Two of the Kremlin's most active hack groups are collaborating, ESET says

But ESET said its most likely hypothesis is that Turla and Gamaredon were working together. "Given that both groups are part of the Russian FSB (though in two different Centers), Gamaredon provided access to Turla operators so that they could issue commands on a specific machine to restart Kazuar, and deploy Kazuar v2 on some others," the company said.

Friday's post noted that Gamaredon has been seen collaborating with other hack groups previously, specifically in 2020 with a group ESET tracks under the name InvisiMole.

In February, ESET said, company researchers spotted four distinct Gamaredon-Turla co-compromises in Ukraine. On all of the machines, Gamaredon deployed a wide range of tools, including those tracked under the names PteroLNK, PteroStew, PteroOdd, PteroEffigy, and PteroGraphin. Turla, for its part, installed version 3 of its proprietary malware Kazuar.

ESET software installed on one of the compromised devices observed Turla issuing commands through the Gamaredon implants.

"PteroGraphin was used to restart Kazuar, possibly after Kazuar crashed or was not launched automatically," ESET said. "Thus, PteroGraphin was probably used as a recovery method by Turla. This is the first time that we have been able to link these two groups together via technical indicators (see First chain: First chain: Restart of Kazuar v3)."

Then, in April and again in June, ESET said it detected Kazuar v2 installers being deployed by Gamaredon malware. In all the cases, ESET software was installed after the compromises, so it wasn’t possible to recover the payloads. Nonetheless, the firm said it believes an active collaboration between the groups is the most likely explanation.

“All those elements, and the fact that Gamaredon is compromising hundreds if not thousands of machines, suggest that Turla is interested only in specific machines, probably ones containing highly sensitive intelligence,” ESET speculated.

https://arstechnica.com/security/2025/09/two-of-the-kremlins-most-active-hack-groups-are-collaborating-eset-says/