

Two ransomware operators arrested in Ukraine

By Catalin Cimpanu

Published: 2022-12-16 · Archived: 2026-04-05 12:48:49 UTC

Two members of a ransomware gang were arrested in Ukraine following a joint international law enforcement operation.

The arrests took place last week, on September 28, in Kyiv, Ukraine's capital, and were carried out by officers of the Ukrainian National Police, with aid from the French Gendarmerie, the FBI, Europol, and Interpol.

Two suspects were arrested, including a 25-year-old believed to be a crucial member of a large ransomware operation.

Officials declined to name the suspect's affiliation to any particular ransomware gang, citing an ongoing official investigation, a Europol spokesperson told *The Record* today.

Ukraine officials said in a [press release](#) the suspect was responsible for attacks on more than 100 companies across the world and has caused more than \$150 million in damages.

Following searches at seven properties, including family members of the 25-year-old main suspect, officers seized computers used to access remote servers from where the ransomware was deployed, two cars, \$375,000 in cash, and \$1.3 million in cryptocurrencies.

In a [press release](#), Europol said the suspects had been active since April 2020 and that their group was "known for their extortionate ransom demands (between €5 to €70 million)."

Several security researchers have suggested that the two suspects arrested last week were members of the REvil ransomware gang.

That certainly sounds like [#REvil #ransomware](#). The [#Kaseya](#) ransom demand was famously \$70 Million, and the average person may think REvil started in April 2020, with the famous hack of Grubman Shire Meiselas & Sacks happening about that time.

— GarWarner (@GarWarner) [October 4, 2021](#)

In addition, a video of one of the house searches released by Ukrainian police shows officers sifting through unlocked computers and tablets, suggesting that investigators might have gained access to sensitive information that may allow them to infiltrate the ransomware gang's structure.

Ett fel inträffade.

Det går inte att köra JavaScript.

Get more insights with the

Recorded Future

Intelligence Cloud.

[Learn more.](#)

 Recorded Future®

Know what matters.

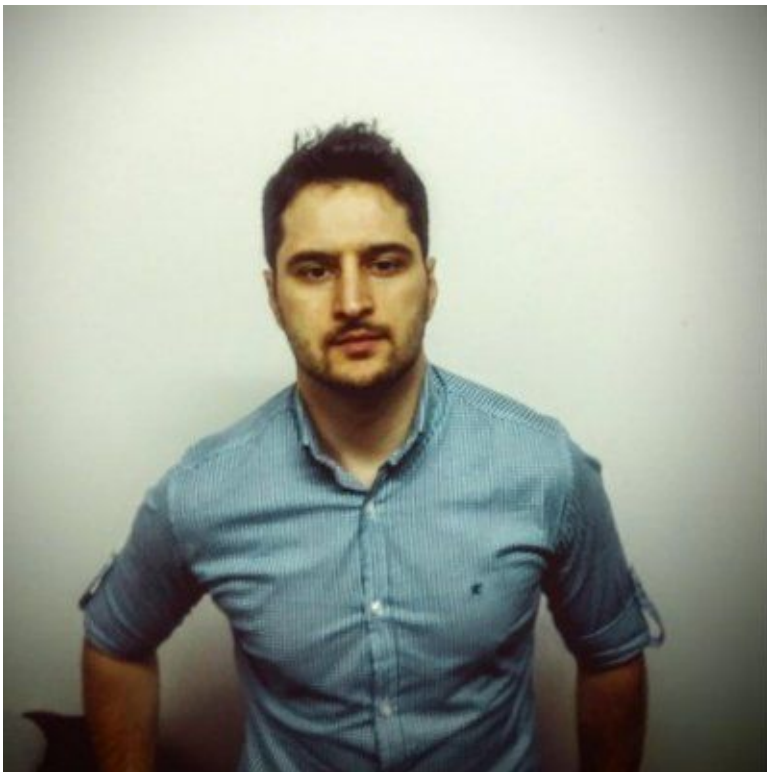
Act first.

Get started



No previous article

No new articles



[Catalin Cimpanu](#)

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

Source: <https://therecord.media/two-ransomware-operators-arrested-in-ukraine/>