Law Enforcement Raid on RagnarLocker Leads to Seizure of Dark Web Site, Arrest of Leader

Another joint international law enforcement effort involving about a dozen countries has taken down another major ransomware gang, this time the Ragnar Locker group known for its attacks on a wide range of high-profile corporate targets, along with hospitals and the city of Antwerp.

Europol appears to have headed up the operation with multiple EU countries participating, but law enforcement from the United States, Ukraine and Japan were involved as well. In addition to the seizure of assets, a man accused of being the group's ringleader was arrested in Paris and possible associates are also being interviewed in Spain and Latvia.

Dark web site takedown, arrests land severe blow on Ragnar Locker operations
The dark web site was seized Thursday, with an announcement following on Friday that at least one arrest had been made. Ransomware victims that visit the negotiation site will now see a message indicating that it has been seized by law enforcement, though there does not yet appear to be any assistance offered.

The announcement indicated that a 35 year old Czech Republic national had been arrested in Paris on October 16, under suspicion of being the group leader, and that law enforcement in his home country had searched his residence. The suspect has not been publicly identified as of yet. Ukrainian authorities also indicated that a suspect who lives in Kiev had their home searched and that a number of devices and electronic media were taken.

In addition to the dark web site, law enforcement authorities confirmed that infrastructure was seized in Germany, the Netherlands and Sweden. This includes nine servers and an undisclosed amount of cryptocurrency.

After years of seeming inactivity against major ransomware gangs, international law enforcement raids of this sort are becoming an annual event. This is the second big bust of a ransomware or data extortion gang in 2023 following the January takedown of Hive, which had become the second-largest group by attack volume at the time. A smaller but long-running ransomware service called NetWalker was also taken down in August, and a similar international operation recently disrupted the Qakbot botnet that is a preferred tool of threat actors.

Law enforcement continues to pick off boldest ransomware groups
Ragnar Locker has been operating since as far back as late 2019, thought to have gotten underway as an associate of Maze or MountLocker. The group was never among the absolute biggest in terms of attack volumes or money collected, but was a major threat and certainly on law enforcement's radar as a priority after penetrating several Fortune 500 companies and a number of critical infrastructure entities in several countries.

A central theme of the groups that attract these major law enforcement campaigns seems to be that they become too bold in attacking sensitive critical infrastructure, things like power or water or hospitals. Ragnar Locker made the news for its attacks on gaming company Capcom and liquor giant Campari, but attacks like the one on Energias de Portugal are more likely what moved it up the priority ladder. A flash warning issued by the FBI in early 2022 indicated that Ragnar Locker

had already successfully attacked 52 critical infrastructure companies across 10 sectors in the US at that point.

The group was also particularly aggressive in demanding payment from victims. It used double extortion techniques, threatening to leak stolen files via its dark web site, and at times simply engaged in data extortion without deploying ransomware. The group did not operate on an open ransomware-as-a-service model, however, either conducting all facets of attacks itself or privately selecting partners for particular jobs. This relative autonomy allowed the group to set its own terms, and in 2021 it declared that any contact with law enforcement or third-party firms would lead to an immediate dump of stolen data to the dark web site.

The group is thought to have successfully attacked at least 168 organizations in total during its roughly four year run. It still isn't clear exactly how much money it stole, or how much of victim funds it was sitting on when its assets were seized, but the group generally demanded payments of between $5 to $70 million from each victim (varying by perceived organization size and ability to pay).

Judging by its dark web site activity, Ragnar Locker slowed down significantly in 2023 but was still active as of September when it attacked the Mayanei Hayeshua hospital in Israel. The group may have seen law enforcement coming and begun disbanding and rebranding prior to the raid, as a new player called DarkAngels has recently been observed using the group's signature ESXi encryptor. This does not necessarily mean that it is former members, as the encryptor could have easily been purchased or stolen, but ransomware operators that are not arrested generally move on to form new groups within months of the dissolution of old ones.

Joint international #lawenforcement effort involving about a dozen countries has taken down Ragnar Locker #ransomware gang's #darkweb site, with an announcement that at least one arrest had been made. #cybersecurity #respectdata

Erich Kron, Security Awareness Advocate at KnowBe4, cautions that the Ragnar Locker saga may thus not be over just yet: "While on the surface, this feels like a win, ultimately it may be no more than an inconvenience for the Ragnar group if they are able to quickly set up other servers to replace these. In addition, this could cause problems for people whose organizations have been impacted by a ransomware attack, but have now lost a method to negotiate with the bad actors. Unless the websites that were seized contain information or decryption keys for these people, it could significantly delay their ability to recover. In the cases where encryption didn't occur but the data was stolen, there's a good chance that that data still resides with people that make up the group."