Europol detains suspects behind LockerGoga, MegaCortex, and Dharma ransomware attacks

By Catalin Cimpanu

Published: 2022-12-18 · Archived: 2026-04-05 16:11:28 UTC

Europol said it detained 12 suspects this week it believes were part of a professional criminal group that orchestrated a long string of ransomware attacks that targeted large companies and which hit more than 1,800 victims across 71 countries since 2019.

The suspects were detained on Tuesday, October 26, in Ukraine and Switzerland.

"Most of these suspects are considered high-value targets because they are being investigated in multiple high-profile cases in different jurisdictions," Europol said in a press release today.

"Some of these criminals were dealing with the penetration effort, using multiple mechanisms to compromise IT networks, including brute force attacks, SQL injections, stolen credentials and phishing emails with malicious attachments," the agency said.

Once inside a network, Europol said the group would spend months probing for weaknesses in order to move laterally across the network and expand their access.

The group would often deploy malware such as TrickBot, or post-exploitation frameworks such as Cobalt Strike or PowerShell Empire, to stay undetected and gain further access.

The group appears to have been an affiliate for multiple Ransomware-as-a-Service (RaaS) platforms, having used different ransomware families, such as **LockerGoga**, **MegaCortex**, and **Dharma**.

Europol said that some of this week's arrests also included individuals who helped the group launder ransom payments once a victim had paid.

Group linked to Norsk Hydro attack

According to a press release from Kripos, the criminal investigation division of Norwegian police, the 12 suspects are believed to have orchestrated the ransomware attack on Norwegian aluminum processor Norsk Hydro in March 2019, a ransomware attack that forced the company's factories across two continents to stop production for almost a week.

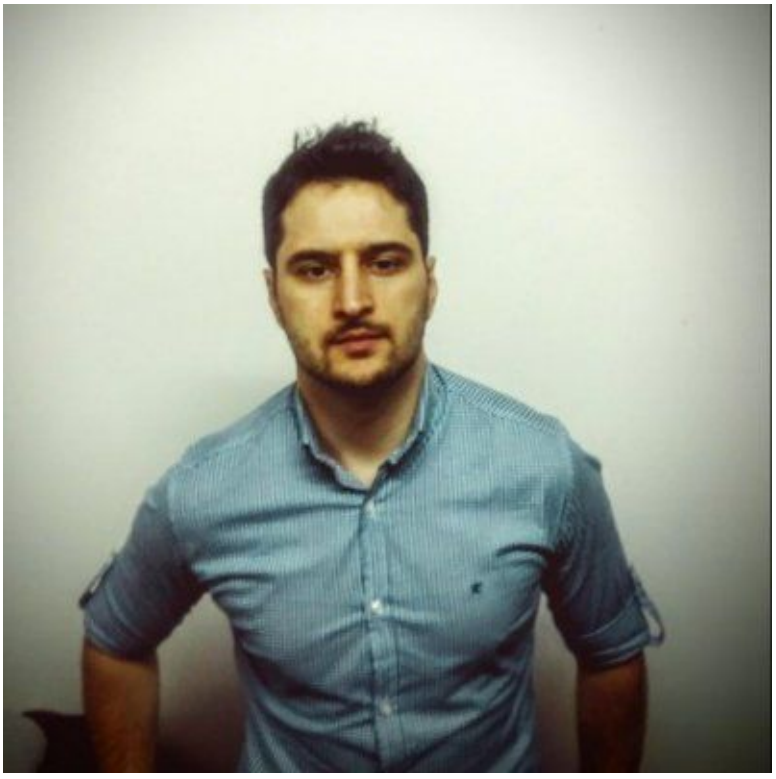
Europol said law enforcement agencies from Norway, France, the UK, Switzerland, Germany, Ukraine, the Netherlands, and the US participated in this week's arrests and investigation.

"More than 50 foreign investigators, including six Europol specialists, were deployed to Ukraine for the action day to assist the National Police with conducting jointly investigative measures. A Ukrainian cyber police officer was also seconded to Europol for two months to prepare for the action day," Europol said.

This week's arrests come after two ransomware operators were also detained in Ukraine three weeks before, at the start of the month, and six suspects who laundered money for the Clop ransomware group were detained in June, also in Ukraine.

No previous article

No new articles



Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
