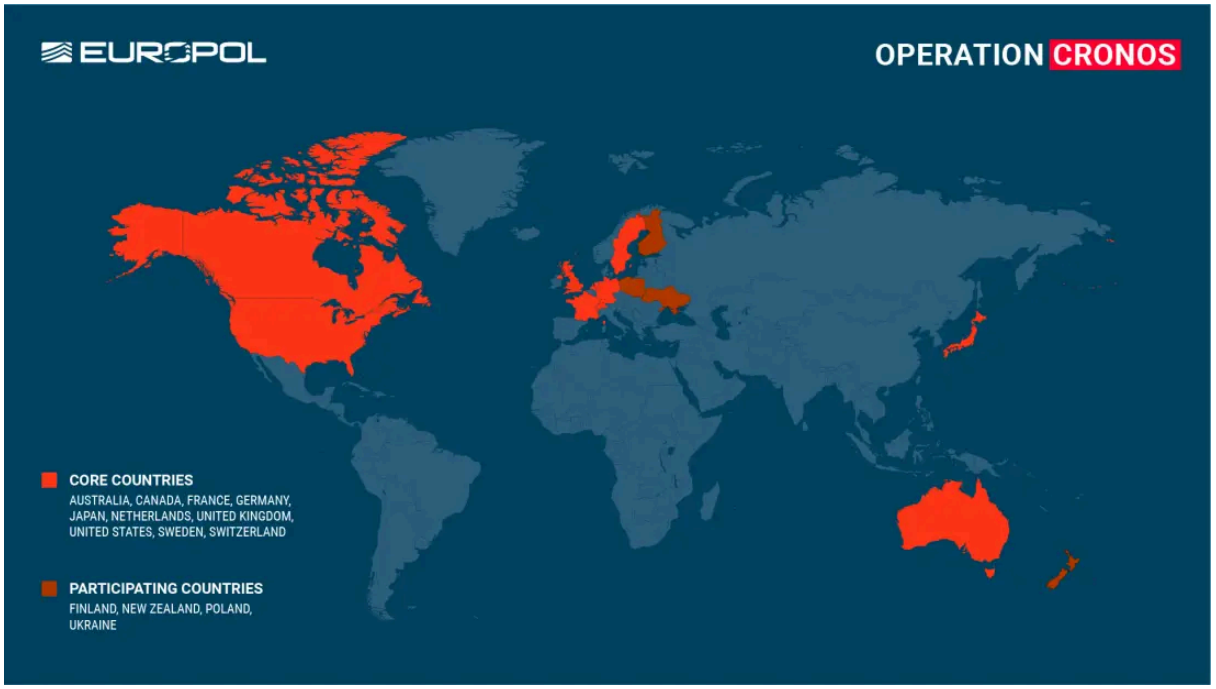
Law enforcement disrupt world's biggest ransomware operation

By Europol

Published: 2024-02-20 · Archived: 2026-04-05 16:17:42 UTC

In a significant breakthrough in the fight against cybercrime, law enforcement from 10 countries have disrupted the criminal operation of the LockBit ransomware group at every level, severely damaging their capability and credibility.

- 

- 

LockBit is widely recognised as the world’s most prolific and harmful ransomware, causing billions of euros worth of damage.

This international sweep follows a complex investigation led by the UK's National Crime Agency in the framework of an international taskforce known as ‘Operation Cronos’, coordinated at European level by Europol and Eurojust.

The months-long operation has resulted in the compromise of LockBit’s primary platform and other critical infrastructure that enabled their criminal enterprise. This includes the takedown of 34 servers in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom.

In addition, two LockBit actors have been arrested in Poland and Ukraine at the request of the French judicial authorities. Three international arrest warrants and five indictments have also been issued by the French and U.S. judicial authorities.

Authorities have frozen more than 200 cryptocurrency accounts linked to the criminal organisation, underscoring the commitment to disrupt the economic incentives driving ransomware attacks.

The UK's National Crime Agency has now taken control of the technical infrastructure that allows all elements of the LockBit service to operate, as well as their leak site on the dark web, on which they previously hosted the data stolen from victims in ransomware attacks.

At present, a vast amount of data gathered throughout the investigation is now in the possession of law enforcement. This data will be used to support ongoing international operational activities focused on targeting the leaders of this group, as well as developers, affiliates, infrastructure and criminal assets linked to these criminal activities.

The world’s most harmful ransomware

LockBit first emerged at the end of 2019, first calling itself ‘ABCD’ ransomware. Since then, it has grown rapidly and in 2022 it became the most deployed ransomware variant across the world.

The group is a ‘ransomware-as-a-service’ operation, meaning that a core team creates its malware and runs its website, while licensing out its code to affiliates who launch attacks.

LockBit’s attack presence is seen globally, with hundreds of affiliates recruited to conduct ransomware operations using LockBit tools and infrastructure. Ransom payments were divided between the LockBit core team and the affiliates, who received on average three-quarters of the ransom payments collected.

The ransomware group is also infamous for experimenting with new methods for pressuring their victims into paying ransoms. Triple extortion is one such method which includes the traditional methods of encrypting the victim's data and threatening to leak it, but also incorporates Distributed Denial-of-Service (DDoS) attacks as an additional layer of pressure.

The gang's move to triple extortion was partly influenced by a DDoS attack they themselves experienced, which impeded their ability to publish stolen data. In response, LockBit enhanced their infrastructure to resist such

attacks.

This infrastructure is now under law enforcement control, and more than 14 000 rogue accounts responsible for exfiltration or infrastructure have been identified and referred for removal by law enforcement.

Europol's coordinating role

With countries involved on either side of the world, Europol – which hosts the world's biggest network of liaison officers from EU Member States – played a central role in coordinating the international activity.

Europol's European Cybercrime Centre (EC3) organised 27 operational meetings, and four technical one-week sprints to develop the investigative leads in preparation of the final phase of the investigation.

Europol also provided analytical, crypto-tracing and forensic support to the investigation, and facilitated the information exchange in the framework of the Joint Cybercrime Action Taskforce (J-CAT) hosted at its headquarters. In addition, three Europol experts were deployed to the command post in London during the action phase.

In total, over 1 000 operational messages have been exchanged on this case via Europol's secure information channel SIENA, making it one of EC3's most active investigations.

The case was opened at Eurojust in April 2022 at the request of the French authorities. Five coordination meetings were hosted by the Agency to facilitate judicial cooperation and to prepare for the joint action.

Decryption tools available on No More Ransom

With Europol's support, the Japanese Police, the National Crime Agency and the Federal Bureau of Investigation have concentrated their technical expertise to develop decryption tools designed to recover files encrypted by the LockBit Ransomware.

These solutions have been made available for free on the 'No More Ransom' portal, available in 37 languages. So far, more than 6 million victims across the globe have benefitted from No More Ransom which contains over 120 solutions capable of decrypting more than 150 different types of ransomware.

Report it to the police

This investigation shows that law enforcement has the capabilities to disrupt high harm cybercriminals and reduce the ransomware threat. However, continued victim and private sector engagement is key to us continuing this work.

The first step to putting cybercriminals behind bars is to report cybercrime when it happens. The earlier people report, the quicker law enforcement is able to assess new methodologies and limit the damage they can cause.

Reporting cybercrime can be as simple as clicking a button on a web browser. Europol has compiled a list of the reporting websites in EU Member States.

Robust cybersecurity measures are also key. Europol has put together some tips and advice on how to prevent ransomware from infecting your electronic devices.

Taskforce Operation Cronos

This activity forms part of an ongoing, concerted campaign by the international Operation Cronos taskforce to target and disrupt LockBit ransomware. The following authorities are part of this taskforce:

- **France:** National Gendarmerie (Gendarmerie Nationale – Unité nationale cyber C3N)
- **Germany:** State Bureau of Criminal Investigation Schleswig-Holstein(LKA Schleswig-Holstein), Federal Criminal Police Office (Bundeskriminalamt)
- **The Netherlands:** National Police (Team Cybercrime Zeeland-West-Brabant, Team Cybercrime Oost-Brabant, Team High Tech Crime) & Public Prosecutor's Office Zeeland-West-Brabant
- **Sweden:** Swedish Police Authority
- **Australia:** Australian Federal Police (AFP)
- **Canada:** Royal Canadian Mounted Police (RCMP)
- **Japan:** National Police Agency (警察庁)
- **United Kingdom:** National Crime Agency (NCA), South West Regional Organised Crime Unit (South West ROCU)
- **United States:** U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI) Newark
- **Switzerland:** Swiss Federal Office of Police (fedpol), Public Prosecutor's Office of the canton of Zurich, Zurich Cantonal Police

The successful action was made possible thanks to the support of the following countries:

- **Finland:** National Police (Poliisi)
- **Poland:** Central Cybercrime Bureau Cracow (Centralne Biuro Zwalczania Cyberprzestępczości - Zarząd w Krakowie)
- **New Zealand:** New Zealand Police (Nga Pirihimana O Aotearoa)
- **Ukraine:** Prosecutor General`s office of Ukraine (Офіс Генерального прокурора України), Cybersecurity Department of the Security Service of Ukraine (Служба безпеки України), National Police of Ukraine (Національна поліція України)

Source: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation