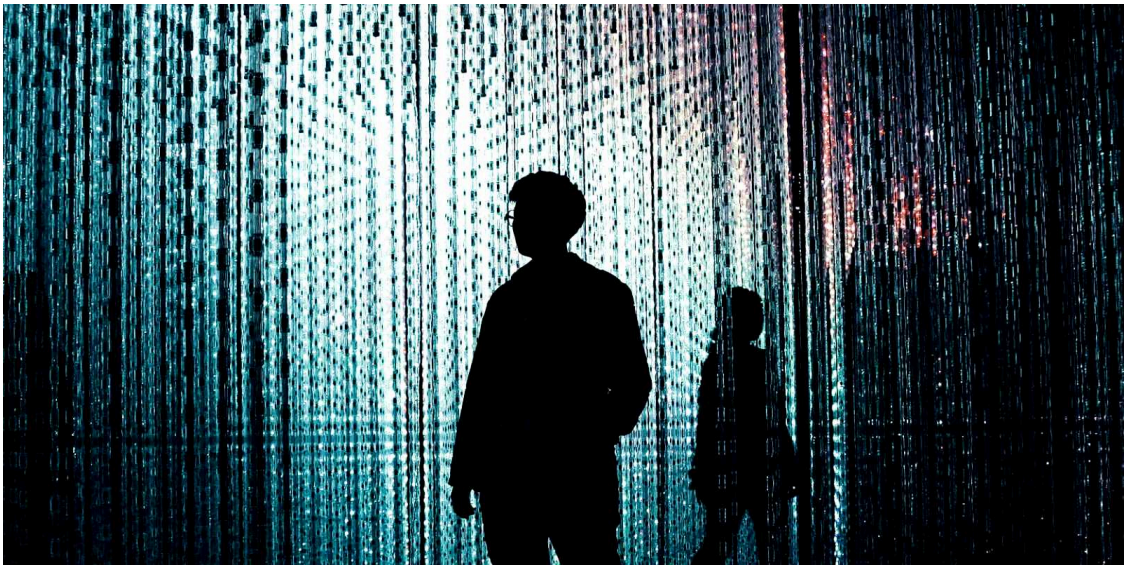
Ukraine links members of Gamaredon hacker group to Russian FSB

By Bill Toulas

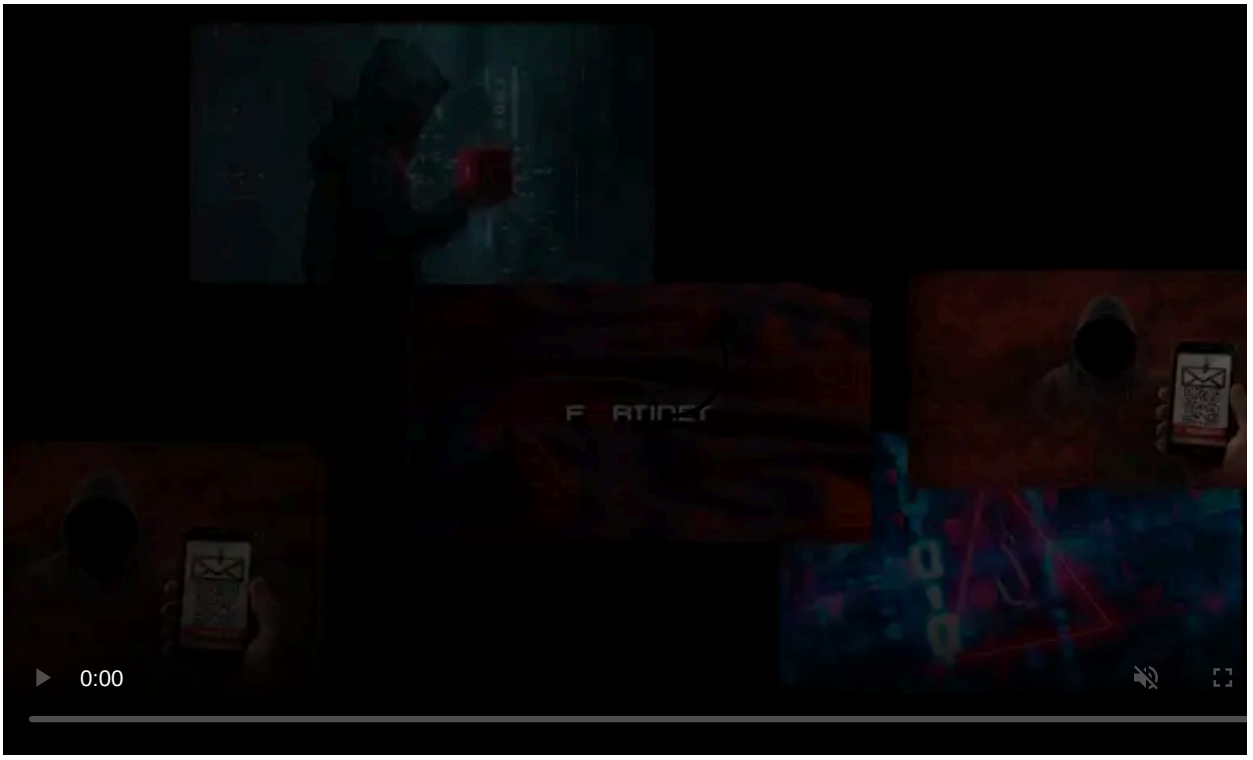
Published: 2021-11-04 · Archived: 2026-04-05 22:58:31 UTC

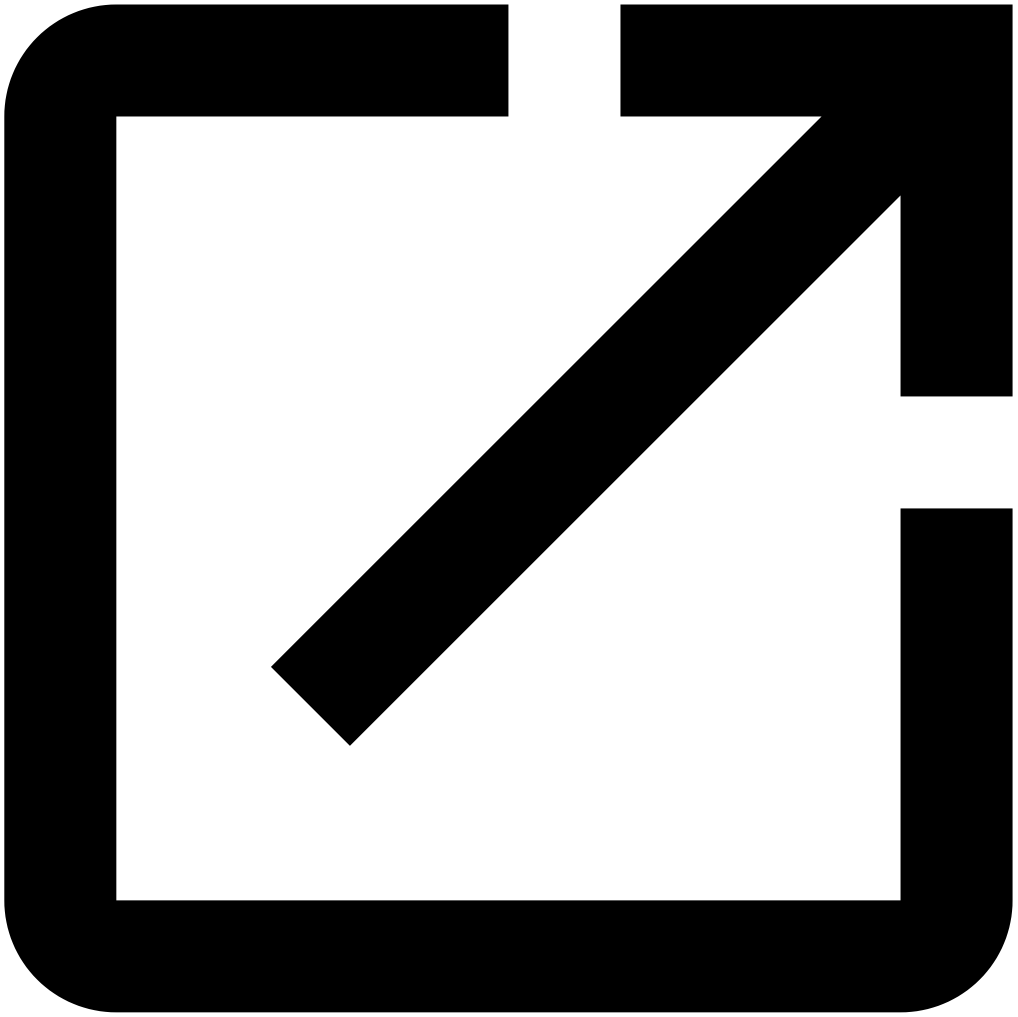


SSU and the Ukrainian secret service say they have identified five members of the Gamaredon hacking group, a Russian state-sponsored operation known for targeting Ukraine since 2014.

This Gamaredon hacking group, tracked as Armageddon by the SSU, is allegedly operated under the FSB (Russian Federal Security Service) and is believed to be responsible for over 5,000 attacks in Ukraine since the operation began.

Over the last seven years, Ukraine says the actors targeted over 1,500 government, public and private entities in the country, aiming to collect intelligence, disrupt operations, and take control over critical infrastructure facilities.

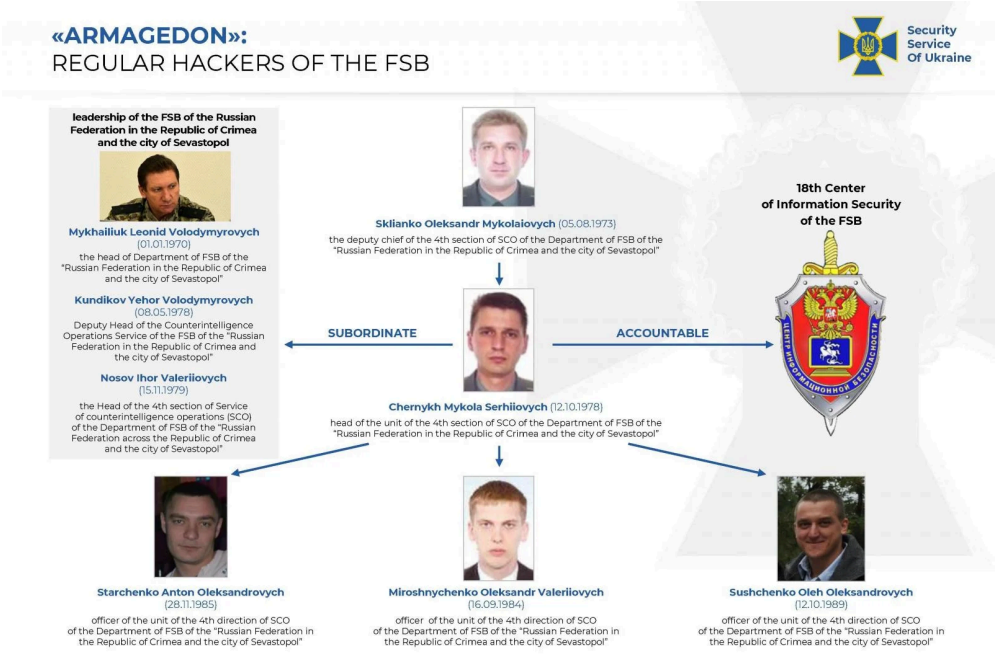

0:00



The five men accused of taking part in these attacks were identified by SSU investigators who claim to have unequivocal evidence of their involvement, coming from communication interceptions.

The investigators underline that they managed to identify the hackers despite using their own custom malware, anonymization tools, and were generally very diligent in hiding their digital trace.

The names of the five individuals the SSU claims are part of the Gamaredon operation are Sklianko Oleksandr Mykolaiovych, Chernykh Mykola Serhiovych, Starchenko Anton Oleksandrovych, Miroshnychenko Oleksandr Valeriovych, and Sushchenko Oleh Oleksandrovych.



Identities of the five identified Armageddon members
Source: SSU

All five were reportedly operating under the guidance of the 18th Center of Information Security of the FSB in Moscow.

Moreover, all of them are officers of the Crimean FSB who sided with Russia during the peninsula's occupation in 2014.

As such, the Ukrainian authorities are also accusing them of treason, espionage, unauthorized inference in the work of electronic computers, and distribution and use of malware.

Although the five men haven't been arrested, the SSU sees their exposure as an effective neutralization measure.

Entire toolset and tactics exposed

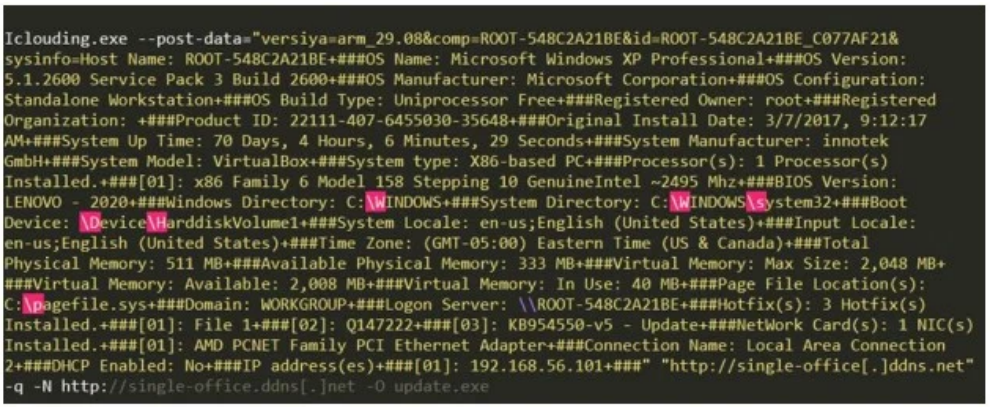
The SSU has published a technical activity report on Gamaredon, where they lay down several key points around the group's toolset and tactics.

The report says the group is known to use Outlook macros and the deployment of EvilGnome backdoor to compromise systems.

Other details include highly targeted vulnerabilities such as the WinRAR CVE-2018-20250 vulnerability, which existed for almost two decades, and CVE-2017-0199, a remote code execution flaw on MS Office.

Moreover, it is mentioned that the actors used removable media to plant malware on offline systems and then moved laterally in isolated networks, using this tactic from 2014 until 2021.

Finally, a novel malware tool named “Pteranodon” is detailed in the report, which is a modular remote administration tool (RAT) with powerful anti-analysis and info-collection features.



Pteranodon exfiltrating data to the C2
Source: SSU

According to SSU, Pteranodon was derived from “Pterodo,” a widely available malware circulating Russian hacking forums since 2016.

The group continued to create new powerful DLL modules for Pteranodon, so it has evolved significantly over the past five years.

The release of these technical details will empower analysts to assign attribution on past attacks and momentarily reduce Russian state actors' operational effectiveness.
