DoppelPaymer ransomware group suspects identified

By Pieter Arntz

Published: 2023-09-19 · Archived: 2026-04-05 14:34:33 UTC

The German police in cooperation with the US Secret Service have executed search warrants against suspected members of the DoppelPaymer ransomware group in Germany and Ukraine.

In March of 2023, we reported how the German Regional Police and the Ukrainian National Police, with support from Europol, the Dutch Police, and the United States Federal Bureau of Investigations (FBI), apprehended two suspects and seized computer equipment.

Since then, cybercrime group specialists from the North Rhine-Westphalia State Criminal Police Office (LKA NRW), together with the Cybercrime Central and Contact Point (ZAC NRW), carried out another targeted strike against people associated with the criminal network.

Two men in particular became the focus during blockchain investigations by the LKA NRW and the US Secret Service. They are a 44-year-old Ukrainian who apparently held a key position within the organization and a 45-year-old man from southern Germany who is suspected of having received suspicious funds, possibly originating from ransomware attacks.

Cryptocurrency investigators use specialized strategies to track down criminals. The investigators use tools to collect evidence, trace funds through the blockchain, and try to determine who converted them into fiat currencies. Although cryptocurrency is anonymous, that doesn't mean it's untraceable. All the transactions are recorded on a public ledger, which provides a treasure trove of data to search, analyze, and categorize.

Over the last years, DoppelPaymer claimed responsibility for a high-profile ransomware attack on Kia Motors America. The gang was also responsible for a costly attack on the St. Lucie County sheriffs department, the Dutch Institute for Scientific Research (NWO), and the Illinois Attorney General's office. Other victims attacked by DoppelPaymer in the past include Compal, PEMEX (Petróleos Mexicanos), the City of Torrance in California, Newcastle University, Hall County in Georgia, Banijay Group SAS, and Bretagne Télécom.

Since March of 2021, DoppelPaymer has been missing from our monthly ransomware reviews, and the last known leak site address we had on record for them has been taken offline.

During their active period (2017 – 2021), more than 600 victims worldwide were extorted, some of them up to double-digit millions. The investigations by the German authorities, which have been ongoing since 2020, led to the international public search for Igor Olegovich Turashev and Igor Garshin in March 2023. Both of these suspects are currently on EUROPOL's "Most-Wanted" list. The suspicion against a third person could not be sufficiently substantiated during further investigations, so the public search was withdrawn.

Source: https://www.malwarebytes.com/blog/news/2023/09/doppelpaymer-ransomware-group-suspects-identified