Operation Endgame Takes Down Droppers

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

Between 27 and 29 May 2024, with the support of Europol and Eurojust, authorities from France, Germany, the Netherlands, and many more EU and non-EU States as well as private partners conducted the largest ever operation against botnets: Operation Endgame. The action included arrests, suspect interviews, searches, seizures, and takedowns of servers and domains. As a result, four persons were arrested, over 100 servers taken down worldwide, and droppers such as IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee were shut down. Several cybercriminals were added on "Europe's Most Wanted" list.

Malware droppers are a type of malicious software designed to install other malware onto a target system. Droppers constitute the first step in an infection chain entering systems through various channels, such as email attachments, compromised websites, or bundled with legitimate software. The dropper subsequently installs the malware onto the victim's computer. The dropper itself is designed to avoid being detected by security software. Having "dropped" the malware, the dropper will either remain inactive or remove itself to evade detection, leaving the payload to carry out the intended malicious activities.

A dedicated website will continue reporting about the results and further actions of Operation Endgame.

The operation was part of the EMPACT cycle - the European permanent platform to identify, prioritise, and address threats posed by organised and serious international crime (→ eucrim 1/2022, 35)

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-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