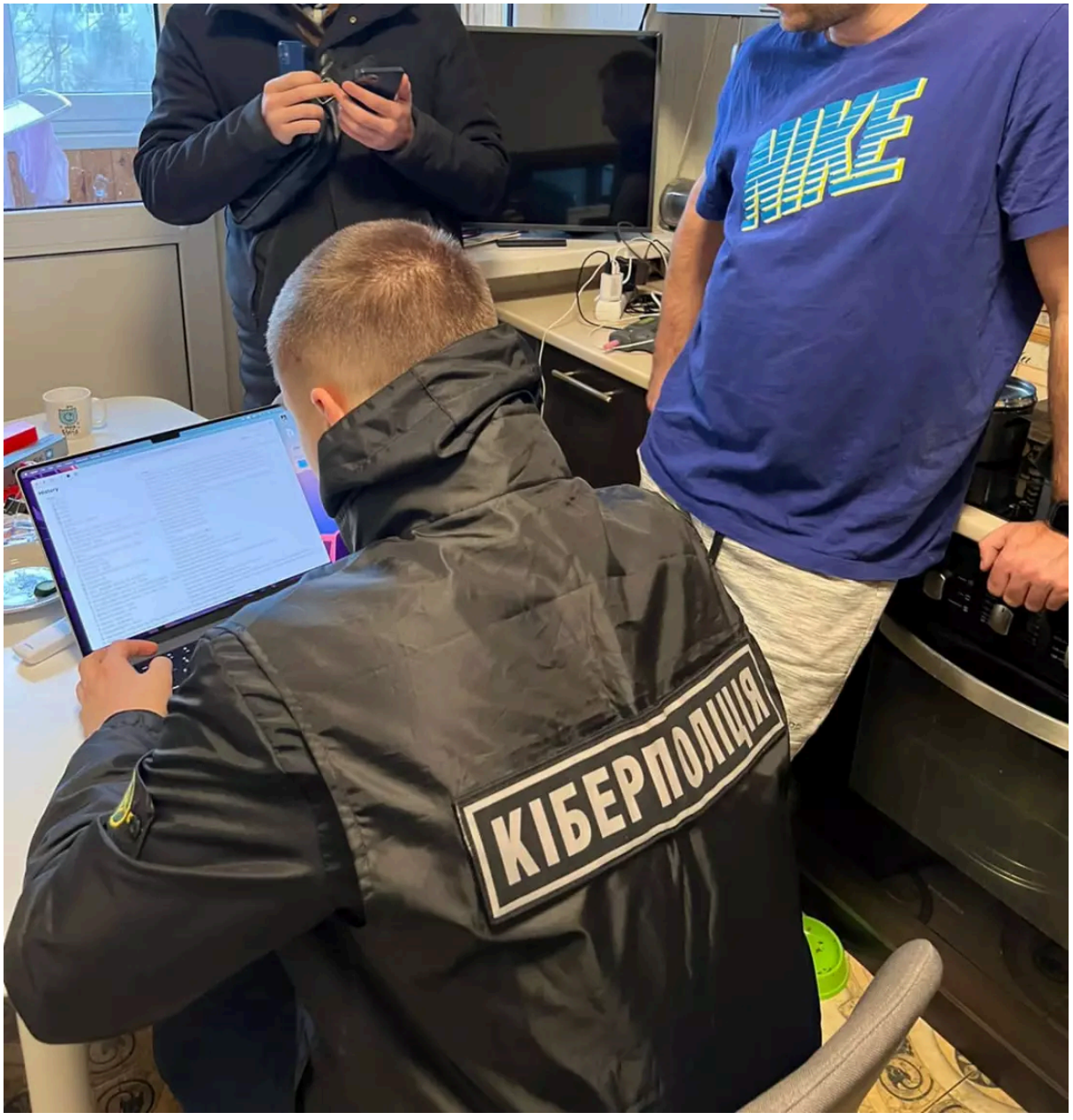
Germany and Ukraine hit two high-value ransomware targets

By Europol

Published: 2023-03-06 · Archived: 2026-04-05 22:27:58 UTC

On 28 February 2023, the German Regional Police (Landeskriminalamt Nordrhein-Westfalen) and the Ukrainian National Police (Націона́льна поліція Украї́ни), with support from Europol, the Dutch Police (Politie) and the United States Federal Bureau of Investigations, targeted suspected core members of the criminal group responsible for carrying out large-scale cyberattacks with the DoppelPaymer ransomware.

- 

- 

This ransomware appeared in 2019, when cybercriminals started using it to launch attacks against organisations and critical infrastructure and industries. Based on the BitPaymer ransomware and part of the Dridex malware family, DoppelPaymer used a unique tool capable of compromising defence mechanisms by terminating the security-related process of the attacked systems. The DoppelPaymer attacks were enabled by the prolific EMOTET malware.

The ransomware was distributed through various channels, including phishing and spam emails with attached documents containing malicious code — either JavaScript or VBScript. The criminal group behind this ransomware relied on a double extortion scheme, using a leak website launched by the criminal actors in early 2020. German authorities are aware of 37 victims of this ransomware group, all of them companies. One of the most serious attacks was perpetrated against the University Hospital in Düsseldorf. In the US, victims payed at least 40 million euros between May 2019 and March 2021.

During the simultaneous actions, German officers raided the house of a German national, who is believed to have played a major role in the DoppelPaymer ransomware group. Investigators are currently analysing the seized equipment to determine the suspect's exact role in the structure of the ransomware group. At the same time, and despite the current extremely difficult security situation that Ukraine is currently facing due to the invasion by Russia, Ukrainian police officers interrogated a Ukrainian national who is also believed to be a member of the core DoppelPaymer group. The Ukrainian officers searched two locations, one in Kiev and one in Kharkiv. During the searches, they seized electronic equipment, which is currently under forensic examination.

Europol on-site to speed up forensic analysis of seized data

On the action days, Europol deployed three experts to Germany to cross-check operational information against Europol's databases and to provide further operational analysis, crypto tracing and forensic support. The analysis of this data and other related cases is expected to trigger further investigative activities. Europol also set up a Virtual Command Post to connect the investigators and experts from Europol, Germany, Ukraine, the Netherlands and the United States in real time and to coordinate activities during the house searches. Europol's Joint Cybercrime Action Taskforce (J-CAT) also supported the operation. This standing operational team consists of cybercrime liaison officers from different countries who work on high-profile cybercrime investigations.

From the beginning of the investigation, Europol facilitated the exchange of information, coordinated the international law enforcement cooperation and supported the operational activities. Europol also provided analytical support by linking available data to various criminal cases within and outside the EU, and supported the investigation with cryptocurrency, malware, decryption and forensic analysis.

Empact

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) tackles the most important threats posed by organised and serious international crime affecting the EU. EMPACT strengthens intelligence, strategic and operational cooperation between national authorities, EU institutions and bodies, and international partners. EMPACT runs in four-year cycles focusing on common EU crime priorities.
