Moldova arrests suspect linked to DoppelPaymer ransomware attacks

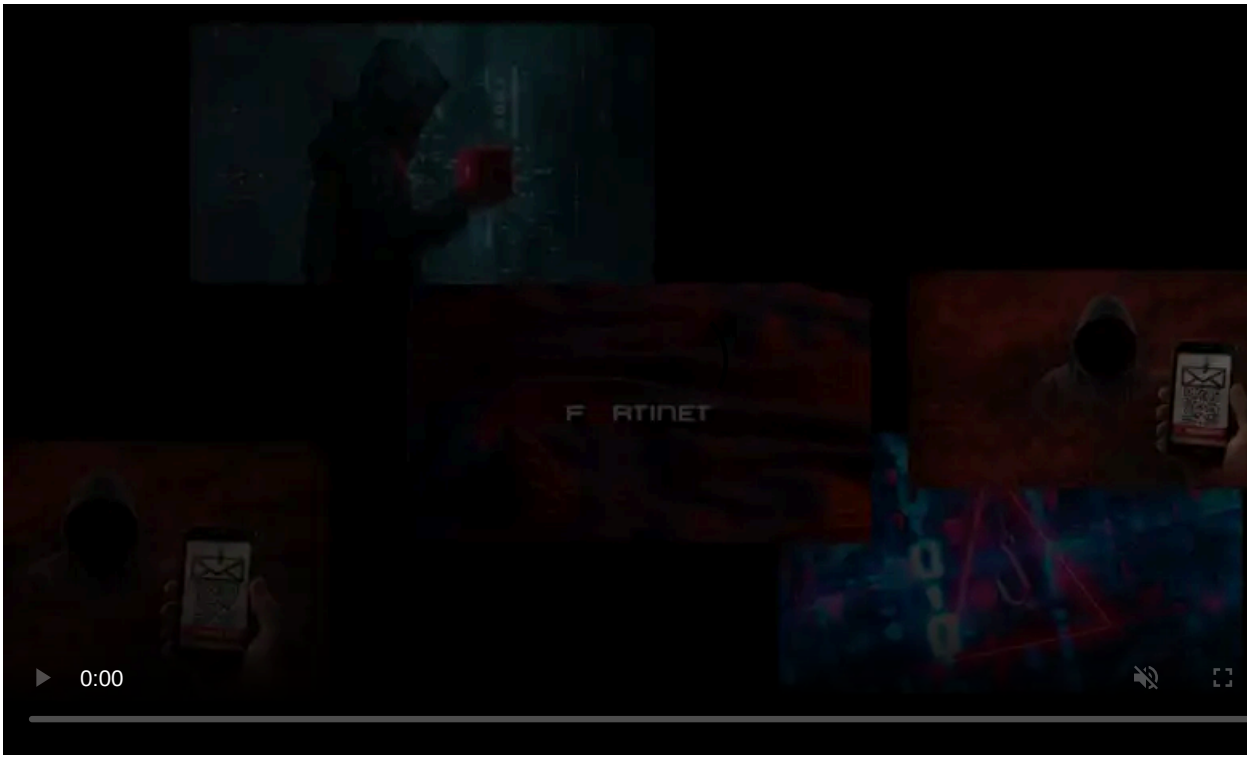
By Sergiu Gatlan

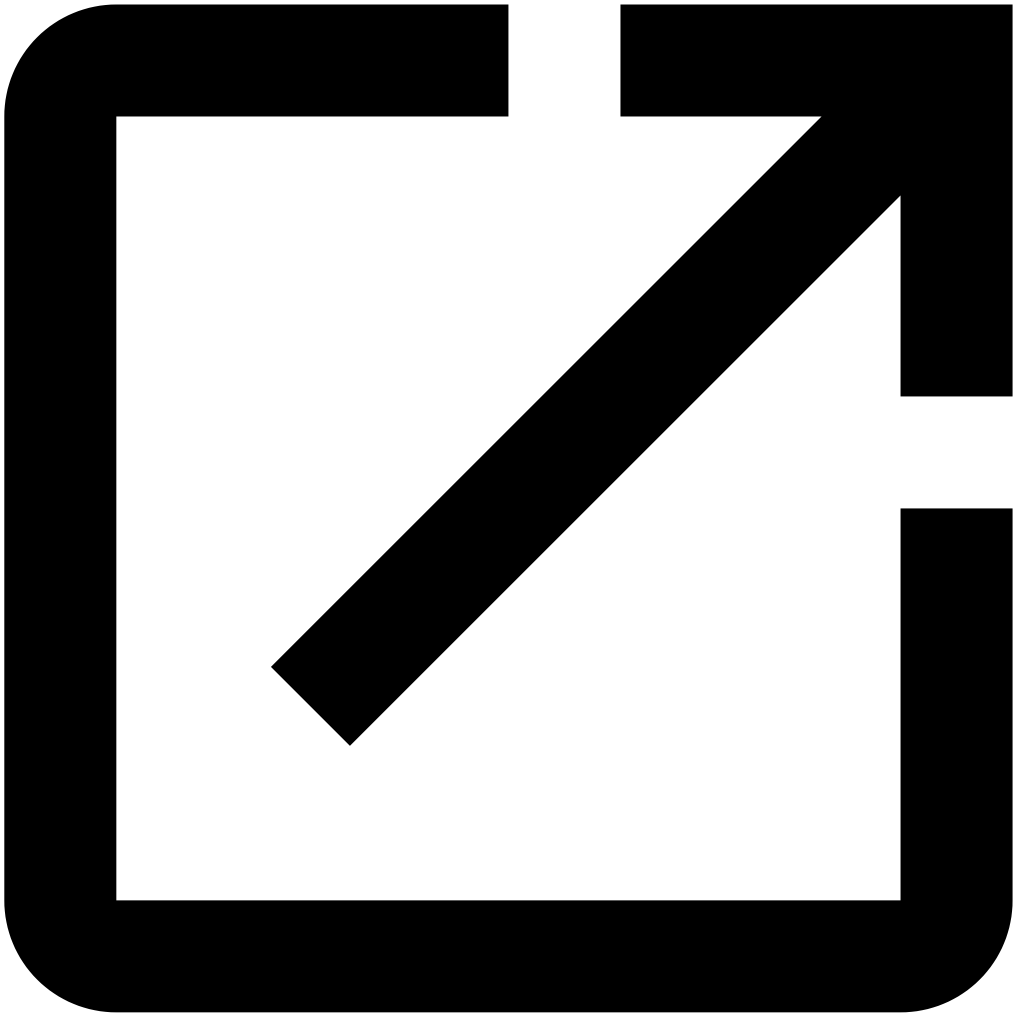
Published: 2025-05-12 · Archived: 2026-04-05 21:35:37 UTC

Moldovan authorities have detained a 45-year-old suspect linked to DoppelPaymer ransomware attacks targeting Dutch organizations in 2021.

Police officers searched the suspect's home and car on May 6, seizing an electronic wallet, €84,800, two laptops, a mobile phone, a tablet, six bank cards, and multiple data storage devices.

The suspect remains in custody, while Moldovan prosecutors have initiated legal procedures to extradite him to the Netherlands.


F RTINET
0:00



The arrest resulted from a joint action involving Moldovan prosecutors, the country's Center for Combating Cybercrimes, and law enforcement in the Kingdom of the Netherlands.

A Monday press release added that the suspect, described as a "foreign citizen," had allegedly orchestrated a 2021 ransomware attack against the NWO (Dutch Research Council) that led to roughly €4.5 million in damages.

The NWO disclosed the incident on February 14, 2021, saying the attack forced it to shut down its grant application system. Ten days later, the attackers published documents stolen from the council's network on DoppelPaymer's dark web leak site after the NWO refused to pay a ransom demand.

DoppelPaymer ransomware

The DoppelPaymer ransomware operation emerged in June 2019 after the Evil Corp cybercrime gang split, with some members creating a new ransomware gang that shared much of the same code as Evil Corp's BitPaymer.

Besides using stolen files as leverage to force victims into paying ransoms as they did in NWO's case, DoppelPaymer ransomware operators threatened to wipe decryption keys if victims contracted professional negotiators to obtain a better price for recovering the encrypted data.

As the FBI warned in a 2020 private industry alert, "Prior to infecting systems with ransomware, the actors' exfiltrate data to use in extortion schemes and have made follow-on telephone calls to victims to further pressure them to make ransom payments."

DoppelPaymer continued to attack large companies and critical infrastructure organizations through 2022, rebranding twice as Grief (a.k.a. Pay or Grief) and Entropy ransomware.

Law enforcement has targeted two other individuals believed to be core members of the DoppelPaymer ransomware group in March 2023 and issued arrest warrants for three other core members.

The gang's victims list includes high-profile companies and organizations worldwide, such as electronics giant Foxconn, Kia Motors America, Delaware County in Pennsylvania, laptop maker Compal, and Newcastle University.
