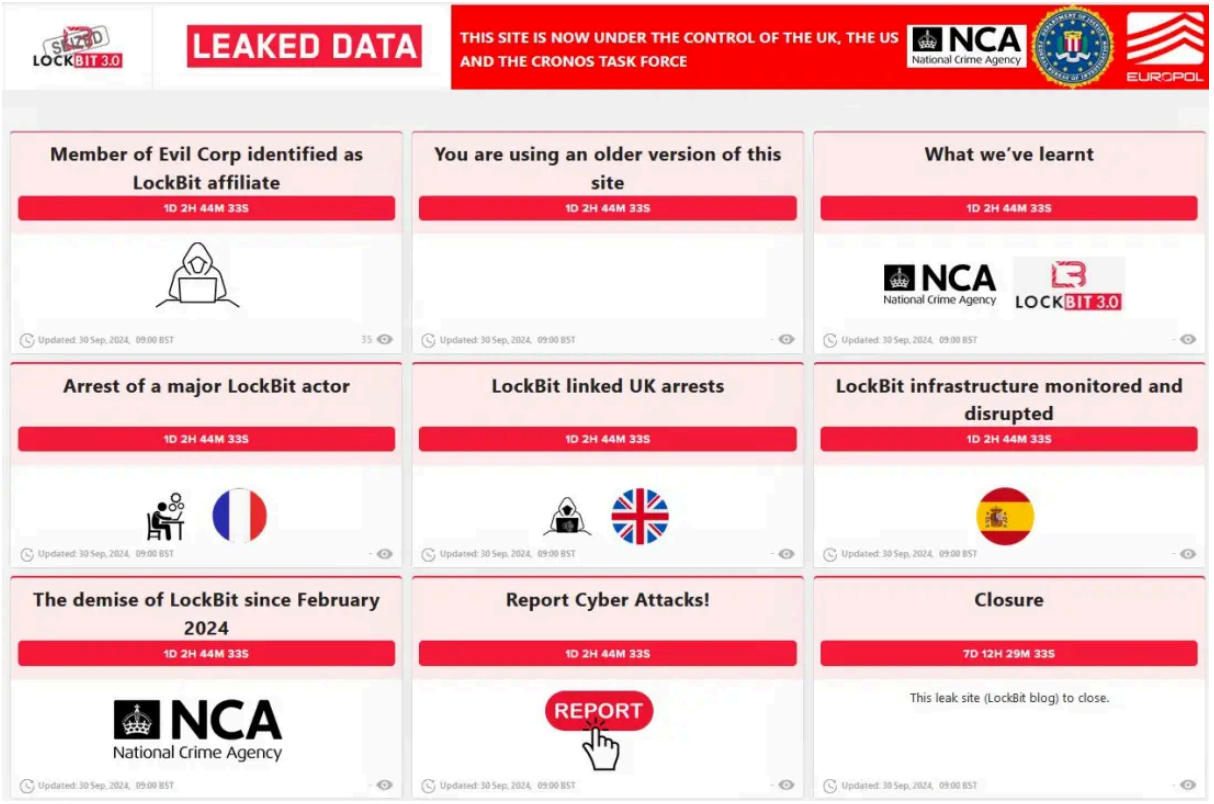
LockBit power cut: four new arrests and financial sanctions against affiliates

By Europol

Published: 2024-10-01 · Archived: 2026-04-05 21:55:18 UTC

Europol supported a new series of actions against LockBit actors, which involved 12 countries and Eurojust and led to four arrests and seizures of servers critical for LockBit's infrastructure. A suspected developer of LockBit was arrested at the request of the French authorities, while the British authorities arrested two individuals for supporting the activity of a LockBit affiliate. The Spanish officers seized nine servers, part of the ransomware's infrastructure, and arrested an administrator of a Bulletproof hosting service used by the ransomware group. In addition, Australia, the United Kingdom and the United States implemented sanctions against an actor who the National Crime Agency had identified as prolific affiliate of LockBit and strongly linked to Evil Corp. The latter comes after LockBit's claim that the two ransomware groups do not work together. The United Kingdom sanctioned fifteen other Russian citizens for their involvement in Evil Corp's criminal activities, while the United States also sanctioned six citizens and Australia sanctioned two.

- 

LockBit full infrastructure in the crosshairs of law enforcement

These are some of the results of the third phase of Operation Cronos, a long-running collective effort of law enforcement authorities from 12 countries, Europol and Eurojust, who joined forces to effectively disrupt at all

levels the criminal operations of the LockBit ransomware group. These actions follow the massive disruption of LockBit infrastructure in February 2024, as well as the large series of sanctions and operational actions that took place against LockBit administrators in May and subsequent months.

Between 2021 and 2023, LockBit was the most widely employed ransomware variant globally with a notable number of victims claimed on its data leak site. Lockbit operated on the ransom as a service model. The core group sold access to affiliates and received portions of the collected ransom payments. Entities deploying LockBit ransomware attacks had targeted organisations of various sizes spanning critical infrastructure sectors such as financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing and transportation. Reflecting the considerable number of independent affiliates involved, LockBit ransomware attacks display significant variation in observed tactics, techniques and procedures.

No More Ransom to decrypt your files

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

The support from the cybersecurity sector has also proven crucial for minimising the damage from ransomware attacks, which remains the biggest cybercrime threat. Many partners have already provided decryption tools for a number of ransomware families via the 'No More Ransom' website.

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 around the globe have benefitted from No More Ransom, which contains over 120 solutions capable of decrypting more than 150 different types of ransomware.

Europol's support

Europol facilitated the information exchange, supported the coordination of the operational activities and provided operational analytical support, as well as crypto tracing and forensic support. The analysis workflow proposed after the first operation enabled a joint work focused on the identification of the LockBit actors. The advanced demixing capabilities of Europol's Cybercrime Centre enabled the identification of several targets. Following the initiation operations against LockBit's infrastructure in the beginning of 2024, Europol organised seven technical sprints, three of which were fully dedicated to cryptocurrency tracing. During the action days, Europol deployed an expert to provide on-the-spot support to the national authorities.

The Joint Cybercrime Action Taskforce (J-CAT) at Europol supported the operation. This standing operational team consists of cyber liaison officers from different countries who work from the same office on high-profile cybercrime investigations.

Authorities participating in Operation Cronos

- Australia: Australian Federal Police
- Canada: Royal Canadian Mounted Police/ Gendarmerie royale du Canada

- France: Gendarmerie - (Gendarmerie Nationale – Unité nationale cyber C3N); Court of Paris JUNALCO (National Jurisdiction against Organised Crime) Cybercrime Unit
- Germany: State Bureau of Criminal Investigation (Landeskriminalamt Kiel) and Federal Criminal Police Office (Bundeskriminalamt)
- Japan: National Police Agency of Japan (警察庁)
- Spain: Spanish Civil Guard (Guardia Civil)
- Sweden: Swedish Police Authority
- Switzerland: Switzerland Fedpol – Zurich State Police
- Netherlands: National Police (Politie) Dienst Regionale Recherche Oost-Brabant
- Romania: National Police Central Cybercrime Unit
- United Kingdom: National Crime Agency, South West Regional Organised Crime Unit (South West ROCU)
- United States: Federal Bureau of Investigation Newark

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.
