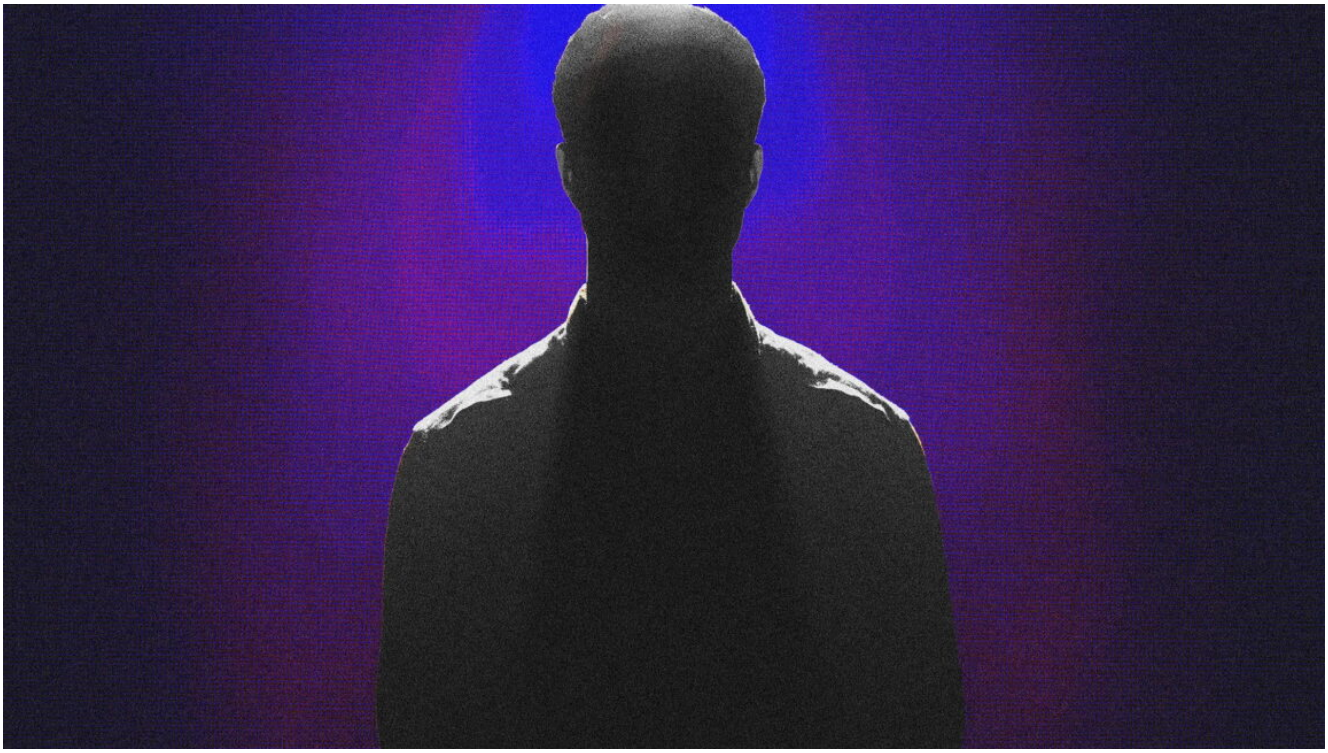
Ransomware kingpin “Stern” apparently IDed by German law enforcement



Stern’s eminence within Russian cybercrime has been widely documented. The cryptocurrency-tracing firm Chainalysis does not publicly name cybercriminal actors and declined to comment on BKA’s identification, but the company emphasized that the Stern persona alone is one of the all-time most profitable ransomware actors it tracks.

“The investigation revealed that Stern generated significant revenues from illegal activities, in particular in connection with ransomware,” the BKA spokesperson tells WIRED.

Stern “surrounds himself with very technical people, many of which he claims to have sometimes decades of experience, and he’s willing to delegate substantial tasks to these experienced people whom he trusts,” says Keith Jarvis, a senior security researcher at cybersecurity firm Sophos’ Counter Threat Unit. “I think he’s always probably lived in

that organizational role.”

Increasing evidence in recent years has indicated that Stern has at least some loose connections to Russia’s intelligence apparatus, including its main security agency, the Federal Security Service (FSB). The Stern handle mentioned setting up an office for “government topics” in July 2020, while researchers have seen other members of the Trickbot group say that Stern is likely the “link between us and the ranks/head of department type at FSB.”

Stern’s consistent presence was a significant contributor to Trickbot and Conti’s effectiveness—as was the entity’s ability to maintain strong operational security and remain hidden.

As Sophos’ Jarvis put it, “I have no thoughts on the attribution, as I’ve never heard a compelling story about Stern’s identity from anyone prior to this announcement.”

This story originally appeared on wired.com.

https://arstechnica.com/security/2025/05/german-police-say-theyve-identified-trickbot-ransomware-kingpin/