# 12 targeted for involvement in ransomware attacks against critical infrastructure

By Europol

Published: 2021-10-29 · Archived: 2026-04-05 20:40:15 UTC

A total of 12 individuals wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries.

These attacks are believed to have affected over 1 800 victims in 71 countries. These cyber actors are known for specifically targeting large corporations, effectively bringing their business to a standstill.

The actions took place in the early hours of 26 October 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.

As the result of the action day, over USD 52 000 in cash was seized, alongside 5 luxury vehicles. A number of electronic devices are currently being forensically examined to secure evidence and identify new investigative leads.

## The ticking time bomb of undetected malware

The targeted suspects all had different roles in these professional, highly organised criminal organisations. 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.

Once on the network, some of these cyber actors would focus on moving laterally, deploying malware such as Trickbot, or post-exploitation frameworks such as Cobalt Strike or PowerShell Empire, to stay undetected and gain further access.

The criminals would then lay undetected in the compromised systems, sometimes for months, probing for more weaknesses in the IT networks before moving on to monetising the infection by deploying a ransomware. These cyber actors are known to have deployed LockerGoga, MegaCortex and Dharma ransomware, among others.

The effects of the ransomware attacks were devastating as the criminals had had the time to explore the IT networks undetected. A ransom note was then presented to the victim, which demanded the victim pay the attackers in Bitcoin in exchange for decryption keys.

A number of the individuals interrogated are suspected of being in charge of laundering the ransom payments: they would funnel the Bitcoin ransom payments through mixing services, before cashing out the ill-gotten gains.;

## International cooperation

International cooperation coordinated by Europol and Eurojust was central in identifying these threat actors as the victims were located in different geographical locations around the world.

Initiated by the French authorities, a joint investigation team (JIT) was set up in September 2019 between Norway, France, the United Kingdom and Ukraine with financial support of Eurojust and assistance of both Agencies. The partners in the JIT have since been working closely together, in parallel with the independent investigations of the Dutch and U.S. authorities, to uncover the actual magnitude and complexity of the criminal activities of these cyber actors to establish a joint strategy.

Eurojust established a coordination centre to facilitate cross-border judicial cooperation during the action day. In preparation of this, seven coordination meetings were held.

Europol's European Cybercrime Centre (EC3) hosted operational meetings, provided digital forensic, cryptocurrency and malware support and facilitated the information exchange in the framework of the Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol's headquarters in The Hague.

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.

This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

The following authorities took part in this operation:

- Norway: National Criminal Investigation Service (Kripos)
- France: Public Prosecutor's Office of Paris, National Police (Police Nationale - OCLCTIC)
- Netherlands: National Police (Politie), National Public Prosecution Service (Landelijk Parket, Openbaar Ministerie)
- Ukraine: Prosecutor General's Office (Офіс Генерального прокурора), National Police of Ukraine (Національна поліція України)
- United Kingdom: Police Scotland, National Crime Agency (NCA)
- Germany: Police Headquarters Reutlingen (Polizeipräsidium Reutlingen)
- Switzerland: Federal Police (fedpol), Polizei Basel-Landschaft
- United States: United States Secret Service (USSS), Federal Bureau of Investigations (FBI)
- Europol: European Cybercrime Centre (EC3)
- Eurojust

## 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.

---