

LockBit Ransomware Disrupted

Cornelia Riehle



euclid

European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle

Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(1) euclid

ISSN: 1862-6947

<https://euclid.eu>

After a month-long operation, law enforcement officers from 10 countries, together with agents from Europol and Eurojust, compromised and took control of LockBit's primary platform and other crucial infrastructure belonging to the cybercriminal group's ransomware operation. The work of the international taskforce "Operation Cronos" significantly compromised the criminal group by the end of February 2024: more than 200 cryptocurrency accounts were frozen, 34 servers taken down, 14,000 rogue accounts closed, and two persons arrested.

LockBit emerged at the end of 2019 using the name "ABCD" ransomware. Over the past three years, this ransomware became the most frequently deployed ransomware variant worldwide. The criminal operation offered 'ransomware-as-a-service', with a core team creating its malware and running the website. It also licensed out its code to affiliates, who launch attacks causing billions of euros worth of damage.

By means of "Operation Cronos", law enforcement officials managed to develop decryption tools designed to recover files encrypted by the LockBit ransomware. These solutions are available for free in 37 languages on the 'No More Ransom' portal.



About euclid

euclid is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.

All news items are freely accessible at: <https://euclid.eu/news/>

Stay informed by emailing to euclid-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).



**Co-funded by
the European Union**