

# Operation ENDGAME Targets Initial Access Malware



**euclid**

European Law Forum: Prevention • Investigation • Prosecution

**Cornelia Riehle**

## News

At the end of May 2025, Operation ENDGAME, ongoing since 2024, led to the takedown of Initial Access Malware. This malware was being used for initial infection, helping cybercriminals to enter victims' systems unnoticed and download more malware, such as ransomware, onto their devices. The following malware strains were neutralised during the operation: Bumblebee, Lactrodectus, Qakbot, Hijackloader, DanaBot, Trickbot, and Warmcookie.

Investigators from Canada, Denmark, France, Germany, the Netherlands, the United Kingdom, and the United States conducted the operation, which was also supported by Eurojust and Europol. Some 300 servers were taken down worldwide, 650 domains were neutralised, and 20 international arrest warrants issued. €3.5 million in cryptocurrency was also seized. In addition, several suspects were added to the [EU Most Wanted list](#).

### AUTHOR

**Cornelia Riehle**

Deputy Head of Section  
Academy of European Law

Published in  
2025, Vol. 20(2) euclid

ISSN: 1862-6947

<https://euclid.eu>



## 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](mailto: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**