

Gamaredon in 2025: Leveraging tunnels, workers, dead drops, and new alliances

By Zoltán Rusnák

Archived: 2026-09-23 02:01:49 UTC

Cyberespionage has remained a constant feature of Russia's war against Ukraine. ESET Research [has long tracked Gamaredon](#), one of the most active Russia-aligned advanced persistent threat (APT) groups targeting Ukraine. The group, [attributed by the Security Service of Ukraine \(SSU\)](#) to the 18th Center of Information Security of Russia's FSB, maintained a high operational tempo throughout 2025.

In our latest research, we analyze Gamaredon's activity during 2025, including new tools added to its arsenal, significant shifts in how it protects its network infrastructure, and its growing use of legitimate third-party services to hide both command and control (C&C) information and stolen data. The full technical details are available in our latest [white paper](#).

Key points of this blogpost:

- Throughout 2025, Gamaredon exclusively targeted governmental and military institutions in Ukraine.
- We observed 35 distinct spearphishing campaigns against new targets. The majority of the campaigns were carried out in the second half of the year, and they were significantly larger than earlier ones.
- Additional targets were compromised via multiple custom weaponizers designed for lateral movement.
- Gamaredon operators developed and deployed six new malicious PowerShell tools, which we analyze in our white paper, and resurrected an old VBScript weaponizer – PteroSetup.
- The file stealers PteroVDoor and PteroPSDoor were upgraded to support exfiltration to cloud storage services (Wasabi, Tebi, and Intercolo), which became the primary exfiltration method.
- Gamaredon operators sought new ways to protect their network infrastructure, with their C&C servers now hidden behind various third-party services such as tunnels, workers, DDNS (dynamic DNS), and PaaS (platform as a service).
- They also abused multiple legitimate messaging, social media, blogging, and paste services as dead drops for resolving C&C servers and distributing payloads.

The white paper is our third in-depth installment describing the tactics, techniques, and procedures (TTPs) of this group, which is believed to operate out of occupied Crimea. In September 2024, we published a white paper covering Gamaredon activities from 2022 and 2023 – [Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023](#) – and in July 2025, we published a white paper covering Gamaredon activities from 2024 – [Gamaredon in 2024: Cranking out spearphishing campaigns against Ukraine with an evolved toolset](#).

Continued data exfiltration and a new alliance

Throughout 2025, Gamaredon stayed highly active and remained focused solely on Ukraine. The group's ultimate goal continues to be the exfiltration of sensitive information and other critical data that could be exploited to support Russian interests in the ongoing war in Ukraine. Gamaredon's activities appear to be closely aligned with Russia's geopolitical objectives, targeting Ukrainian governmental and military institutions to gain an intelligence advantage.

New tooling and cooperation in the first half of the year

While the group took a short operational break in January 2025, Gamaredon spent much of its effort in the first half of the year developing and deploying new tools. We describe them in the [Six new tools, mostly delivery-focused](#) section of this blogpost. While we don't provide the exact timestamps for all changes introduced to the group's tooling, we observed that many updates were made in the lead-up to major holidays in Russia and Crimea. Notably, no updates were observed during or immediately after these holidays, further suggesting that Gamaredon operators are probably government-affiliated employees.

Notably, we uncovered that in early 2025, Gamaredon collaborated with Turla, another Russia-aligned threat actor also [linked to the FSB](#); we documented our findings in our blogpost [Gamaredon X Turla collab](#). This cooperation underscores the potential for coordinated cyberespionage campaigns among Russia-aligned groups, likely to amplify their operational impact. In the past, Gamaredon also [collaborated](#) with a threat actor that we discovered and named InvisiMole.

More broadly, 2025 also provided another example of cooperation and task sharing among Russia-aligned actors: we observed the Russia-aligned UAC-0099 group conducting initial access operations and subsequently transferring validated targets to Sandworm for follow-up activity. We documented our findings in [ESET APT Activity Report Q2 2025–Q3 2025](#).

Larger and more frequent spearphishing campaigns in the second half

In the second half of the year, the group shifted more toward larger and more frequent spearphishing campaigns; during 2025, we identified 35 of these. As in previous years, most campaigns used archive attachments or XHTML files employing [HTML smuggling](#) to deliver malicious HTA downloaders, which in turn fetched the VBScript downloader PteroSand and additional payloads. We also observed campaigns that probably used malicious hyperlinks instead of attachments.

Figure 1 shows a chart of unique samples of HTA downloaders delivered per month in Gamaredon spearphishing campaigns. Note that these figures represent minimums for spearphishing attempts, as one HTA downloader may target multiple individuals, and individuals can be targeted in several campaigns within the same month.

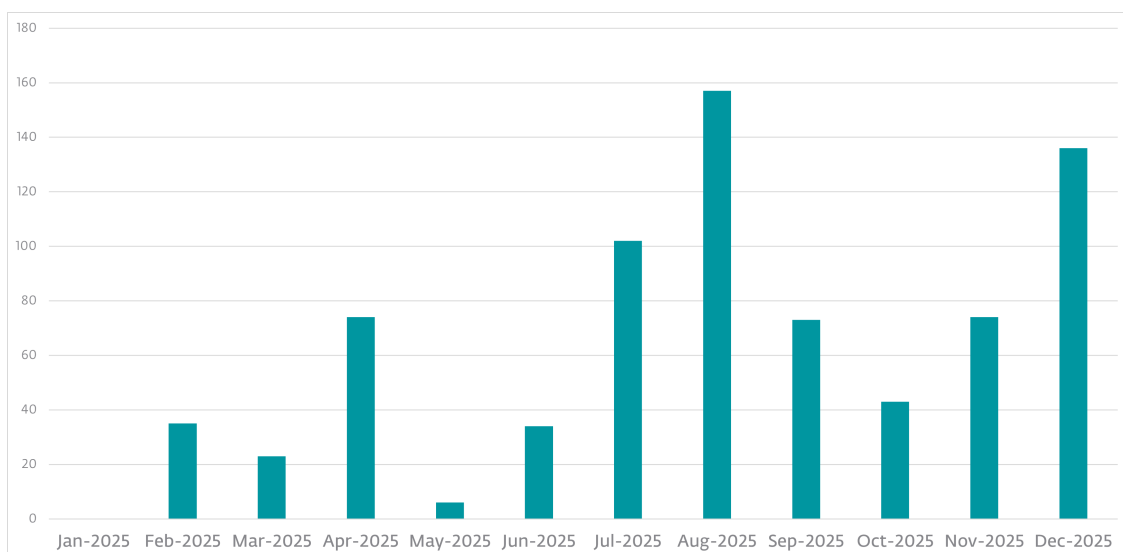


Figure 1. Unique Gamaredon spearphishing samples seen per month

What changed most noticeably was the tempo. Gamaredon was much more active in the second half of the year, when campaigns became both more frequent and larger in scale. Late in the year, the group also introduced a new technique – from September 26th, 2025 onward, it began abusing [CVE-2025-8088](#), a WinRAR vulnerability, to place its usual malicious HTA downloader into the victim’s Startup folder. That allowed the downloader to execute on the next login, adding persistence to a compromise chain that had previously relied more heavily on user interaction.

Weaponizers for movement beyond the compromised system

Beyond spearphishing, Gamaredon also continued using custom weaponizers for lateral movement. These tools weaponize USB drives, mapped network drives, and even software installers, helping the group spread within or across organizations after the initial compromise.

Six new tools, mostly delivery-focused

Gamaredon introduced six new tools in 2025, all written in PowerShell. Five of them appeared in the first quarter of the year, suggesting that the group spent the early months of 2025 building new delivery chains before shifting more attention to large-scale spearphishing in the second half.

Most of these new tools are relatively simple:

- **PteroDee** and **PteroCache** are straightforward PowerShell downloaders for fetching and executing PowerShell payloads in memory.
- **PteroDum** serves a similar purpose, but for VBScript payloads, writing them temporarily to disk, executing them, and then deleting them.
- **PteroOdd** is a tiny downloader used to retrieve a single PowerShell payload via the [Telegra.ph API](#), and based on what we observed, it appears to have been used mainly in cases connected to Gamaredon’s collaboration with Turla.
- **PteroEffigy** is another lightweight downloader, notable mainly for using the [GoFile](#) cloud storage service to obtain the next C&C server.

The standout among the new tools is **PteroPaste**, which is considerably more complex than the others. It combines a downloader, a USB weaponizer, and a runner component used for persistence and orchestration. Early versions of PteroPaste used [Rentry](#) as an intermediary staging point for encrypted payloads. Later versions moved away from that approach and instead retrieve an encrypted C&C hostname from Dropbox, decrypt it locally, and then connect to infrastructure hidden behind tunnel services. PteroPaste is also one of the tools involved in the [Gamaredon X Turla](#) collaboration that we documented in 2025.

Gamaredon also brought back **PteroSetup**, an older VBScript weaponizer that had likely been discontinued years earlier. The resurrected version scans fixed, removable, and network drives for installer-like executable files and replaces them with malicious self-extracting archives containing both the original installer and a malicious VBScript downloader. To the victim, the file still appears legitimate, but running it launches both the expected installer and the malicious code.

Overall, the new additions to Gamaredon's arsenal fit a pattern that we have seen before – rather than investing in highly sophisticated malware, the group prefers a larger number of simple tools that can be updated quickly and combined flexibly.

Important updates to previously known tools such as **PteroLNK**, **PteroPSLoad**, **PteroPSDoor**, **PteroVDoor**, and **PteroBox** can be found in the [white paper](#).

Advanced network infrastructure

Gamaredon continued to refine its techniques for protecting its network infrastructure and hiding its C&C servers. In 2025, the group's reliance on third-party services grew significantly, with tunnel services and serverless worker platforms becoming an increasingly important part of how it hid its real back-end infrastructure.

Tunnel services are legitimate tools that allow a system or application to be exposed to the internet through a provider-controlled domain, without revealing the real server directly. Workers serve a similar purpose, but go a step further: instead of simply forwarding traffic, they are serverless platforms that can run code and process requests before passing them on. In practice, both help obscure the underlying infrastructure and make disruption more difficult.

Tunnels, workers, and a return to DDNS

By the end of 2024, Gamaredon was already relying heavily on Cloudflare tunnels (trycloudflare.com) to conceal its infrastructure, and in 2025 it expanded that approach further. In May, we began seeing the group hide C&C servers behind Cloudflare workers (workers.dev), and in June it added Microsoft's devtunnels.ms and Loophole (loophole.site). These services were often used together, with one acting as the primary communication path and others serving as fallbacks.

In a few isolated cases, we also saw experiments with other tunnel services, such as loca.lt and bore.pub, but these did not appear to become part of the group's regular toolkit.

Gamaredon also returned to a technique that had once been a [hallmark of its operations](#): dynamic DNS (DDNS). After several years of relying more heavily on registered domains, the group again began using [No-IP domains](#)

across multiple tools, especially in HTA downloaders delivered in spearphishing campaigns. In parallel, we observed Gamaredon abuse platform-as-a-service offerings from [Clever Cloud](https://cleverapps.io/) (cleverapps.io) and [Supabase](https://supabase.co/) (supabase.co) in several campaigns, suggesting that the group is still actively looking for cheap, disposable infrastructure that blends in with legitimate traffic.

Leveraging an old espionage concept: Dead drops

One of the most important aspects of Gamaredon's 2025 operations was its heavy use of so-called dead-drop services. The term comes from traditional espionage – instead of meeting directly, one operative leaves information in a public or hidden location and another retrieves it later. Online, the principle is similar. Rather than embedding the real malicious server directly in malware, operators place that information on a legitimate website or platform, and the malware retrieves it from there. This means that the malware may first contact a public page on a legitimate service, read a hidden or staged value from it, and only then connect to the actual C&C server.

This approach gives attackers several advantages. It makes their operations more flexible, because they can switch servers quickly. It also complicates blocking, because defenders may be reluctant to block legitimate and widely used services outright.

In 2025, Gamaredon abused numerous services in this way: Telegram channels (via t.me; Telegram's official URL shortener service), posts on the Telegra.ph (telegra.ph) and Teletype (teletype.in) platforms, reentry.co, write.as, Dropbox, [GoFile](https://gofile.io/), social networks DEV Community (dev.to) and Mastodon (mastodon.social), lesma (lesma.eu), nopaste.net, and Paste.ee (pastee.dev). In some cases, these services were used to publish updated C&C information. In others, they were used to deliver payloads or cloud-storage configuration data.

Compared to 2024, we also saw a shift in how Gamaredon used these dead drops. Rather than simply publishing raw C&C IP addresses, operators increasingly used them to point malware to infrastructure already hidden behind tunnels or workers. In other words, the dead drop often no longer revealed the real server directly; instead, it pointed to another intermediate layer.

Cloud storage became the preferred exfiltration channel

The other major infrastructure shift we observed was on the data-exfiltration side. Gamaredon upgraded two of its flagship file stealers, PteroPSDoor and PteroVDoor, to upload stolen files to S3-compatible cloud storage services – providers that support the [Amazon S3 API](https://aws.amazon.com/s3/), allowing the same tools and code to work across different storage vendors. Over the course of the year, configurations moved from [Wasabi](https://wasabisys.com/) (wasabisys.com) to [Tebi](https://tebi.io/) (tebi.io) and then to [Intercolo](https://de-fra.i3storage.com/) (de-fra.i3storage.com), which by December had become the primary exfiltration destination.

At the same time, PteroBox continued to upload files to Dropbox, and one newer variant used the [rclone](https://rclone.org/) utility to do so.

Uploading stolen files to cloud storage reduces the need for Gamaredon to maintain its own infrastructure for receiving large amounts of stolen data. It also helps malicious traffic blend in with access to legitimate storage providers. Essentially, Gamaredon increasingly uses third-party services not only to hide where instructions come from, but also to hide where stolen data goes.

Conclusion

Gamaredon continued to focus its cyberespionage activity exclusively on Ukraine throughout 2025, and nothing in ESET telemetry suggests that this will change in the near future.

While the six new tools introduced in 2025 were, for the most part, simple downloaders, the more important development was the continued evolution of the infrastructure supporting the group's operations. Gamaredon further expanded its use of dead drops, tunnels, workers, dynamic DNS, and cloud storage, making its operations more flexible and harder to disrupt.

As in previous years, the group compensated for the relative simplicity of its malware with persistence, frequent updates, and an increasingly creative abuse of legitimate online services. As long as Russia's war against Ukraine continues, we expect Gamaredon to remain a significant cyberespionage threat to Ukrainian institutions.

IoCs

A comprehensive list of indicators of compromise (IoCs) can be found in [our GitHub repository](#) and the [Gamaredon white paper](#).



Source: <https://www.welivesecurity.com/en/eset-research/gamaredon-2025-leveraging-tunnels-workers-dead-drops-new-alliances/>