ESET Research: Russia's Gamaredon APT group unleashed spearphishing campaigns against Ukraine with an evolved toolset

Archived: 2026-04-05 21:57:29 UTC

- In 2024, Gamaredon refocused exclusively on targeting Ukrainian governmental institutions.
- The group significantly increased the scale and frequency of spearphishing campaigns, employing new delivery methods.
- Gamaredon introduced six new malware tools, leveraging PowerShell and VBScript, designed primarily for stealth, persistence, and lateral movement.
- Gamaredon operators managed to hide almost their entire C&C infrastructure behind Cloudflare tunnels.
- Gamaredon increasingly relied on third-party services (Telegram, Telegraph, Cloudflare, Dropbox) to protect its C&C infrastructure.

BRATISLAVA — July 2, 2025 — ESET Research has released a white paper about Gamaredon's updated cyberespionage toolset, new stealth-focused techniques, and aggressive spearphishing operations observed across the previous year. Gamaredon, attributed by the Security Service of Ukraine (SSU) to the 18th Center of Information Security of Russia's Federal Security Service (FSB), has targeted Ukrainian governmental institutions since at least 2013. In 2024, Gamaredon exclusively attacked Ukrainian institutions. ESET's latest research shows that the group remains highly active, consistently targeting Ukraine, but has notably adapted its tactics and tools. The group's objective is cyberespionage aligned with Russian geopolitical interests. Last year, the group significantly increased the scale and frequency of spearphishing campaigns, employing new delivery methods, and one attack payload was used solely to spread Russian propaganda.

Gamaredon's spearphishing activities significantly intensified during the second half of 2024. Campaigns typically lasted one to five consecutive days, with emails containing malicious archives (RAR, ZIP, 7z) or XHTML files employing HTML smuggling techniques. These files delivered malicious HTA or LNK files that executed embedded VBScript downloaders, such as PteroSand. In October 2024, ESET observed a rare case where spearphishing emails included malicious hyperlinks instead of attachments – a deviation from Gamaredon's usual tactics. Furthermore, Gamaredon introduced another novel technique: using malicious LNK files to execute PowerShell commands directly from Cloudflare-generated domains, bypassing some traditional detection mechanisms.

Gamaredon's toolset underwent several notable updates. While fewer new tools were introduced, substantial resources went into updating and improving existing tools. New tools were designed primarily for stealth, persistence, and lateral movement. Existing tools received major upgrades, including enhanced obfuscation, improved stealth tactics, and sophisticated methods for lateral movement and data exfiltration.

"A particularly intriguing finding was the discovery in July 2024 of a unique ad hoc VBScript payload, delivered by Gamaredon downloaders. This payload had no espionage functionality; rather, its sole purpose was to automatically open a Telegram propaganda channel named Guardians of Odessa, which spreads pro-Russian messaging targeting the Odessa region," says ESET researcher Zoltán Rusnák, who tracks Gamaredon's activities.

Additionally, throughout 2024, Gamaredon showed persistent dedication to evading network-based defenses. The group continued, albeit at a reduced scale, to leverage fast-flux DNS techniques, frequently rotating IP addresses behind its domains. Gamaredon increasingly relied on third-party services such as Telegram, Telegraph, Codeberg, Dropbox, and Cloudflare tunnels to obfuscate and dynamically distribute its C&C infrastructure.

“Despite observable capacity limitations and abandoning older tools, Gamaredon remains a significant threat actor due to its continuous innovation, aggressive spearphishing campaigns, and persistent efforts to evade detections. As long as the Russia's war against Ukraine continues, we anticipate that Gamaredon will persist in evolving its tactics and intensify its cyberespionage operations against Ukrainian institutions,” concludes Rusnák.

For a more detailed analysis and technical breakdown of Gamaredon’s toolset, check out the latest ESET Research white paper, “Gamaredon in 2024: Cranking out spearphishing campaigns against Ukraine with an evolved toolset,” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

Unique Gamaredon spearphishing samples seen per month

About ESET

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown — securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts and blogs.
