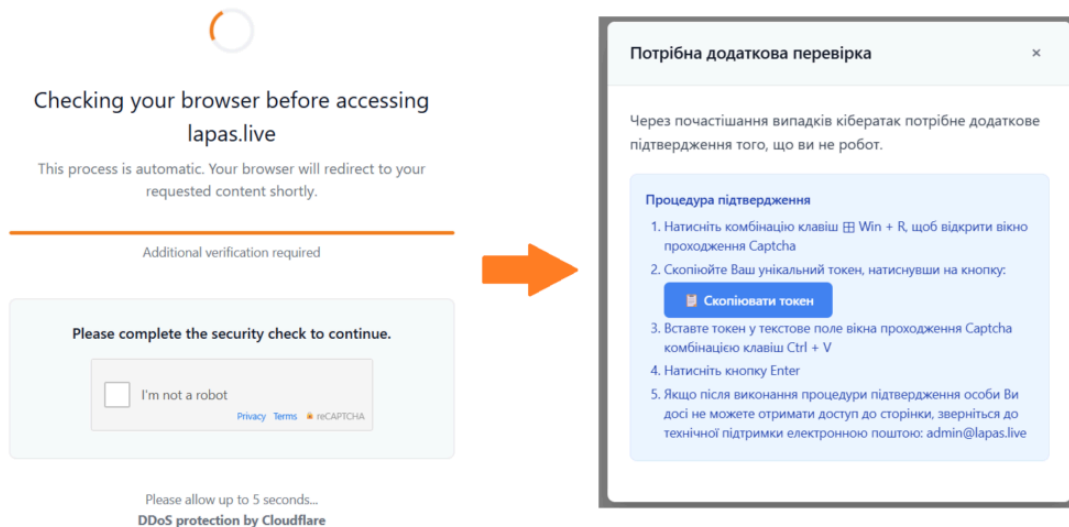


Figure 3. Example of fake captcha site and prompted instructions (Ukrainian)

PrincessClub – fake Ukrainian adult-club websites

A notable and persistent campaign, tracked as PrincessClub, used fake Ukrainian adult-club websites to deliver FallSpy on Android and PhantomRelayV1 or LegionRelay on Windows. Confirmed victimology included Ukrainian combatants, with many victims located in Kharkiv, Ukraine. The sites included victim-facing functionality intended to appear legitimate, while the infection chain executed in the background. The group has used fake female personas on Telegram, including via local dating channels, to build trust with victims before directing them to the lure sites or delivering malware directly. Later iterations of the lure sites introduced a WebRTC-based live call feature, accessible only post-infection, that could capture victim audio and video, turning the lure site from a static decoy into a potential human intelligence (HUMINT) collection mechanism.

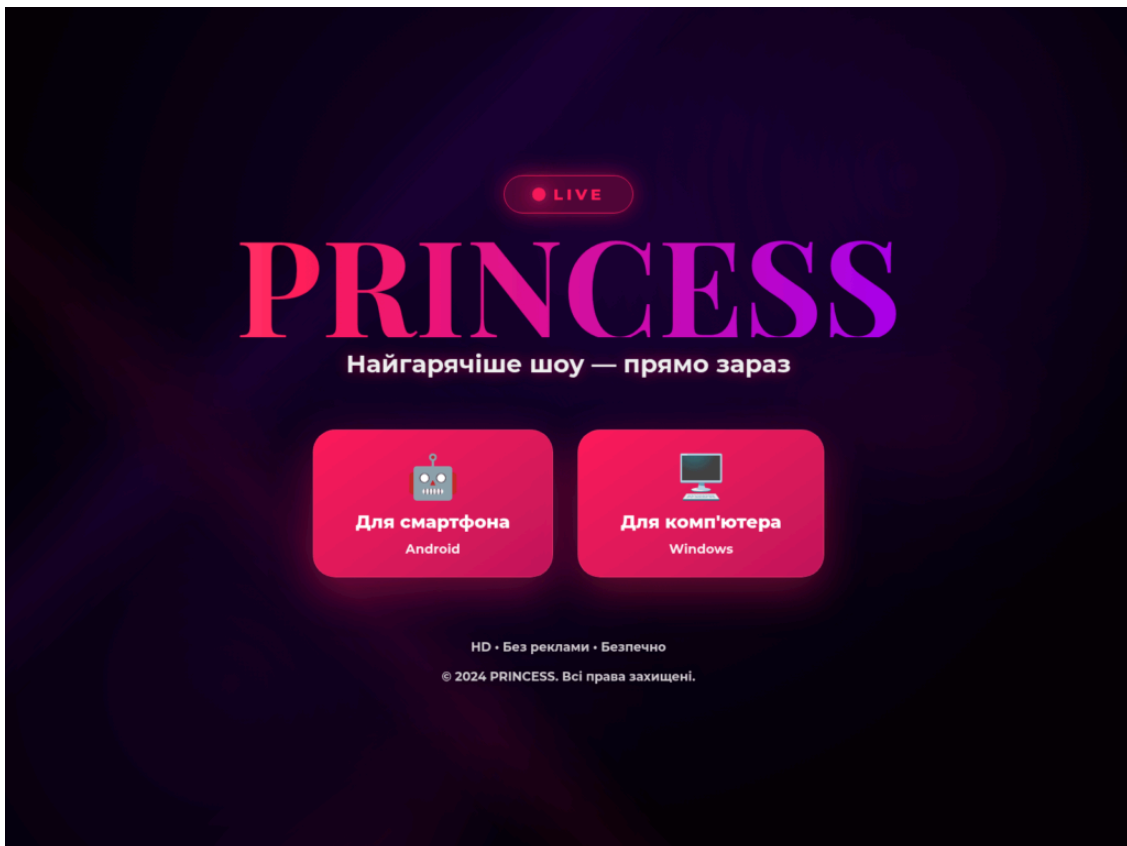


Figure 4. PrincessClub site offering Android and Windows client download

Other associated activity

DroneLink – drone-themed charity lures

In March and April 2026, we observed an operational overlap between PrincessClub and a campaign leveraging websites masquerading as charitable foundations supporting the Armed Forces of Ukraine (FPV drones, UAVs, and related initiatives). Overlaps included shared C2 infrastructure, shared post-compromise tooling such as WireGuard and ZAPiXDESK, and DAYLIGHT-obfuscated LegionRelay scripts hosted on the charity sites. Although these overlaps strongly suggest the activity is closely associated with GREYVIBE, WithSecure continues to separately monitor and further investigate activity associated with DroneLink, its lineage, and its association with GREYVIBE.

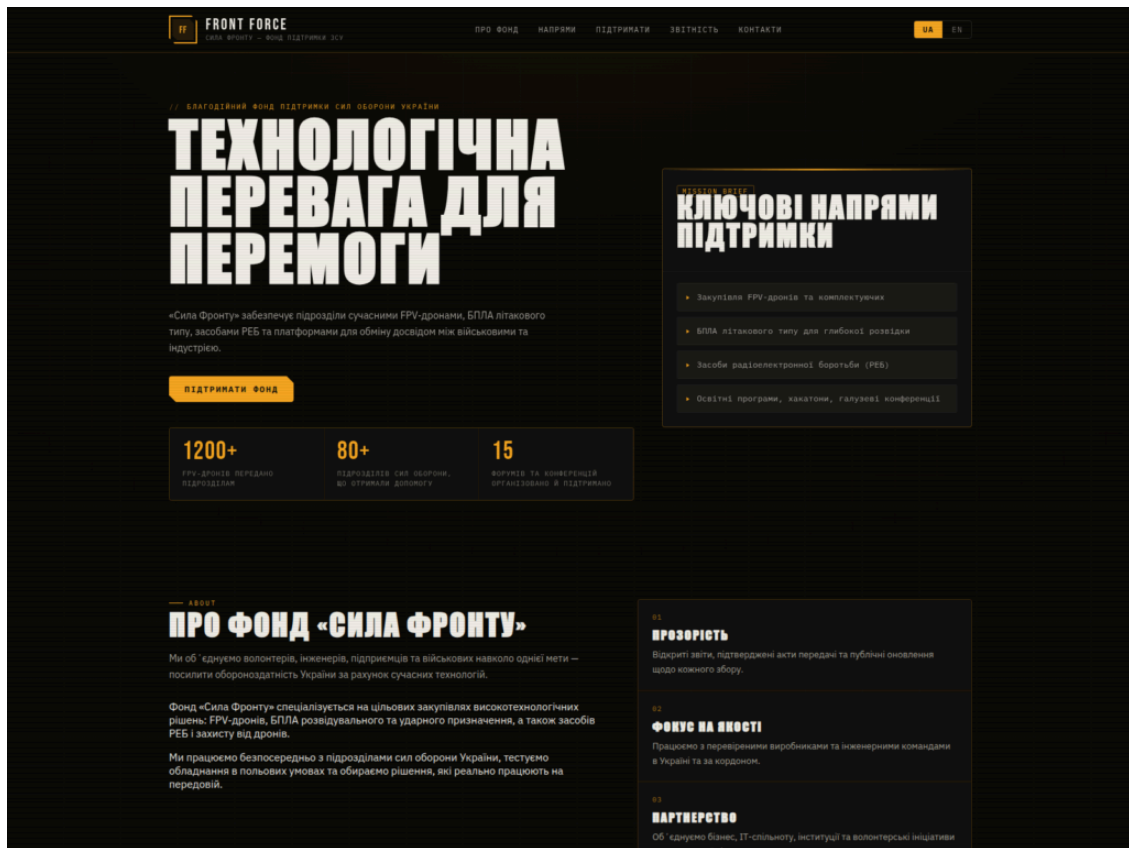


Figure 5. Frontpage of one of the fake charity domains used in the DroneLink campaign (frontforce[.]org)

Nebo – a Russian-language lure

A smaller cluster of artefacts highly likely associated with GREYVIBE were found masquerading as “СПО НЕБО” (transliterated as “SPO NEBO”). These include a FallSpy sample mimicking a Russian-language login screen and a similar fake login page hosted on PrincessClub infrastructure. Both referenced hard-coded telephone exchange (“ATC-P”) numbers consistent with secure communications systems primarily used in Russian military and defence settings. The intended victimology of this activity remains unclear. However, the most plausible hypothesis is that the lure was designed to deceive Ukrainian military personnel by presenting the illusion of access to a Russian military terminal.

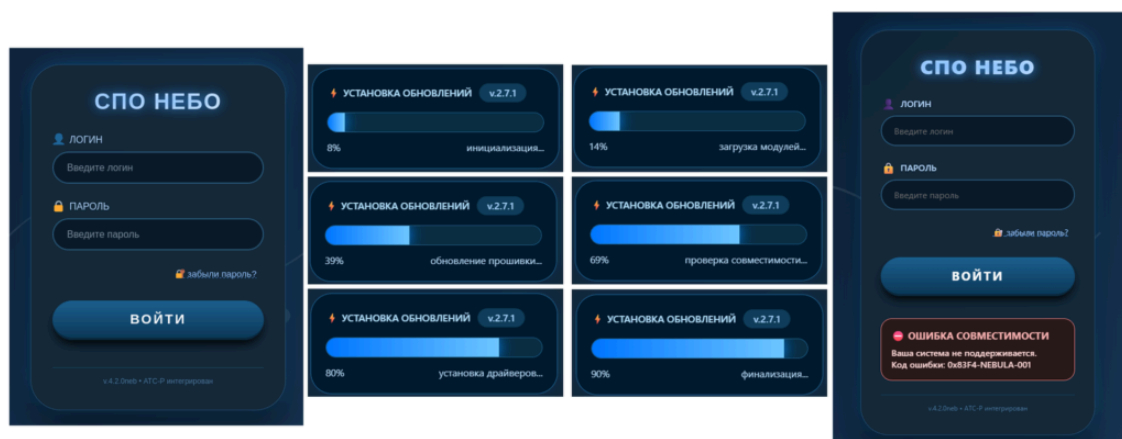


Figure 6. SPO NEBO fake login page and post-authentication “update” progress screens

AI as an operational enabler

One of the most notable aspects of GREYVIBE's activity is their apparent systematic use of generative AI and large language models across the attack lifecycle. We identified strong indicators suggesting the group has used several AI platforms including: Ideogram AI, ChatGPT, and Google Gemini.

Observed indicators suggest AI-assisted activity across:

- **Lure development**, including the generation of images used in the PrincessClub campaign and the development of lure sites associated with PrincessClub and PhantomClick.
- **Resource development**, including the development of obfuscation and loader scripts (LOOKVALJS, DAYLIGHT, TEASOUP), full-stack development of LegionRelay, and backend infrastructure setup and configuration.
- **Post-compromise activity**, including the generation of post-compromise commands, scripts, and tooling delivered through PhantomRelay and LegionRelay.



Figure 7. Examples of LLM markers present across images used by GREYVIBE

WithSecure assesses that this usage is likely deliberate and operationally integrated rather than isolated or experimental. The group's use of AI may serve several purposes:

- Bridging technical capability gaps.
- Accelerating development and operational tempo.
- Reducing reliance on historically reused malware, code patterns, or tooling that could support attribution.

This may also complicate continuous threat tracking and attribution. If an actor can frequently generate, refactor, or replace components of its operational footprint with AI assistance, traditional clustering methods based on stable technical artifacts may become less reliable over time.

Custom malware, loaders, and obfuscators

The group has relied on a small set of custom-developed malware and obfuscators across their campaigns.

PhantomRelay

PhantomRelay is a PowerShell-based RAT that uses a two-stage execution chain: a fingerprinting script, followed by the main RAT client. The RAT uses WebSockets to communicate with its C2 and supports execution of both PowerShell scripts and Windows commands. Despite its limited native functionality, the RAT is modular in design. Its capabilities are extended through additional PowerShell scripts delivered by the C2 and dynamically executed on the victim machine.

We initially assessed PhantomRelay was custom-developed and exclusively associated with GREYVIBE; however, subsequent analysis identified the same malware in use across additional, seemingly unrelated cybercrime activity clusters. To distinguish these uses we track three variants:

1. **PhantomRelayLite**, a base variant observed across both GREYVIBE's early development activity and the cybercrime clusters (including a Microsoft Teams voice-phishing intrusion set, and a KongTuke ClickFix delivery chain).
2. **PhantomRelayV1**, the first operational variant developed and weaponised by GREYVIBE, distinguished by a custom watchdog persistence mechanism, a shift from the SAWDUST and CRUEDUST obfuscators to the group's own DAYLIGHT obfuscator, as well as distinct C2 infrastructure.
3. **PhantomRelayV2**, the second operational variant developed and weaponised by GREYVIBE, which reconstructs the malware while preserving its core functionality.

We cannot at present ascertain the origin of PhantomRelayLite; nevertheless, its appearance across multiple cybercrime clusters places GREYVIBE in close proximity to the cybercrime ecosystem.

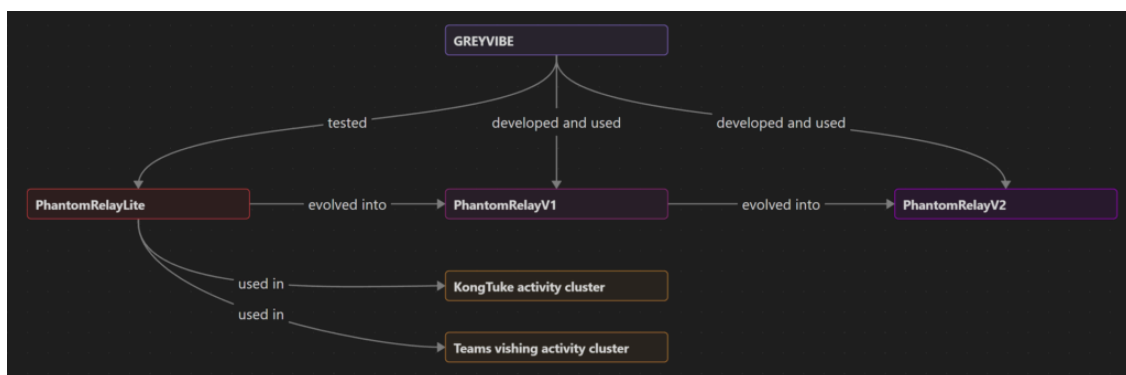


Figure 8. Perceived relationship between PhantomRelay variants and associated activity clusters

FallSpy

FallSpy is an Android spyware first observed in August 2025. It has been observed across several GREYVIBE-associated campaigns, including PrincessClub and Nebo.

The malware presents decoy content to the victim while covertly collecting and exfiltrating information from the victim's device, including contacts, call logs, installed applications, SIM-linked phone numbers, device and

network information, Wi-Fi SSID, last-known location, public IP, and media files. Based on its functionality and deployment context, FallSpy appears to be developed for surveillance and intelligence-gathering objectives.

LegionRelay

LegionRelay is a lightweight PowerShell-based RAT that communicates with its command-and-control server through REST API methods. Although the client-side implementation is limited to executing operator-issued PowerShell commands, the broader capability set is realised through operator-staged scripts deployed during post-compromise activity.

WithSecure observed operators using LegionRelay for file enumeration, file exfiltration, screenshot capture, browser data theft, Telegram and WhatsApp data exfiltration, RDP access setup, among other actions.

Custom obfuscators

The group has developed and rotated through several custom obfuscators and loaders: LOOKVALPS (PowerShell), LOOKVALJS (JavaScript), DAYLIGHT (PowerShell), and TEASOUP (JavaScript).

DAYLIGHT, in active use from October 2025, likely replaced LOOKVALPS and was routinely applied to both initial-stage and post-compromise payloads. TEASOUP, observed from March 2026, similarly succeeded LOOKVALJS.

We assess with moderate-to-high confidence that all four were custom-developed by the group, and with moderate confidence that several were developed with LLM assistance.

The blurred lines of attribution

WithSecure found associated operators and developers are Russian-speaking and operate within the Russian (Moscow) time zone. This assessment is supported by converging indicators, including:

- The prevalence of Russian-language comments across development, backend, and code artefacts
- Russian-language administrative panels for FallSpy, LegionRelay, and PrincessClub.
- Operator- and developer-linked machines configured to the Russian locale and UTC+3 (Moscow time)
- C2 servers similarly configured to UTC+3
- Evidence of operators communicating in Russian and translating between Russian and Ukrainian.

Analysis of operator post-compromise activity over several months further showed patterns consistent with Moscow working hours.

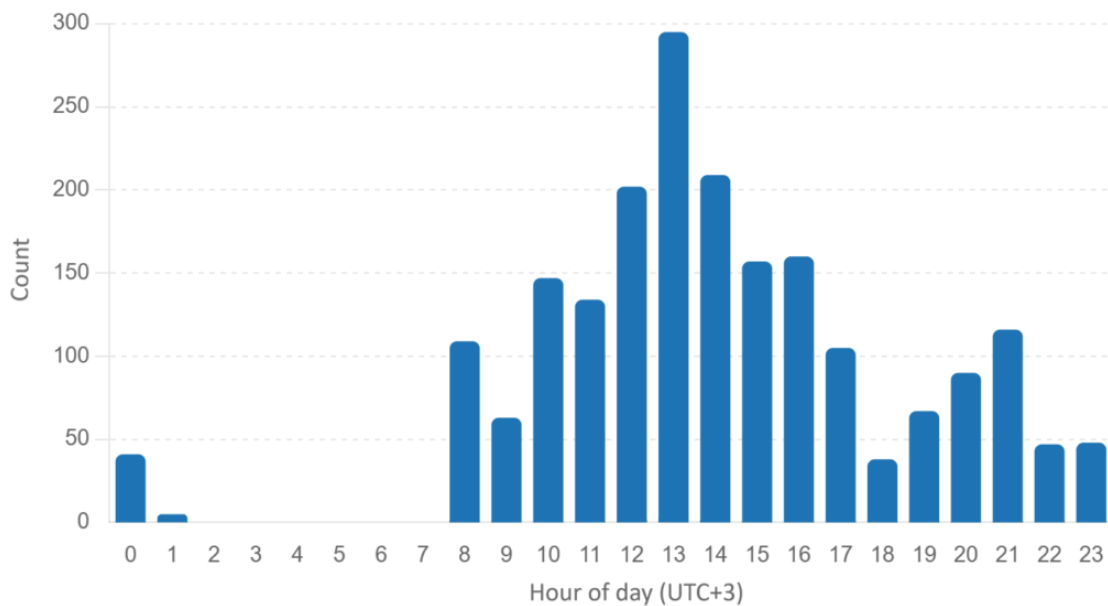


Figure 9. Operator post-compromise activity grouped by hour of day (UTC+3)

Moreover, we assess with high confidence that GREYVIBE’s activities align with Russian state interests, particularly intelligence-gathering objectives in the context of the ongoing Russia-Ukraine war. This assessment is supported by the group’s primary focus on Ukrainian targets, the nature of the lures and victimology observed, and the actions on objectives identified during post-compromise activity.

At the same time, several indicators align more closely with cybercriminal actors than with traditional nation-state operations, including:

- Suspected access to and use of a unique ISO builder across early development samples, potentially linked to the [TrickBot ecosystem](#) and [UAC-0098](#) (an activity cluster likely involving former TrickBot members previously observed targeting Ukraine)
- The presence of PhantomRelay variants across seemingly unrelated cybercrime activity clusters
- Development and test samples being uploaded to public platforms such as VirusTotal
- The use of Internet slang-based naming conventions across early-stage development artefacts (for example, “letsrollboyos,” “totallyunsus,” “cuteuwu”)
- The deployment of an XMRig miner payload on a small number of LegionRelay-infected machines.

Taken together, we assess with moderate confidence that the group has ties to the broader cybercrime ecosystem, and with low-to-moderate confidence that it involves current or former cybercriminal members. The exact nature of their relationship to the Russian state remains unclear, whether such members have been absorbed into a state-backed group, operate independently under state-directed tasking, or have formed a hybrid team. There is established [precedent](#) for Russian intelligence services leveraging or co-opting cybercriminal groups in support of state objectives.

While certain technical overlaps suggest proximity to UAC-0098, there is at present insufficient evidence to assess that GREYVIBE represents a direct continuation or reconstitution of that cluster. This hypothesis therefore remains low likelihood, but warrants further investigation.

Conclusion

GREYVIBE represents a persistent Russia-nexus threat operating primarily against Ukrainian targets, leveraging a broad range of delivery vectors and a small family of custom-developed malware, loaders, and obfuscators.

The group's operation aligns with Russian state interests but does not consistently exhibit the operational maturity associated with more seasoned adversaries, and indicators also suggest ties to the broader cybercrime ecosystem. The group occupies a grey area between cybercrime and state-affiliated activity, complicating attribution efforts and blurring traditional distinctions between these categories.

The group's extensive use of GenAI and LLMs is a notable aspect of its tradecraft. GREYVIBE appears to use AI not only for isolated development tasks, but across multiple operational phases. This likely enables the group to compensate for capability gaps, accelerate development cycles, and potentially reduce historical backlinks to prior activity. Given this extensive use, we expect the group's tradecraft to continue evolving and diversifying, likely increasing the complexity of continuous detection, tracking, and attribution.

At the time of writing, WithSecure has not identified definitive links between GREYVIBE and any previously tracked threat group. WithSecure continues to monitor the group, its associated campaigns, and potential links to other activity clusters.

A full list of Indicators of Compromise and associated YARA rules can be found in [WithSecure's GitHub](#)

Source: <https://labs.withsecure.com/publications/greyvibe>