Four arrested in international anti-malware sweep

May 30 2024, by Julie Capelle in The Hague and Tiphaine Le Liboux in Paris

The May 27-29 Operation Endgame led to one arrest in Armenia and three in Ukraine.

Authorities arrested four people and took down or disrupted more than 100 servers in the "largest ever" operation against botnets that deploy

ransomware, Europol said Thursday.

Dubbed Operation Endgame, the sweep was initiated and led by France, Germany and the Netherlands, with a French official saying they wanted to act before this summer's Paris Olympics.

The attacks cost the victims, which were mainly companies and national institutions, hundreds of millions of euros, according to Dutch police, adding that the systems of millions of individuals were infected.

The May 27-29 operation led to one arrest in Armenia and three in Ukraine, with searches in both countries as well as in the Netherlands and Portugal, Europol said.

The servers were located in Bulgaria, Canada, Germany, Lithuania, the Netherlands, Romania, Switzerland, Britain, the United States and Ukraine.

In addition to the four arrests, eight fugitive suspects linked to the case will be added to Europe's Most Wanted list.

One of the suspects earned at least 69 million euros ($75 million) in cryptocurrency by renting out criminal infrastructure sites to disseminate ransomware, Europol said.

"This is the largest ever operation against botnets, which play a major role in the deployment of ransomware," the agency based in The Hague said.

A botnet is a network of computers infected by malware and controlled by hackers.

Authorities targeted malware "droppers"—a type of software used to

insert malicious software into a system—named IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot.

Trickbot was used to launch ransomware attacks on US hospitals during the COVID pandemic.

Pre-Olympics sting

The operation had "a global impact on the dropper ecosystem", Europol said.

Droppers allow criminals to bypass security measures and deploy viruses, ransomware or spyware, the agency said.

The malicious software is generally installed via emails with infected links or Word and PDF attachments, according to Eurojust, the European Union Agency for Criminal Justice Cooperation.

The agency said the operation was ongoing, with more arrests expected.

"We wanted to do this operation before the Olympic Games," Nicolas Guidoux, head of the French police's cybercrime unit, told AFP.

He said it was "important to weaken the attacking infrastructure" and "limit their resources" before the global event, as authorities fear that it could be targeted by numerous cyberattacks.

Endgame also involved authorities from Denmark, Britain and the United States, with additional support from Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland and Ukraine.

SystemBC and Pikabot

The investigation was launched in 2022.

German cybercrime prosecutor Benjamin Krause said health, education and public administration institutions were targeted.

Hackers would encrypt files or whole systems to block access to them and then demand money to unlock them, Krause said at a news conference, adding that such attacks threatened "the existence of companies".

French investigators identified the administrator of the SystemBC dropper, which Europol said "facilitated anonymous communication between an infected system" and "command-and-control servers".

The administrator of Pikabot—a Trojan horse allowing the deployment of ransomware, the remote takeover of computers and data theft—was also identified by French authorities.

French police participated in the suspect's arrest and house search in Ukraine, with authorization from local authorities, said Paris prosecutor Laure Beccuau.

Guidoux said the number of victims will be known only after the dismantled servers are analyzed.

Cybersecurity experts said Operation Endgame helped to destabilize a criminal ecosystem that is difficult to crack.

"The dropper network is a piece of infrastructure that makes life easier for many cybercriminal groups," said Jerome Saiz, founder of cybersecurity firm OPFOR Intelligence.