German investigators identify REvil ransomware gang core member

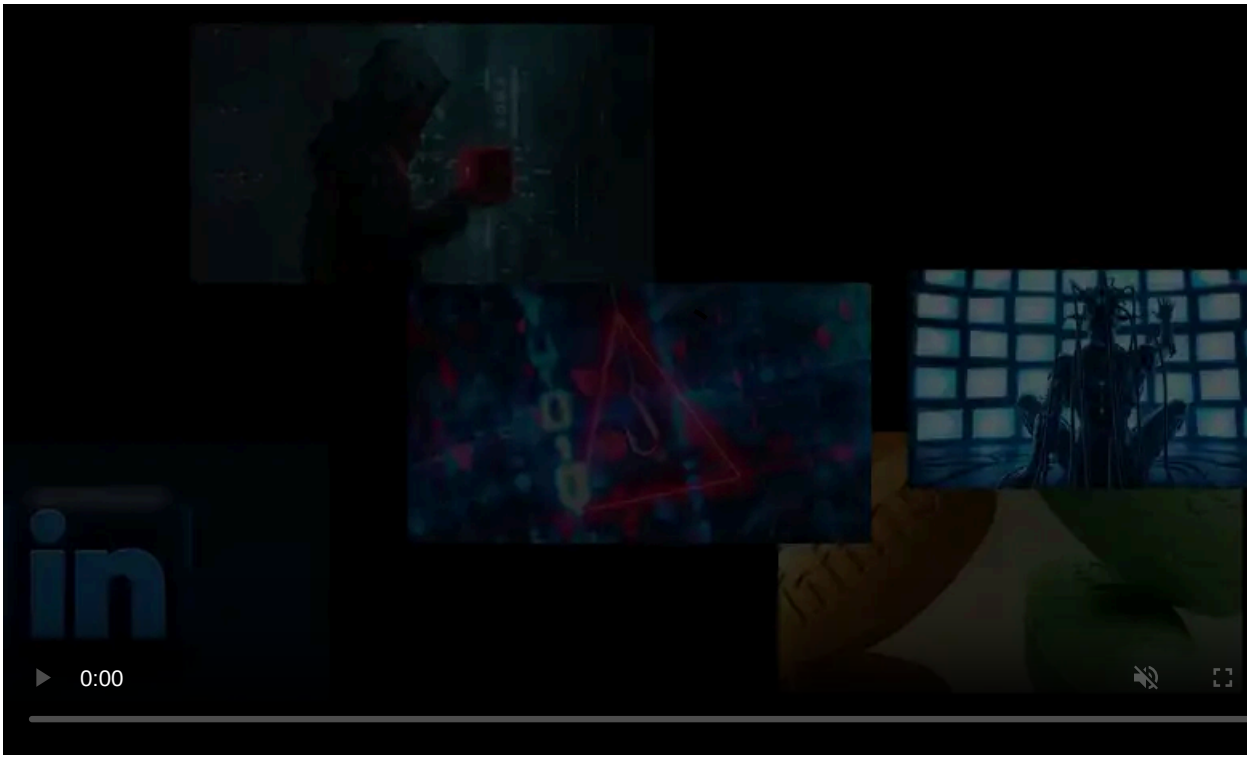
By Bill Toulas

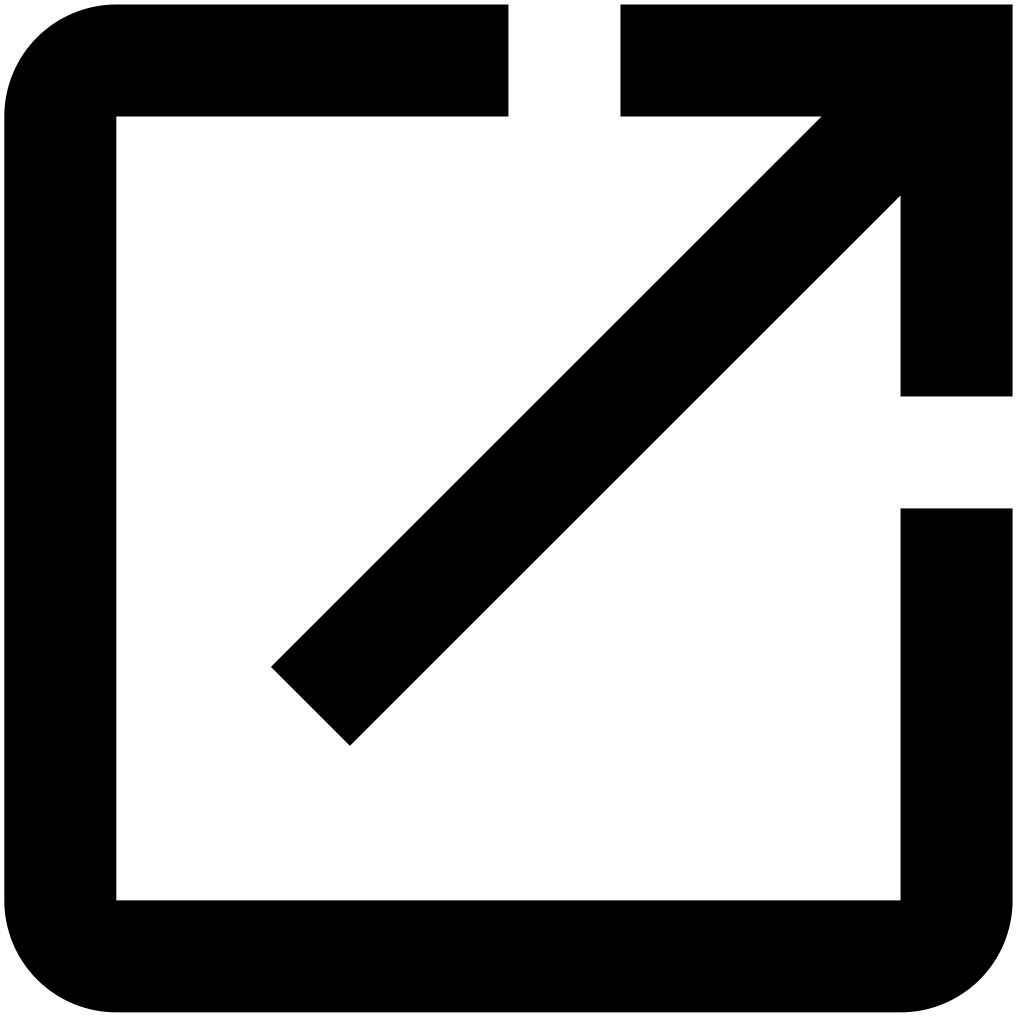
Published: 2021-10-28 · Archived: 2026-04-05 16:10:39 UTC

German investigators have reportedly identified a Russian man whom they believe to be one of REvil ransomware gang's core members, one of the most notorious and successful ransomware groups in recent years.

The man is presenting himself as a cryptocurrency investor and trader, but German authorities (including Bundeskriminalamt and Landeskriminalamt Baden-Württemberg) think otherwise after tracking some of the Bitcoin payments he made over the years.

While the suspect's real identity has not been revealed, German media is calling him by the fictitious name 'Nikolay K.', and report that investigators linked him to Bitcoin ransom payments associated with the GandCrab ransomware group.


0:00



Law enforcement tracked these payments following attacks against a software development firm and the State Theater in Stuttgart.

The same sources claim that the investigators have found strong links between REvil and GandCrab, something that has been suggested numerous times by security researchers and analysts.

Nikolay K. didn't hold back when it came to boasting on social media and showcasing his holidays on the Mediterranean, posting images from lavish yacht parties.

But he wasn't careful enough when it came to hiding his true identity, falsely assuming that masking his links to ransomware operations with crypto-investment would be enough.

Tracked down using an email address

As the reports detail, the police were able to find Nikolay's email address, which he used to register to over 60 websites, as well as a phone number that he used for his Telegram account.

That account was supposedly used for legit crypto-trading, but the police were reportedly able to link multiple transactions worth over 400,000 Euros in crypto to ransom payment events.

Since the crackdown on REvil's infrastructure, from two weeks ago, the group's members have been extra cautious, but it appears that Nikolay was unaware of how close the investigators really were to arrest him.

This summer, Nikolay's wife traveled for holidays alone, while the ransomware actors stayed in Russia, possibly to avoid any unexpected arrests while on foreign grounds.

Neither the Federal Criminal Police Office of Baden-Württemberg nor the Stuttgart public prosecutor's office have offered a comment on whether they have issued an extradition request to Russia yet, so we are still waiting for an official confirmation on the above.

Considering the dimensions that the ransomware threat has taken at the highest political level, it would be a surprise to see the Russians denying the prosecution of Nikolay.

Correction 10/28/21: Clarified that 'Nikolay K' is a fictitious name and that the real identity has not been revealed.

Source: https://www.bleepingcomputer.com/news/security/german-investigators-identify-revil-ransomware-gang-core-member/