Largest ever operation against botnets hits dropper malware ecosystem

By Europol

Published: 2024-05-30 · Archived: 2026-04-02 10:51:51 UTC

Between 27 and 29 May 2024 Operation Endgame, coordinated from Europol's headquarters, targeted droppers including, IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot. The actions focused on disrupting criminal services through arresting High Value Targets, taking down the criminal infrastructures and freezing illegal proceeds. This approach had a global impact on the dropper ecosystem. The malware, whose infrastructure was taken down during the action days, facilitated attacks with ransomware and other malicious software. Following the action days, eight fugitives linked to these criminal activities, wanted by Germany, will be added to Europe's Most Wanted list on 30 May 2024. The individuals are wanted for their involvement in serious cybercrime activities.

This is the largest ever operation against botnets, which play a major role in the deployment of ransomware. The operation, initiated and led by France, Germany and the Netherlands was also supported by Eurojust and involved Denmark, the United Kingdom and the United States. In addition, Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland and Ukraine also supported the operation with different actions, such as arrests, interviewing suspects, searches, and seizures or takedowns of servers and domains. The operation was also supported by a number of private partners at national and international level including Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, HaveIBeenPwned, Spamhaus, DIVD, abuse.ch and Zscaler.

The coordinated actions led to:

- 4 arrests (1 in Armenia and 3 in Ukraine)
- 16 location searches (1 in Armenia, 1 in the Netherlands, 3 in Portugal and 11 in Ukraine)
- Over 100 servers taken down or disrupted in Bulgaria, Canada, Germany, Lithuania, the Netherlands, Romania, Switzerland, the United Kingdom, the United States and Ukraine
- Over 2 000 domains under the control of law enforcement

Furthermore, it has been discovered through the investigations so far that one of the main suspects has earned at least EUR 69 million in cryptocurrency by renting out criminal infrastructure sites to deploy ransomware. The suspect's transactions are constantly being monitored and legal permission to seize these assets upon future actions has already been obtained.

What is a dropper and how does it work?

Malware droppers are a type of malicious software designed to install other malware onto a target system. They are used during the first stage of a malware attack, during which they allow criminals to bypass security measures and deploy additional harmful programs, such as viruses, ransomware, or spyware. Droppers themselves do not

usually cause direct damage but are crucial for accessing and implementing harmful softwares on the affected systems.

SystemBC facilitated anonymous communication between an infected system and a command-and-control servers. Bumblebee, distributed mainly via phishing campaigns or compromised websites, was designed to enable the delivery and execution of further payloads on compromised systems. SmokeLoader was primarily used as a downloader to install additional malicious softwares onto the systems it infects. IcedID (also known as BokBot), initially categorised as a banking trojan, had been further developed to serve other cybercrimes in addition to the theft of financial data. Pikabot is a trojan used to get initial access to infected computers which enables ransomware deployments, remote computer take-over and data theft. All of them are now being used to deploy ransomware and are seen as the main threat in the infection chain.

Droppers' operation phases

Infiltration: Droppers can enter systems through various channels, such as email attachments, compromised websites, they can also be bundled with legitimate software.

Execution: Once executed, the dropper installs the additional malware onto the victim's computer. This installation often occurs without the user's knowledge or consent.

Evasion: Droppers are designed to avoid detection by security software. They may use methods like obfuscating their code, running in memory without saving to disk, or impersonating legitimate software processes.

Payload Delivery: After deploying the additional malware, the dropper may either remain inactive or remove itself to evade detection, leaving the payload to carry out the intended malicious activities.

Endgame doesn't end here

Operation Endgame does not end today. New actions will be announced on the website Operation Endgame. In addition, suspects involved in these and other botnets, who have not yet been arrested, will be directly called to account for their actions. Suspects and witnesses will find information on how to reach out via this website.

Command post at Europol to coordinate the operational actions

Europol facilitated the information exchange and provided analytical, crypto-tracing and forensic support to the investigation. To support the coordination of the operation, Europol organised more than 50 coordination calls with all the countries as well as an operational sprint at its headquarters.

Over 20 law enforcement officers from Denmark, France, Germany and the United States supported the coordination of the operational actions from the command post at Europol and hundreds of other officers from the different countries involved in the actions. In addition, a virtual command post allowed real-time coordination between the Armenian, French, Portuguese and Ukrainian officers deployed on the spot during the field activities.

The command post at Europol facilitated the exchange of intelligence on seized servers, suspects and the transfer of seized data. Local command posts were also set up in Germany, the Netherlands, Portugal, the United States and Ukraine. Eurojust supported the action by setting up a coordination centre at its headquarters to facilitate the

judicial cooperation between all authorities involved. Eurojust also assisted with the execution of European Arrest Warrants and European Investigation Orders.

National authorities at the core of Operation Endgame

EU Member States:

- **Denmark:** Danish Police (Politi)
- **France:** National Gendarmerie (Gendarmerie Nationale) and National Police (Police Nationale); Public Prosecutor Office JUNALCO (National Jurisdiction against Organised Crime) Cybercrime Unit; Paris Judicial Police (Préfecture De Police de Paris)
- **Germany:** Federal Criminal Police Office (Bundeskriminalamt), Prosecutor General's Office Frankfurt am Main – Cyber Crime Center
- **Netherlands:** National Police (Politie), Public Prosecution Office (Openbaar Ministerie)

Non-EU Member States:

- **The United Kingdom:** National Crime Agency
- **The United States:** Federal Bureau of Investigation, United States Secret Service, The Defense Criminal Investigative Service, United States Department of Justice

Authorities involved in local coordination centres for Operation Endgame:

- **Portugal:** Judicial Police (Polícia Judiciária)
- **Ukraine:** Prosecutor General’s Office (Офіс Генерального прокурора); National Police (Національна поліція України); Security Service (Служба безпеки України)

The list of participating authorities was updated on 30 May 2024 at 12:10 CET.

The list of private partners was updated on 30 May 2024 at 17:00 CET.

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.
