REvil ransomware affiliates arrested in Romania and Kuwait

By Sergiu Gatlan

Published: 2021-11-08 · Archived: 2026-04-05 14:55:21 UTC

Romanian law enforcement authorities have arrested two suspects believed to be Sodinokibi/REvil ransomware affiliates on November 4, both of them allegedly responsible for infecting thousands of victims.

DIICOT (the Romanian Directorate for Investigating Organized Crime and Terrorism) and judicial police officers carried out four home searches in Constanța, seizing mobile devices (laptops, mobile phones) and storage media.

The Bucharest Tribunal also ordered the pre-trial detention for the two REvil affiliates for 30 days.


DIE LINKE.
0:00

On the same day, Kuwaiti authorities also arrested a GandGrab ransomware affiliate, the three of them being suspected of roughly 7,000 attacks and of asking more than €200 million in ransoms.

In total, together with the ones apprehended on November 4, **authorities arrested seven suspects linked to REvil and GandGrab since February 2021.**

Three other individuals believed to be REvil affiliates were apprehended in South Korea in February, April, and October, and one was arrested in Europe last month.

The announcement, made today by Europol (the European Union Agency for Law Enforcement Cooperation), says the arrests are the result of operation GoldDust, which involved law enforcement agents from 17 countries, the Europol, Eurojust, and the INTERPOL.

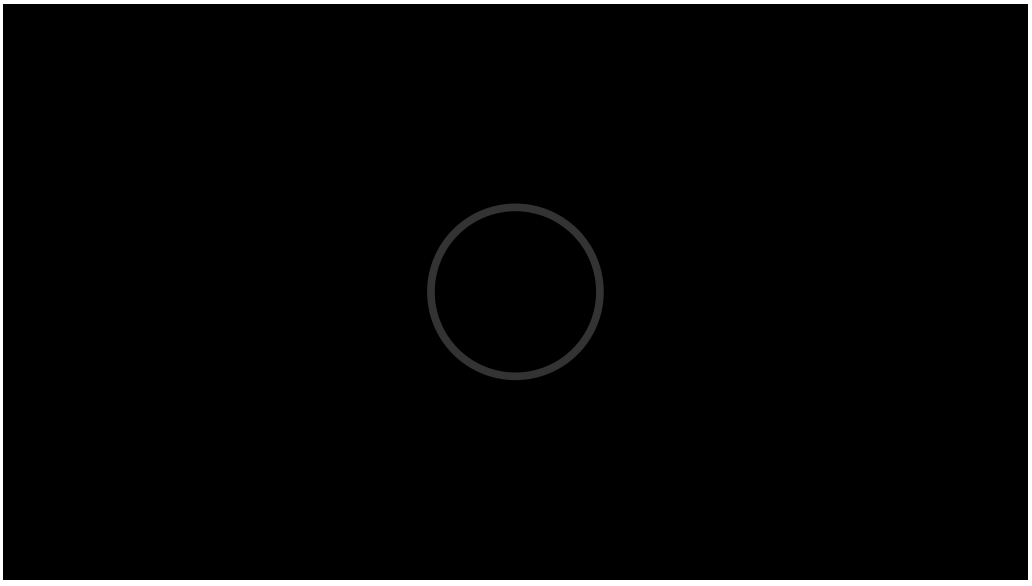
"Since 2018, Europol has supported a Romanian-led investigation which targets the GandCrab ransomware family and involved law enforcement authorities from a number of countries, including the United Kingdom and the United States," the Europol said.

"All these arrests follow the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family, which is seen as the successor of GandCrab."

These recent arrests show that law enforcement worldwide has realized that they can't get to the core ransomware gang operators who are safe in Russia.

However, their Ransomware-as-a-Service (RaaS) operations can easily be disrupted by arresting ransomware affiliates located all over the world.

US Deputy Attorney General Lisa Monaco also announced that the US will crack down on ransomware activity in an interview with the Associated Press on November 4.



Source: https://www.bleepingcomputer.com/news/security/revil-ransomware-affiliates-arrested-in-romania-and-kuwait/