Russia arrests three alleged SugarLocker ransomware members

By Daryna Antoniuk

Published: 2024-02-22 · Archived: 2026-04-05 19:16:49 UTC

Russian authorities have identified and arrested three alleged members of a local ransomware gang called SugarLocker.

The group operates under the guise of a legitimate tech company called Shtazi-IT, offering services for the development of landing pages, mobile apps, and online stores, according to a report by F.A.C.C.T., a Russia-based company that was involved in investigating the group's activities alongside authorities.

F.A.C.C.T. is a spinoff of the cybersecurity firm Group-IB, which left the Russian market last year and is currently headquartered in Singapore.

The timing of the arrest announcement is “extraordinary” as it overlapped with a massive international operation against the ransomware gang Lockbit, said Dmitry Smilyanets, a product management director at Recorded Future, the parent company of The Record.

“It could be coincidental or could be timed specifically to show they can also do arrests,” he said.

Another security expert, who asked not to be identified due to security concerns, also suggested that this arrest could be a PR attempt by Russia. The suspects identified might not be under the strict operational control of the government and would likely continue their operations, they said.

According to F.A.C.C.T., the SugarLocker malware has been deployed since at least 2021 as ransomware-as-a-service, a model in which malicious tools are offered for a fee or a share of the ransom payments collected by the criminals.

For instance, they found that SugarLocker receives 30% of its customers' profits or 10% if they exceed $5 million.

The group has mostly attacked its targets through the Remote Desktop Protocol (RDP), which allows users to access and control a computer remotely over a network.

Upon its launch, SugarLocker pledged not to attack Eastern European countries, except the Baltic States and Poland. The group does not operate a data leak site, so it's not clear who their victims are.

SugarLocker affiliates purport to be motivated exclusively by financial interests in carrying out cyberattacks.

“It's just a business. We absolutely do not care about you and your deals, except getting benefits,” the group’s ransom note said. “If you will not cooperate with our service — for us, it does not matter. But you will lose your time and data.”

The person who announced the malware’s launch in 2021 on the darknet forum called RAMP went by the username "Gustave Dore" — a pseudonym that was also used by the Russian citizen Aleksandr Ermakov, who

was sanctioned by Australia, the U.K., and the U.S. in January for his alleged involvement in the 2022 attack on the Australian health insurance provider, Medibank.

Ermakov is believed to be part of the infamous Russian cybercrime group REvil — one of the most active ransomware gangs. F.A.C.C.T. has not officially confirmed Ermakov's link to SugarLocker.

The security expert familiar with the group's operation who asked not to be identified told Recorded Future News that Aleksandr Ermakov is definitely connected to SugarLocker, but they speculated that a different hacker with the same name could have been involved with the Medibank attack.

When the police searched SugarLocker members' apartments earlier in January, they reportedly found laptops, mobile phones, correspondence, and other digital evidence of illegal activity.

The detained members went by the nicknames blade_runner, GustaveDore, and JimJones.

The defendants have already been charged with creating, using, and distributing malicious computer programs. If found guilty, they could face up to four years in prison. The investigation is ongoing, according to F.A.C.C.T.

Researchers said that after group members saw that SugarLocker was under investigation, one of them joked in private chats: "Guys, I'm going to Siberia, I definitely need to."

Siberia is associated with Russian prisons and exile due to its harsh climate and remote unpopulated areas.

The hacker's joke, F.A.C.C.T. said, turned out to be "prophetic."

No previous article

No new articles

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
