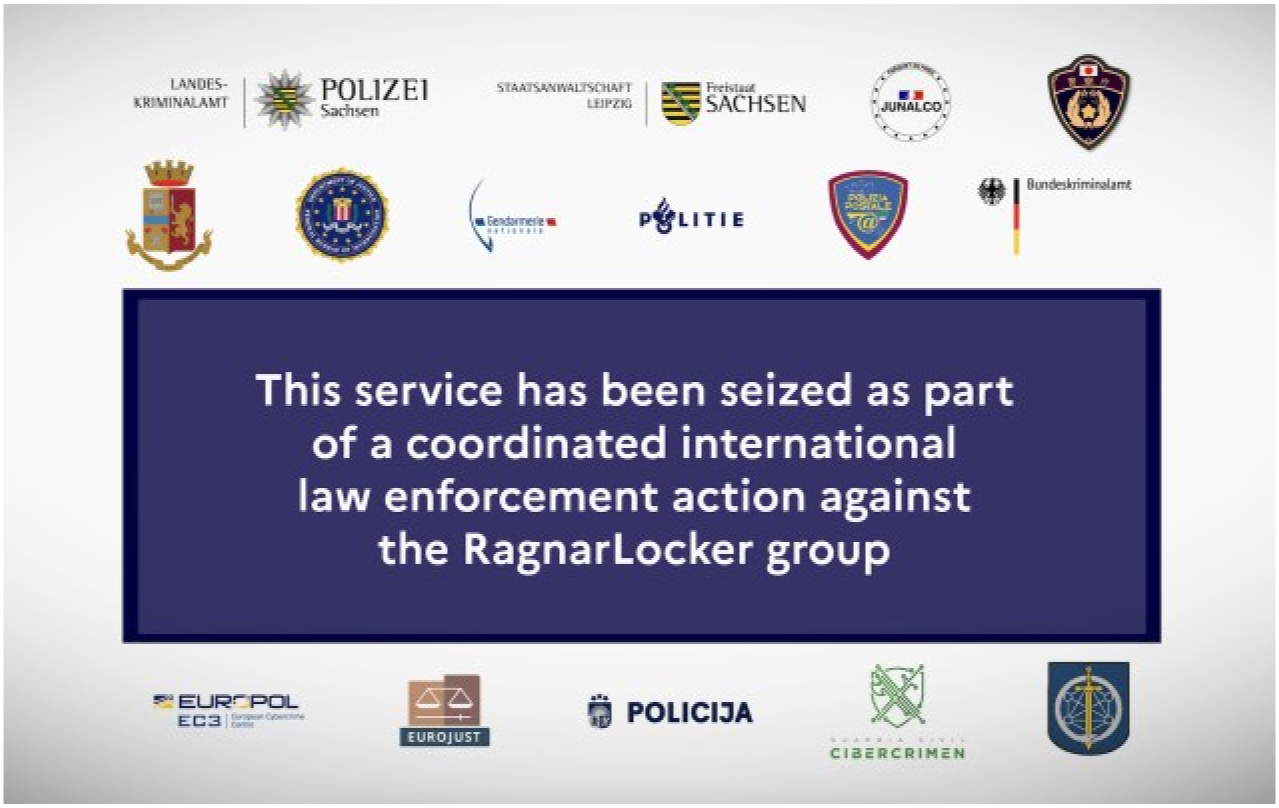
Authorities confirm RagnarLocker ransomware taken down during international sting

techcrunch.com/2023/10/20/ragnarlocker-ransomware-dark-web-portal-seized-in-international-sting/

October 20, 2023

Carly Page 6 months



This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group

An international group of law enforcement agencies have disrupted the notorious RagnarLocker ransomware operation.

TechCrunch reported Thursday that an international law enforcement operation involving agencies from the U.S., European Union and Japan had seized the RagnarLocker group’s dark web portal. The portal, which the gang used to extort its victims by publishing their stolen data, now reads: “This service has been seized by a part of a coordinated international law enforcement action against the RagnarLocker group.”

Announcing the takedown on Friday, Europol confirmed it took coordinated action against RagnarLocker, which it says was responsible for “numerous high-profile attacks.” The European police agency also confirmed the arrest of a 35-year-old man in Paris on October 16, who the authorities accuse of being the “main perpetrator” of the operation. Authorities searched the alleged RagnarLocker developer’s home in the Czech Republic. Alleged associates of the developer were also interviewed in Spain and Latvia.

RagnarLocker's infrastructure was also seized in the Netherlands, Germany and Sweden. According to Eurojust, the EU agency that coordinates criminal justice cooperation across the bloc, a total of nine servers were seized: five in the Netherlands, two in Germany and two in Sweden. Eurojust also reports that it seized various cryptocurrencies, though their value is currently unknown.

Ukrainian authorities, who were part of the 11-country operation, said in a separate announcement on Friday that its officers searched the premises of another RagnarLocker suspect near Kiev, and recovered laptops, mobile phones and other electronic media.

In a press release, Italy's Polizia di Stato (State Police) confirmed its involvement in the coordinated international effort, which it called "Operation Mole." The Italian law enforcement agency also published a video that shows footage from a raid conducted by French, Italian and Czech police agents, presumably in the house of the 35-year-old man they had arrested.

RagnarLocker is both the name of a ransomware strain and the criminal group that develops and operates it. The gang, which some security experts have linked to Russia, has been observed targeting victims since 2020, and has predominantly attacked organizations in the critical infrastructure sectors.

Authorities raiding the home of the alleged developer behind the RagnarLocker ransomware. **Image Credits:** Polizia di Stato (opens in a new window)

In an alert published last year, the FBI warned that it had identified at least 52 U.S. entities across 10 critical infrastructure sectors, including manufacturing, energy and government, that had been affected by RagnarLocker ransomware. At the same time, the FBI released indicators of compromise associated with RagnarLocker, including Bitcoin addresses used to collect ransom demands, and email addresses used by the gang's operators.

In its announcement on Friday, Ukraine's police said that since 2020 the RagnarLocker group had attacked and exfiltrated data from 168 international companies in Europe and the United States. The group demanded between $5 and $70 million dollars in cryptocurrency from its victims.

If a victim refused to pay or notified law enforcement of the intrusion, the hackers would publish the victim's data on the group's since-seized dark web site.

"Ragnar Locker explicitly warned their victims against contacting law enforcement, threatening to publish all the stolen data of victimised organisations seeking help on its dark web 'Wall of Shame' leak site," Europol said on Friday. "Little did they know that law enforcement was closing in on them."

Although the gang has been under the watchful eye of law enforcement for some time, RagnarLocker has been targeting victims as recently as this month, according to ransomware tracker Ransomwatch. In September, the gang claimed responsibility for an attack on Israel's Mayanei Hayeshua hospital and threatened to leak more than a terabyte of data allegedly stolen during the incident.

Lorenzo Franceschi-Bicchierai contributed reporting and writing. This article was first published on October 19, and updated with new details and comment from Europol and Italy's Polizia di Stato (State Police).

> Ragnarok ransomware gang shuts down and releases its decryption key