Germany doxxes Conti ransomware and TrickBot ring leader

By Sergiu Gatlan

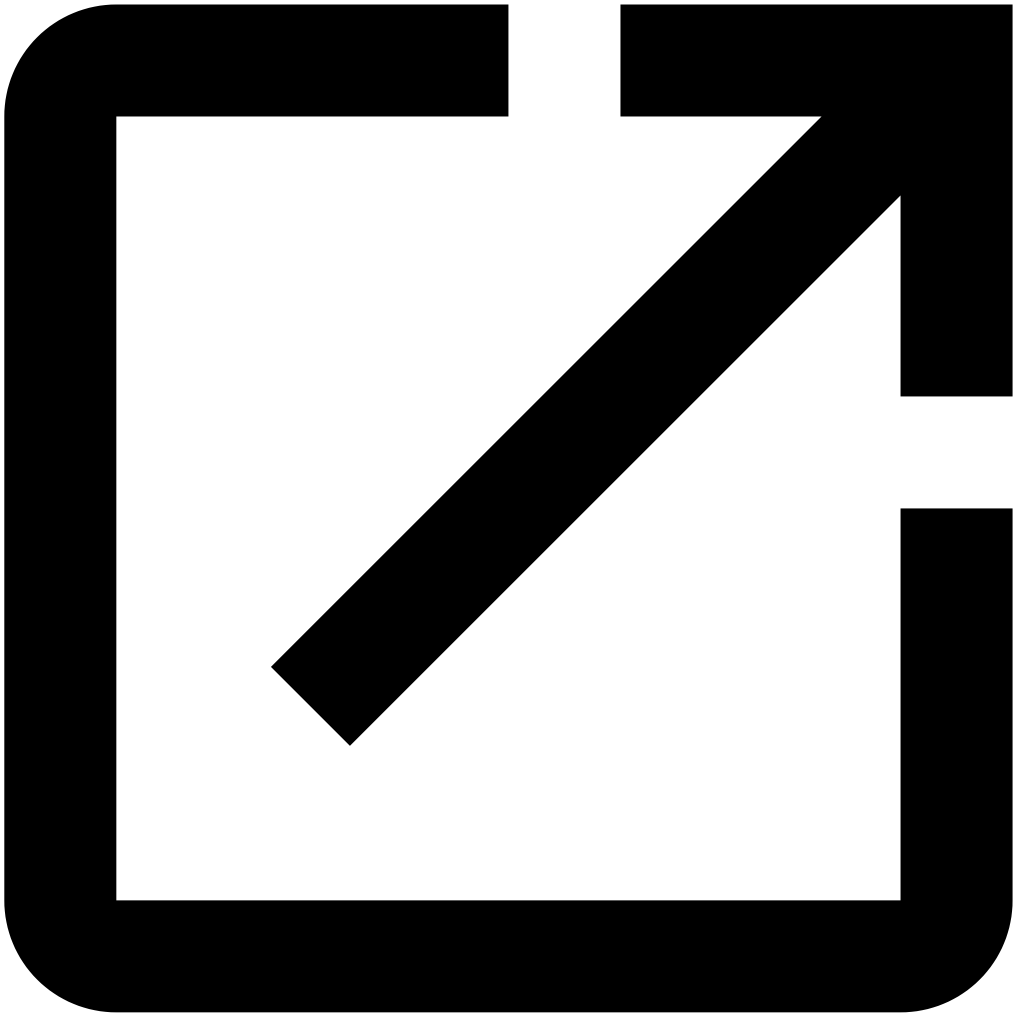
Published: 2025-05-30 · Archived: 2026-04-05 14:16:07 UTC

The Federal Criminal Police Office of Germany (Bundeskriminalamt or BKA) claims that Stern, the leader of the Trickbot and Conti cybercrime gangs, is a 36-year-old Russian named Vitaly Nikolaevich Kovalev.

"The subject is suspected of having been the founder of the 'Trickbot' group, also known as 'Wizard Spider,'" BKA said last week [English PDF], after another round of seizures and charges part of Operation Endgame, a joint global law enforcement action targeting malware infrastructure and the threat actors behind it.

"The group used the Trickbot malware as well as other malware variants such as Bazarloader, SystemBC, IcedID, Ryuk, Conti and Diavol."


DIE LINKE.
0:00



Kovalev is now also wanted in Germany, according to a recently issued Interpol red notice saying he was charged with being the ringleader of an unnamed criminal organization.

However, this isn't the first time law enforcement has targeted Kovalev for his involvement in a cybercriminal organization. In February 2023, he was one of seven Russians sanctioned and charged in the United States for their links to the TrickBot and Conti cybercrime gangs.

Still, he was only tagged at the time as a senior figure within the Trickbot group using the aliases "Bentley," "Bergen," "Alex Konor," and "Ben."

Vitaly Nikolayevich Kovalev (U.S. Secret Service)

The sanctions came after a massive trove of personal information and internal conversations was leaked from TrickBot and Conti members in what was called TrickLeaks and ContiLeaks.

While ContiLeaks provided access to the gang's internal conversations and source code, TrickLeaks went one step further, leaking the identities, online accounts, and personal information of TrickBot members on Twitter.

These conversations exposed that Kovalev, under the alias "Stern," was in charge of the TrickBot operation and the Ryuk and Conti ransomware gangs. The chats illustrated how the other members would contact Stern for approval before conducting attacks or hiring lawyers for Trickbot members arrested in the United States.

The leaks ultimately expedited Conti's shutdown, with the cybercrime members moving to other operations or starting new gangs, including Royal, Black Basta, BlackCat, AvosLocker, Karakurt, LockBit, Silent Ransom, DagonLocker, and ZEON.

"According to the investigations conducted by the BKA, at times, the Trickbot group consisted of more than 100 members. It works in an organized and hierarchically structured manner and is project and profit-oriented," BKA added last Friday.

"The group is responsible for the infection of several hundred thousand systems in Germany and worldwide; through its illegal activities it has obtained funds in the three-digit million range. Its victims include hospitals, public facilities, companies, public authorities, and private individuals."

While Kovalev's current whereabouts are unknown, German police believe that he currently lives in Russia and have asked for any information that could lead to his capture, including his current online accounts or what communication channels he uses.
