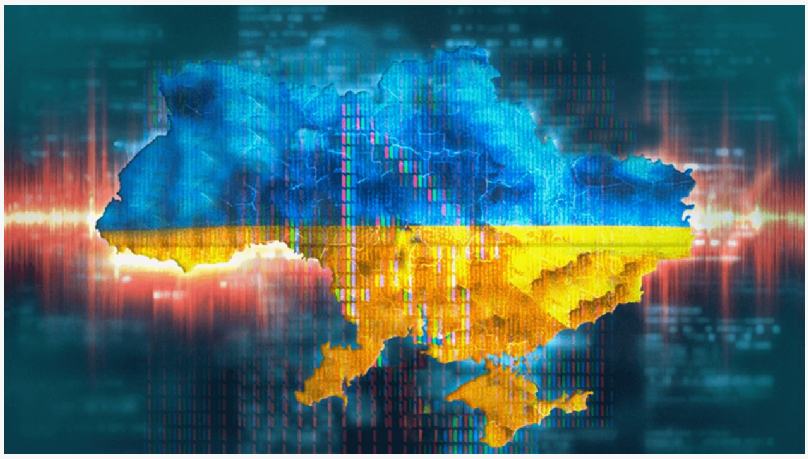
ESET Research: Russian FSB-linked Gamaredon and Turla team up to target high-profile Ukrainian entities



DUBAI , DUBAI, UNITED ARAB EMIRATES, September 30, 2025 /EINPresswire.com/ -- ESET Research has uncovered the first known cases of collaboration between Gamaredon and Turla. Both threat groups are associated with the main Russian intelligence agency, the FSB, and in tandem attacked high-profile targets in Ukraine. On the affected machines, Gamaredon deployed a wide range of tools, and on one of those machines, Turla was able to issue commands via Gamaredon implants.

“In the course of this year, ESET has detected Turla on seven machines in Ukraine. Since Gamaredon is compromising hundreds if not thousands of machines, this suggests that Turla is only interested in specific machines, probably those containing highly sensitive intelligence,” says ESET researcher Matthieu Faou, who discovered the Turla and Gamaredon collaboration in cooperation with ESET researcher Zoltán Rusnák.

Notably, in February 2025, ESET Research detected the execution of Turla’s Kazuar backdoor by Gamaredon’s PteroGraphin and PteroOdd on a machine in Ukraine. PteroGraphin was used to restart the Kazuar v3 backdoor, possibly after it crashed or was not launched automatically. Thus, PteroGraphin was probably used as a recovery method by Turla. This is the first time that anyone has been able to link these two groups together via technical indicators. In April and June 2025, ESET detected that Kazuar v2 was deployed using Gamaredon tools PteroOdd and PteroPaste.

Kazuar v3 is the latest branch of the Kazuar family, itself an advanced C# espionage implant that ESET believes is used exclusively by Turla; it was first seen in 2016. Other malware deployed by Gamaredon was PteroLNK, PteroStew, and PteroEffigy.

“Gamaredon is known for using spearphishing and malicious LNK files on removable drives, thus one of these was the most likely compromise vector. We believe with high confidence that both groups – separately associated with the FSB – are cooperating and that Gamaredon is providing initial access to Turla,” says Rusnák.

As already mentioned, both are part of the Russian FSB. According to Security Service of Ukraine, Gamaredon is thought to be operated by officers of Center 18 of the FSB (aka the Center for Information Security) in Crimea, which is part of the FSB’s counterintelligence service. As for Turla, the UK’s National Cyber Security Centre attributes the group to the Center 16 of the FSB, which is Russia’s main signals intelligence agency.

From an organizational perspective, it is worth noting that the two entities commonly associated with Turla and Gamaredon have a long history of reported collaboration, which can be traced back to the Cold War era. 2022’s full-scale invasion of Ukraine has probably reinforced this convergence, with ESET data clearly showing Gamaredon and Turla activities focusing on the Ukrainian defense sector in recent months.

Gamaredon has been active since at least 2013. It is responsible for many attacks, mostly against Ukrainian governmental institutions. Turla, also known as Snake, is an infamous cyberespionage group that has been active since at least 2004, possibly extending back into the late 1990s. It mainly focuses on high-profile targets, such as governments and diplomatic entities, in Europe, Central Asia, and the Middle East. It is known for having breached major organizations such as the US Department of Defense in 2008 and the Swiss defense company RUAG in 2014.

For a more detailed analysis and technical breakdown of Turla and Gamaredon’s interactions, check out the latest ESET Research blogpost “Gamaredon X Turla collab” 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.

About ESET
ESET® provides cutting-edge cybersecurity 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 ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications

+971 55 972 4623
email us here