Ragnar Locker ransomware developer arrested in France

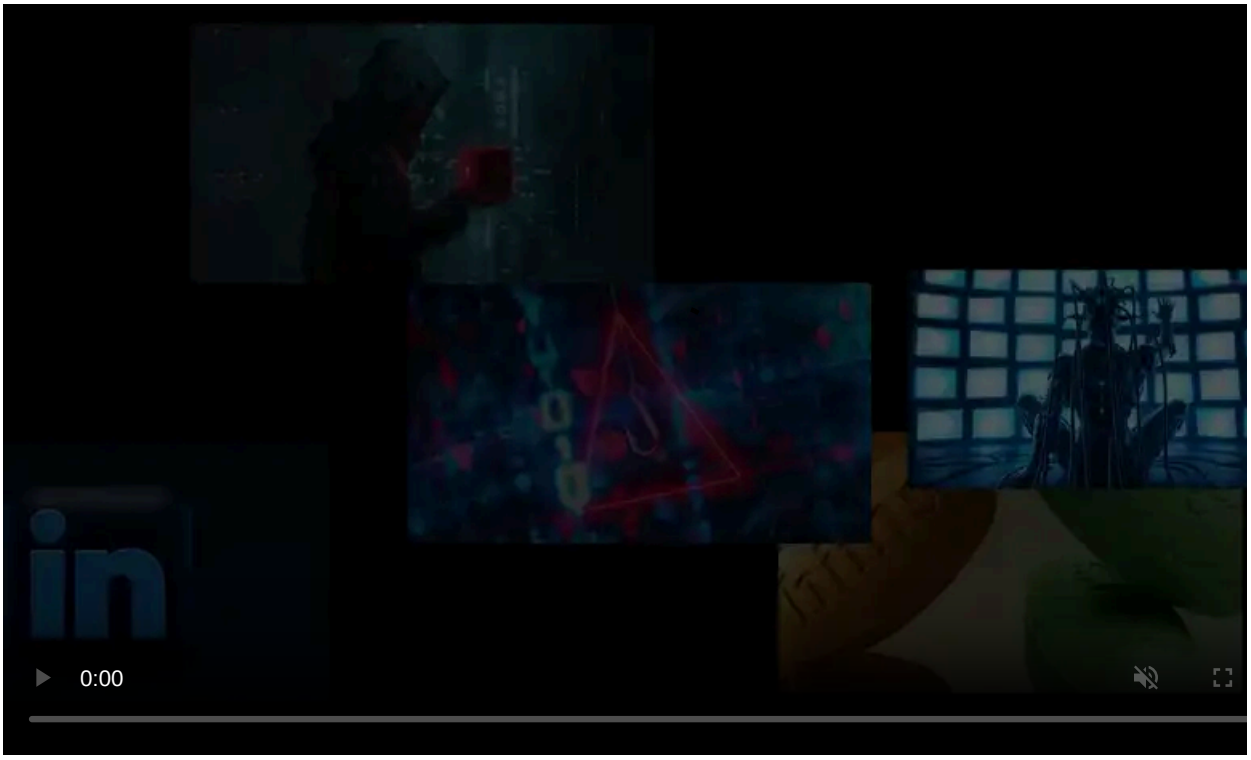
By Sergiu Gatlan

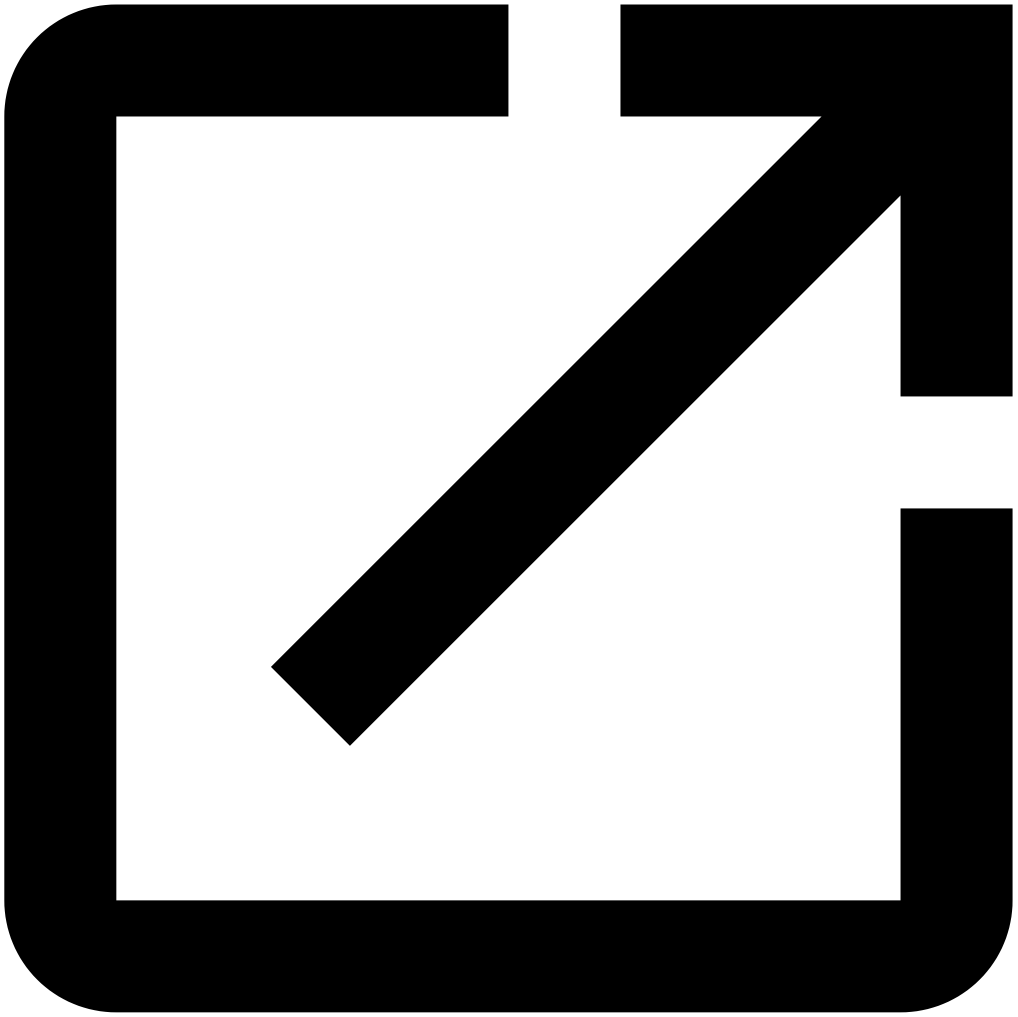
Published: 2023-10-20 · Archived: 2026-04-05 18:48:37 UTC

Law enforcement agencies arrested a malware developer linked with the Ragnar Locker ransomware gang and seized the group's dark web sites in a joint international operation.

The Ragnar Locker ransomware gang is believed to have carried out attacks against 168 international companies globally since 2020.

"The 'key target' of this malicious ransomware strain was arrested in Paris, France, on 16 October, and his home in Czechia was searched. Five suspects were interviewed in Spain and Latvia in the following days," Europol said today.


0:00



"At the end of the action week, the main perpetrator, suspected of being a developer of the Ragnar group, has been brought in front of the examining magistrates of the Paris Judicial Court."

Ukrainian police also raided the premises of another suspected gang member in Kyiv, seizing laptops, mobile phones, and electronic devices.

Eurojust opened the case in May 2021 at the French authorities' request. The agency conducted five coordination meetings to facilitate judicial collaboration among authorities involved in the investigation.

This joint operation between authorities from France, the Czech Republic, Germany, Italy, Latvia, the Netherlands, Spain, Sweden, Japan, Canada, and the United States marks the third action against the same ransomware gang.

In September 2021, coordinated efforts involving French, Ukrainian, and US authorities led to the arrest of two suspects in Ukraine.

Subsequently, in October 2022, another suspect was apprehended in Canada through a joint operation conducted by French, Canadian, and US law enforcement agencies.

During the coordinated operation, law enforcement agents also seized cryptocurrency assets and took down the Ragnar Locker's Tor negotiation and data leak sites on Thursday.

"Furthermore, nine servers were taken down; five in the Netherlands, two in Germany and two in Sweden," Europol said.

"This service has been seized as part of a coordinated law enforcement action against the Ragnar Locker group," a banner displayed on Ragnar Locker's data leak site reads.

Ragnar Locker seizure banner (BleepingComputer)

Alongside the successful seizure of Ragnar Locker's infrastructure, the Ukrainian Cyber Alliance (UCA) hacked the Trigona Ransomware operation, successfully retrieving data and wiping the cybercriminals' servers.

The Ragnar Locker (also known as Ragnar_Locker and RagnarLocker) ransomware operation surfaced in late December 2019 when it started targeting enterprise victims worldwide.

In contrast to many modern ransomware gangs, Ragnar Locker did not operate as a Ransomware-as-a-Service, where affiliates are recruited to breach targets' networks and deploy the ransomware in exchange for a share of the revenue.

Instead, Ragnar Locker operated semi-private, as they didn't actively recruit affiliates, choosing to collaborate with external penetration testers to breach networks.

Its list of previous victims includes prominent entities such as computer chip manufacturer ADATA, aviation giant Dassault Falcon, and Japanese game maker Capcom.

According to a March 2022 FBI advisory, this ransomware has been deployed on the networks of at least 52 organizations across various critical infrastructure sectors in the United States since April 2020.

Source: https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-developer-arrested-in-france/