La policía arresta a miembros del ransomware LockBit y libera el descifrador en una ofensiva global.

Link de la Noticia

Fuente

In a joint advisory released in June, U.S. cybersecurity authorities and partners worldwide estimated that LockBit had extorted at least $91 million from U.S. organizations after as many as 1,700 attacks since 2020.

Today, the U.S. Department of Justice said the gang had over 2,000 victims and collected more than $120 million in ransom payments after demands totaling hundreds of millions of dollars.

Most recently, Bank of America warned customers of a data breach after third-party service provider Infosys McCamish Systems (IMS) was hacked in an attack claimed by LockBit.

In recent years, international law enforcement operations have also led to the seizure of servers and dark websites used by ALPHV (BlackCat) and Hive ransomware.

Who is LockBit?

The LockBit ransomware-as-a-service (RaaS) operation surfaced in September 2019 and has since been linked to or has claimed attacks on many high-profile organizations worldwide, including Boeing, the UK Royal Mail, the Continental automotive giant, and the Italian Internal Revenue Service.

LockBit ransomware seizure banner (BleepingComputer)

The ransomware group's affiliate panel has also been seized by the police, now showing a message to affiliates after they log in that their information, LockBit source code, chats, and victim information were also seized.

"We have source code, details of the victims you have attacked, the amount of money extorted, the data stolen, chats, and much, much more," the message reads.

"We may be in touch with you very soon. Have a nice day. Regards, The National Crime Agency of the U.K., the FBI, Europol, and the Operation Cronos Law Enforcement Task Force."

LockBit infrastructure seized

As part of this joint action, the NCA has taken control of LockBit servers used to host data stolen from victims' networks in

double extortion attacks and the gang's dark web leak sites.

LockBit's dark websites were taken down yesterday, showing seizure banners that revealed the disruption resulted from an ongoing international law enforcement action.

Operation Cronos

The global LockBit crackdown was coordinated by Operation Cronos, a task force headed by the U.K. National Crime Agency (NCA) and coordinated in Europe by Europol and Eurojust. The investigation began in April 2022 at Eurojust, following a request from the French authorities.

"The months-long operation has resulted in the compromise of LockBit's primary platform and other critical infrastructure that enabled their criminal enterprise," Europol said today.

"This includes the takedown of 34 servers in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom.

"This infrastructure is now under law enforcement control, and more than 14 000 rogue accounts responsible for exfiltration or infrastructure have been identified and referred for removal by law enforcement."

Europol has told BleepingComputer that those rogue accounts were used by LockBit members to host tools and software used in attacks and to store data stolen from companies.

As part of Operation Cronos, law enforcement also retrieved over 1,000 decryption keys from the seized LockBit servers. Using these decryption keys, the Japanese Police, the NCA, and the Federal Bureau of Investigation (FBI) developed a LockBit 3.0 Black Ransomware decryption tool with Europol's support.

This free decryptor is now available via the 'No More Ransom' portal. BleepingComputer contacted Europol to learn if the decryptor only helps LockBit victims after a certain date, but a response was not immediately available.

At this time, it is unknown how much cryptocurrency was stored in the 200 seized wallets. However, it may be possible for victims who paid ransom demands to recover some of their ransomware payments now, like the FBI previously did for Colonial Pipeline and various healthcare orgs.

Europol says that they have gathered a "vast amount" of data about the LockBit operation, which will be used in ongoing operations targeting the leaders of the group, as well as its developers and affiliates.

Two of the indictments were unsealed by the U.S. Justice Department against two Russian nationals, Artur Sungatov and Ivan Gennadievich Kondratiev (aka Bassterlord), for their involvement in LockBit attacks.

Previous charges against Lockbit ransomware actors include Mikhail Vasiliev (November 2022), Ruslan Magomedovich Astamirov (June 2023), Mikhail Pavlovich Matveev aka Wazawaka (May 2023)

French and U.S. judicial authorities also issued three international arrest warrants and five indictments targeting other LockBit threat actors.

Law enforcement arrested two operators of the LockBit ransomware gang in Poland and Ukraine, created a decryption tool to recover encrypted files for free, and seized over 200 crypto-wallets after hacking the cybercrime gang's servers in an international crackdown operation.