Ragnar Locker ransomware’s dark web extortion sites seized by police

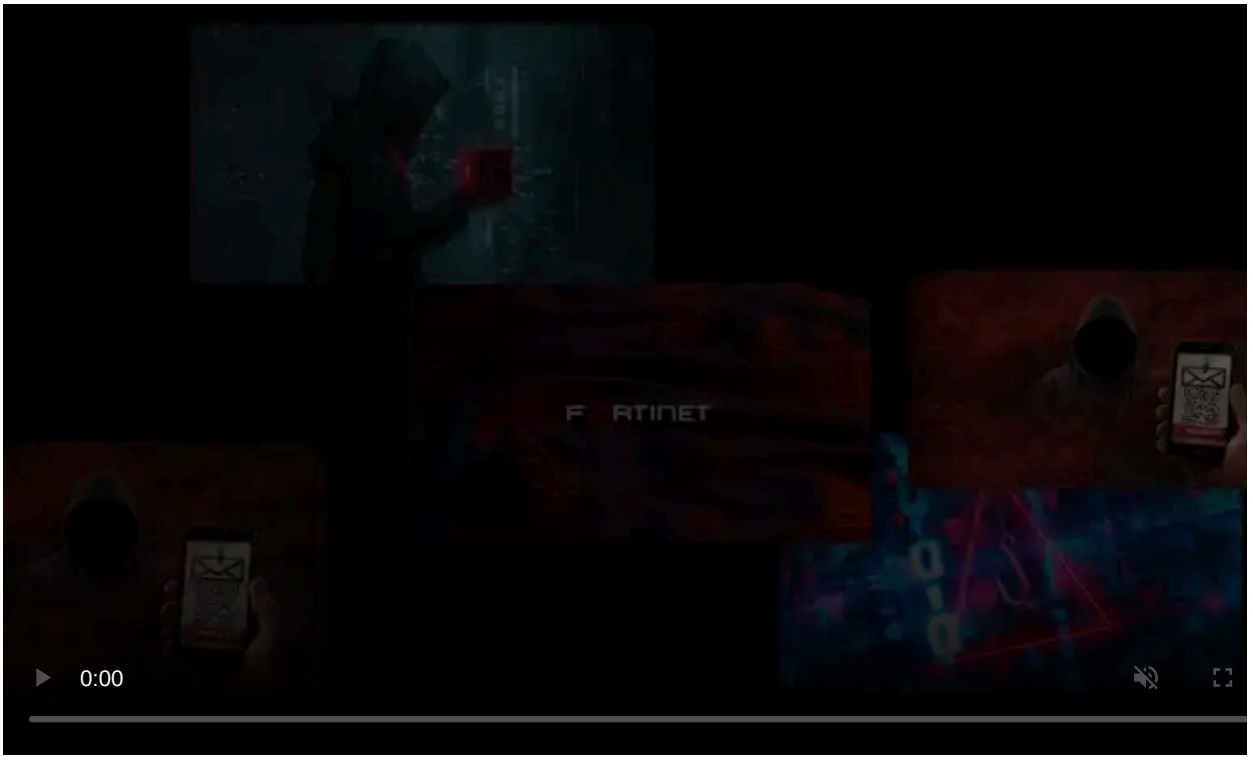
By Lawrence Abrams

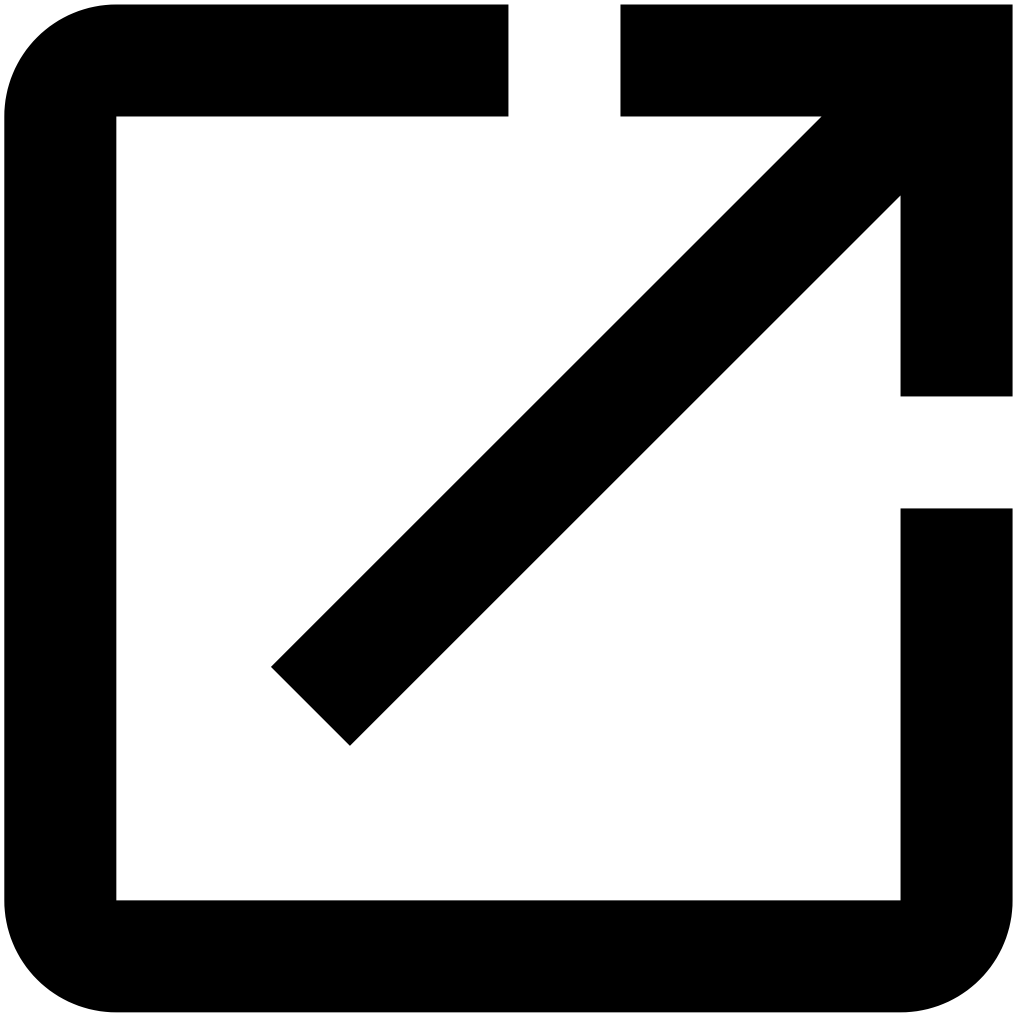
Published: 2023-10-19 · Archived: 2026-04-05 23:49:45 UTC

The Ragnar Locker ransomware operation's Tor negotiation and data leak sites were seized Thursday morning as part of an international law enforcement operation.

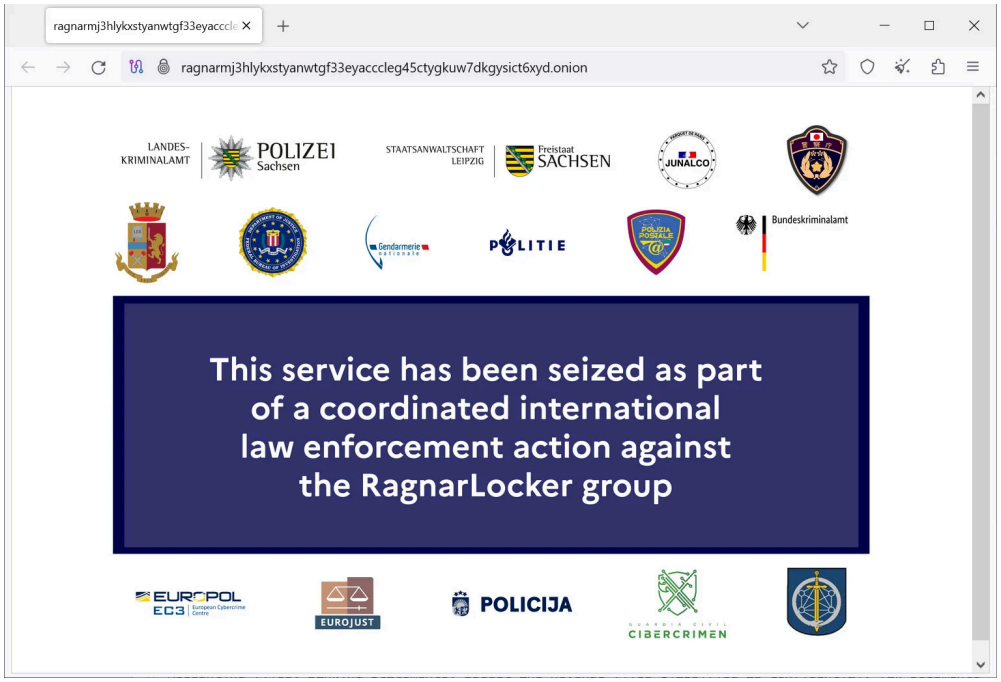
BleepingComputer has confirmed that visiting either website now displays a seizure message stating that a large assortment of international law enforcement from the US, Europe, Germany, France, Italy, Japan, Spain, Netherlands, Czech Republic, and Latvia were involved in the operation.

"This service has been seized as part of a coordinated law enforcement action against the Ragnar Locker group," reads the message.


F RTINET
0:00



A Europol spokesperson has confirmed the seizure message is legitimate as part of an ongoing action targeting the Ragnar Locker ransomware gang and that a press release will be published tomorrow. The FBI declined to comment.



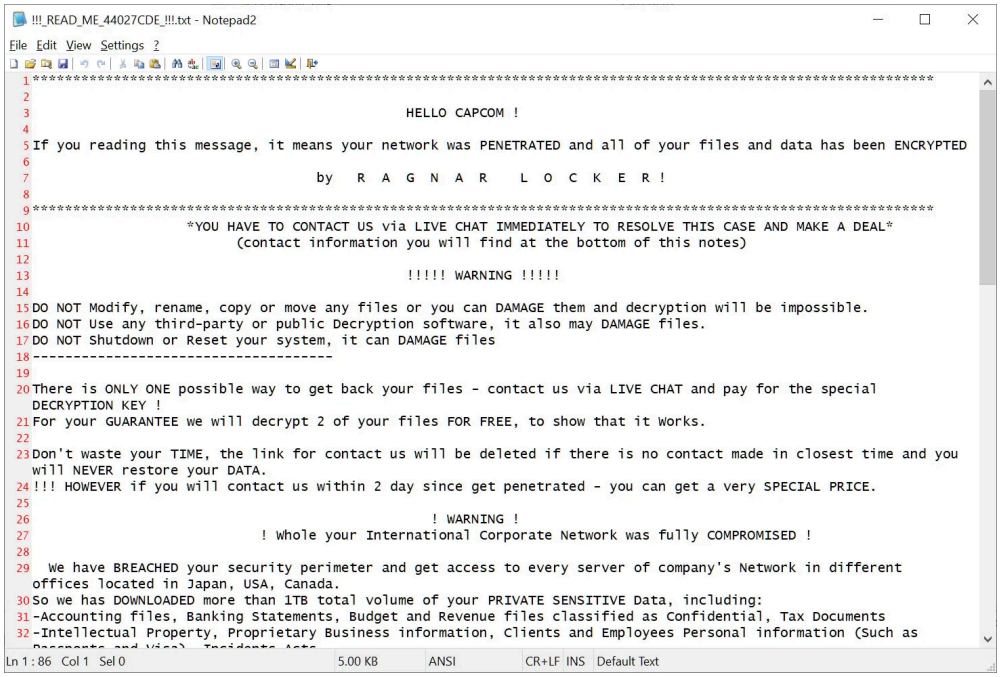
Ragnar Locker Tor negotiation site seized by law enforcement
Source: BleepingComputer

Who is Ragnar Locker

Ragnar Locker (aka Ragnar_Locker and RagnarLocker) is one of the longest-running ransomware operations at this time, launching at the end of 2019 as they began targeting the enterprise.

Like other ransomware operations, Ragnar Locker would breach corporate networks, spread laterally to other devices while harvesting data, and then encrypt the computers on the network.

The encrypted files and stolen data were used as leverage in double-extortion schemes to pressure a victim to pay.



RangarLocker ransom note for Capcom

Source: BleepingComputer

However, unlike most modern operations, Ragnar Locker was not considered a Ransomware-as-a-Service that actively recruited outside affiliates to breach networks and deploy the ransomware, earning a revenue share in the process.

Instead, Ragnar Locker was semi-private, meaning they did not actively promote their operation to recruit affiliates but worked with outside pentesters to breach networks.

The ransomware gang also conducts pure data theft attacks rather than deploying an encryptor, using their data leak site to extort the victim.

According to cybersecurity researcher MalwareHunterTeam, RagnarLocker has more recently switched to using a VMware ESXi encryptor based off of Babuk's leaked source code.

However, a new ransomware operation named DarkAngels was seen utilizing Ragnar Locker's original ESXi encryptor in an attack on Industrial giant Johnson Controls.

It is unclear if this new operation is an offshoot of Ragnar Locker, or a rebrand, or if they bought the source code.

The ransomware operation is responsible for numerous high-profile attacks over the years, including Energias de Portugal (EDP), Capcom, Campari, Dassault Falcon Jet, ADATA, and the City of Antwerp, Belgium.

It has been a bad week for ransomware operations and a win for law enforcement and cybersecurity. In addition to the RagnarLocker seizure, the Ukrainian Cyber Alliance (UCA) hacked the Trigona Ransomware operation and retrieved data before wiping their servers.

UCA says they will share the ransomware gang's data with law enforcement.

Source: https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomwares-dark-web-extortion-sites-seized-by-police/