Operation Endgame follow-up leads to five detentions and interrogations as well as server takedowns

By Europol

Published: 2025-04-09 · Archived: 2026-04-05 18:56:13 UTC

Following the massive botnet takedown codenamed Operation Endgame in May 2024, which shut down the biggest malware droppers, including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee, law enforcement agencies across North America and Europe dealt another blow to the malware ecosystem in early 2025.

In a coordinated series of actions, customers of the Smokeloader pay-per-install botnet, operated by the actor known as ‘Superstar’, faced consequences such as arrests, house searches, arrest warrants or ‘knock and talks’. Superstar used his botnet to run a pay-per-install service, enabling customers to gain access to victims’ machines. Customers used the service to deploy malware for their own criminal activities. Investigations revealed that botnet access was purchased for a range of purposes, including keylogging, webcam access, ransomware deployment, cryptomining and more. Law enforcement tracked down the customers as they were registered in a database seized during Operation Endgame.

While the actions in May 2024 targeted high-level actors who facilitated cybercrime, by deploying ransomware, for example, this follow-up operation targets a different level. Law enforcement moved – and continues to move – against the criminals who used the services taken down during Operation Endgame, focusing on the demand side of the criminal ecosystem. Customers of crime-as-a-service providers are now learning the painful lesson that their personal data was not protected by these individuals who involuntarily painted targets on their backs.

Law enforcement agencies in all the involved countries have closely followed the leads uncovered during Operation Endgame, helping them to link online personas and their usernames to real-life individuals. When called in for questioning, several suspects chose to cooperate with the authorities by facilitating the examination of digital evidence stored on their personal devices. Several suspects resold the services purchased from Smokeloader at a markup, thus adding an additional layer of interest to the investigation.

…and a dedicated website for those who want to get in touch

Some of the suspects had assumed they were no longer on law enforcement's radar, only to come to the harsh realisation that they were still being targeted. Operation Endgame does not end today. New actions will be announced on the website operation-endgame.com. Anyone with information is invited to contact the authorities through this website. In addition, suspects involved in these and other botnets, who have not yet been arrested, will be held directly accountable for their actions.

Europol and the Joint Cybercrime Action Taskforce (J-CAT), hosted by Europol, continue to support the investigation of Operation Endgame. It has facilitated the information exchange between the authorities involved and provided analytical and forensic support to the investigators. To support the coordination of the operation, Europol organised coordination calls and operational sprints at its headquarters in The Hague.

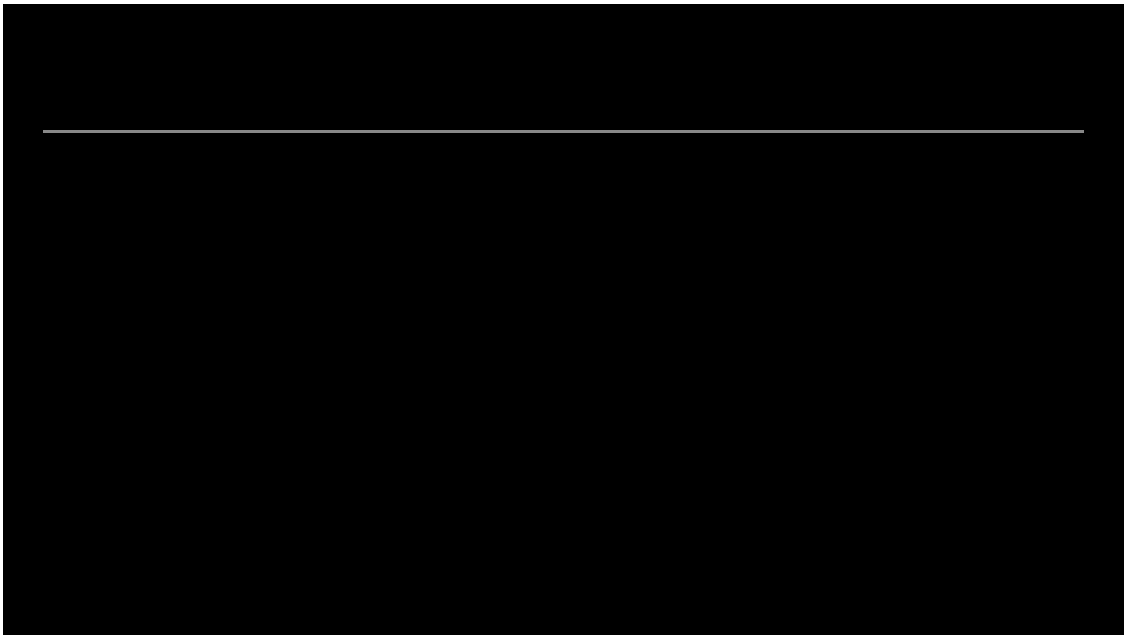
Participating authorities:

- Canada: Royal Canadian Mounted Police (RCMP)
- Czech Republic: Police of the Czech Republic (Policie České republiky)
- Denmark: Danish Police (Dansk Politi)
- France: National Police (OFAC) (Police Nationale - Office Anti-Cybercriminalité)
- Germany: Federal Criminal Police Office (Bundeskriminalamt); Prosecutor General's Office Frankfurt am Main – Cyber Crime Center (Generalstaatsanwaltschaft Frankfurt am Main – ZIT)
- Netherlands: National Investigations and Special Operations (NIS), Netherlands Police (Politie)
- United States of America: Federal Bureau of Investigation (FBI); United States Secret Service; United States Department of Defense - Defense Criminal Investigative Service (DCIS)

Participating agencies:

- Eurojust

Operation Endgame - think about (y)our next move:



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.

Source: https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-follow-leads-to-five-detentions-and-interrogations-well-server-takedowns