Russia arrests REvil ransomware gang members, seize $6.6 million

By Ionut Ilascu

Published: 2022-01-14 · Archived: 2026-04-05 13:25:51 UTC

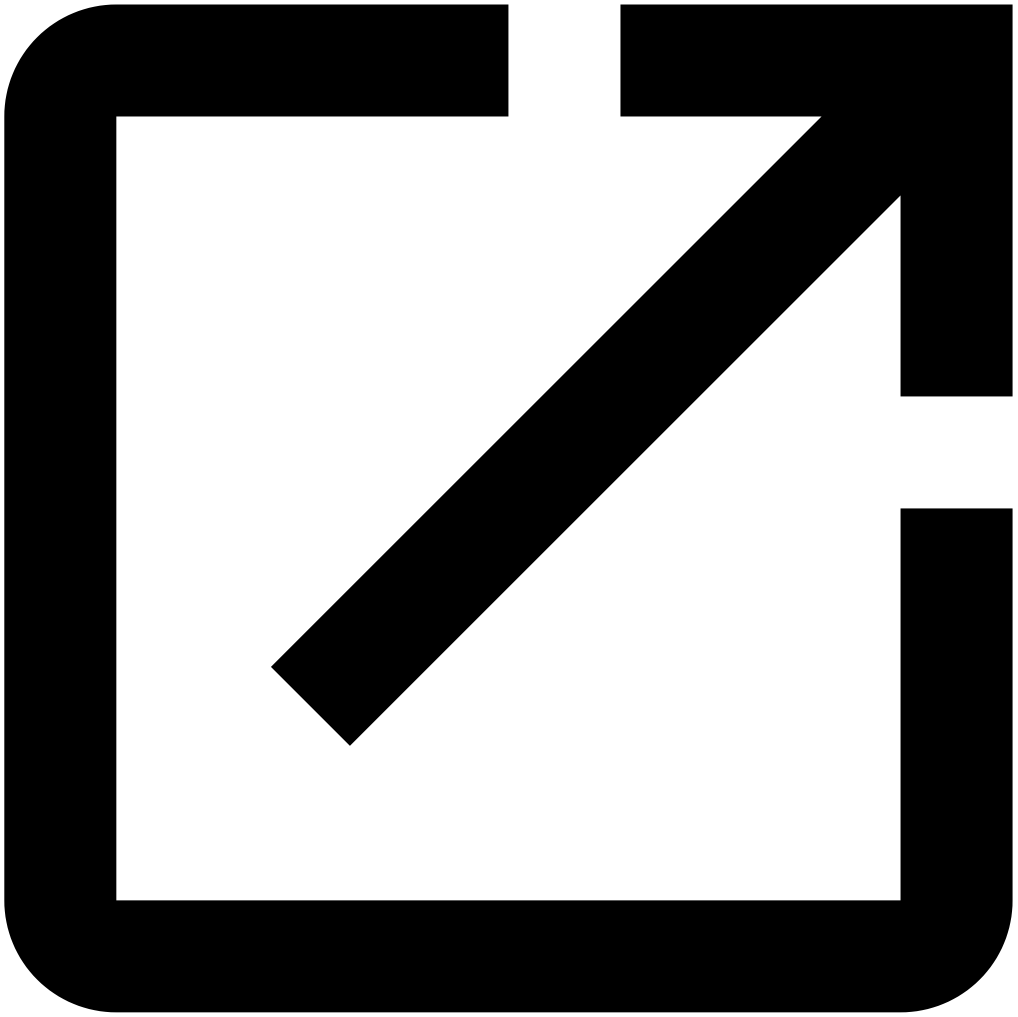
The Federal Security Service (FSB) of the Russian Federation says that they shut down the REvil ransomware gang after U.S. authorities reported on the leader.

More than a dozen members of the gang have been arrested following police raids at 25 addresses, the Russian security agency says in a press release today.

“The basis for the search activities was the appeal of the competent US authorities, who reported on the leader of the criminal community and his involvement in encroachments on the information resources of foreign high-tech companies by introducing malicious software, encrypting information and extorting money for its decryption” - Russia’s Federal Security Service

Russian authorities have detained 14 individuals suspected to be part of the REvil ransomware-as-a-service (RaaS) operation and confiscated cryptocurrency and fiat money as follows:


DIE LINKE.
0:00



- more than 426 million rubles (approximately $5,5 million)
- 600 thousand US dollars
- 500 thousand euros (approximately $570,000)

Russian authorities also confiscated 20 luxury cars purchased with money obtained from cyberattacks, computer equipment and cryptocurrency wallets used to develop and maintain the RaaS operation.

Footage from the raids available below shows how officers detained the suspects and confiscated money and electronics:

The raids took place at addresses in Moscow, St. Petersburg, Leningrad, and Lipetsk regions.

The FSB says that it was able to **identify all members of the REvil gang**, documented their illegal activities, and establish their participation in "illegal circulation of means of payment."

Apart from creating the file-encrypting malware and deploying it on enterprise networks across the globe, REvil members were also involved in stealing money from the bank accounts of foreign citizens.

"As a result of the joint actions of the FSB and the Ministry of Internal Affairs of Russia, the organized criminal community ceased to exist, the information infrastructure used for criminal purposes was neutralized" Russia's Federal Security Service

The FSB says that they informed the representatives of the competent U.S. authorities about the results of the operation.

REvil ransomware crumbles

REvil ransomware (aka Sodin and Sodinokibi) emerged in April 2019 from the void left behind by the shut down of the GandCrab operation.

In less than a year, the gang became the most prolific ransomware group, asking for some of the highest ransoms from its victims. It rose to infamy in August 2019 when it hit multiple local administrations in Texas and demanded a collective ransom of $2.5 million - the highest to that date.

Soon, asking for huge amounts of money from large organizations and getting paid became the norm. In a year, the gang claimed profits in excess of $100 million.

REvil's most publicized hit was the Kaseya supply-chain attack that crippled around 1,500 businesses all over the world. The ransom demand to decrypt all organizations was $70 million in Bitcoin.

This attack prompted a stern response from the U.S., with President Biden asking President Putin to take action against cybercriminals residing in Russia; otherwise, the U.S. would take action on its own.

The gang was also the first to have a representative going by the forum name UNKN at first, later switching to Unknown, who promoted the REvil RaaS business in the Russian-speaking criminal hacker community.

This public-facing representative disappeared soon after the Kaseya attack (some assumed Unknown was arrested) and pressure from international law enforcement increased.

After the Kaseya attack, the REvil operation took a break and then resumed operations two months later. What the operators did not know was that law enforcement had breached their servers before the hiatus and when they restored the systems from backups the criminals also restored machines controlled by law enforcement.

FSB's action against REvil comes after the U.S. and international law enforcement organizations joined forces to identify and arrest members of ransomware operations.

As a result, the U.S. announced in November 2021 that it had arrested a REvil ransomware affiliate (Ukrainian national Yaroslav Vasinskyi) responsible for the Kaseya attack and seized over $6 million from another Revil partner (Russian national Yevgeniy Polyanin), believed to have deployed about 3,000 ransomware attacks.

The same month, authorities in Romania arrested two REvil ransomware affiliates responsible for 5,000 attacks that brought them EUR 500,000 from collected ransoms.

Update [January 14, 2022, 13:26 EST]: Added background information about the REvil ransomware gang and arrests of its affiliates

---

Source: https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/