Russia sentences REvil ransomware members to over 4 years in prison

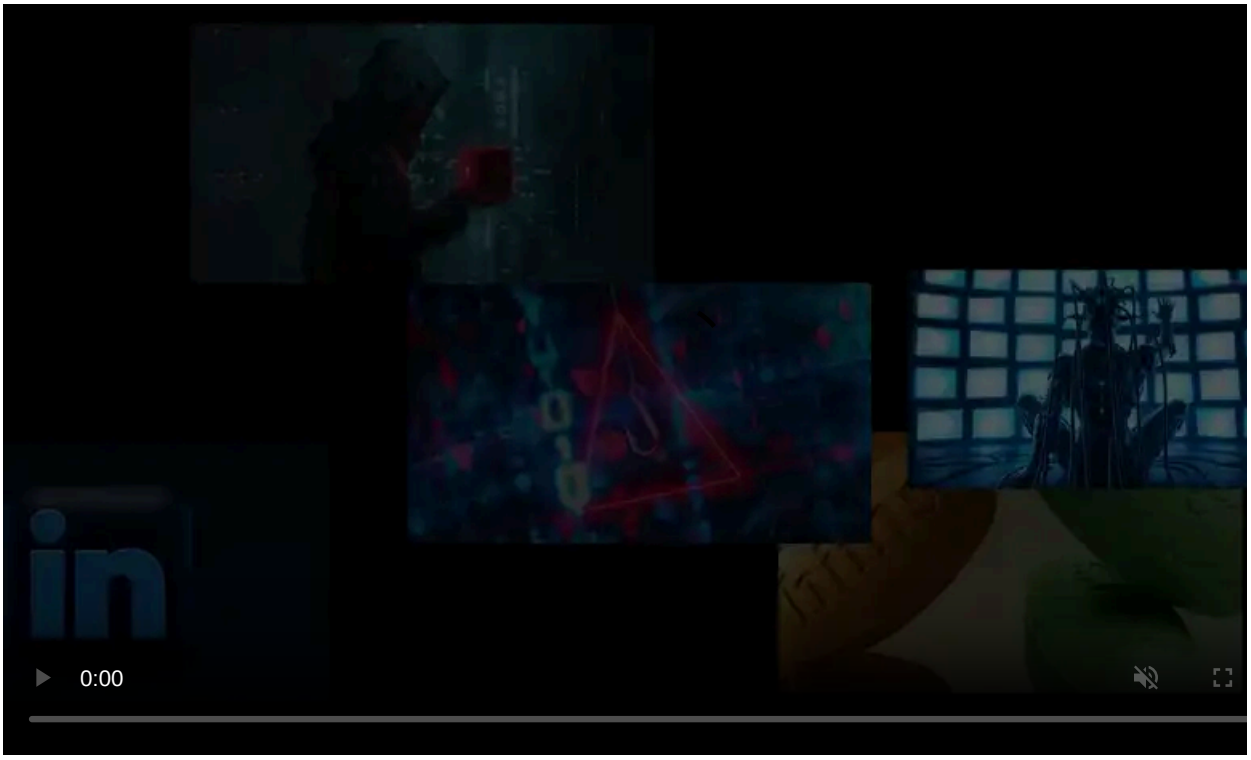
By Lawrence Abrams

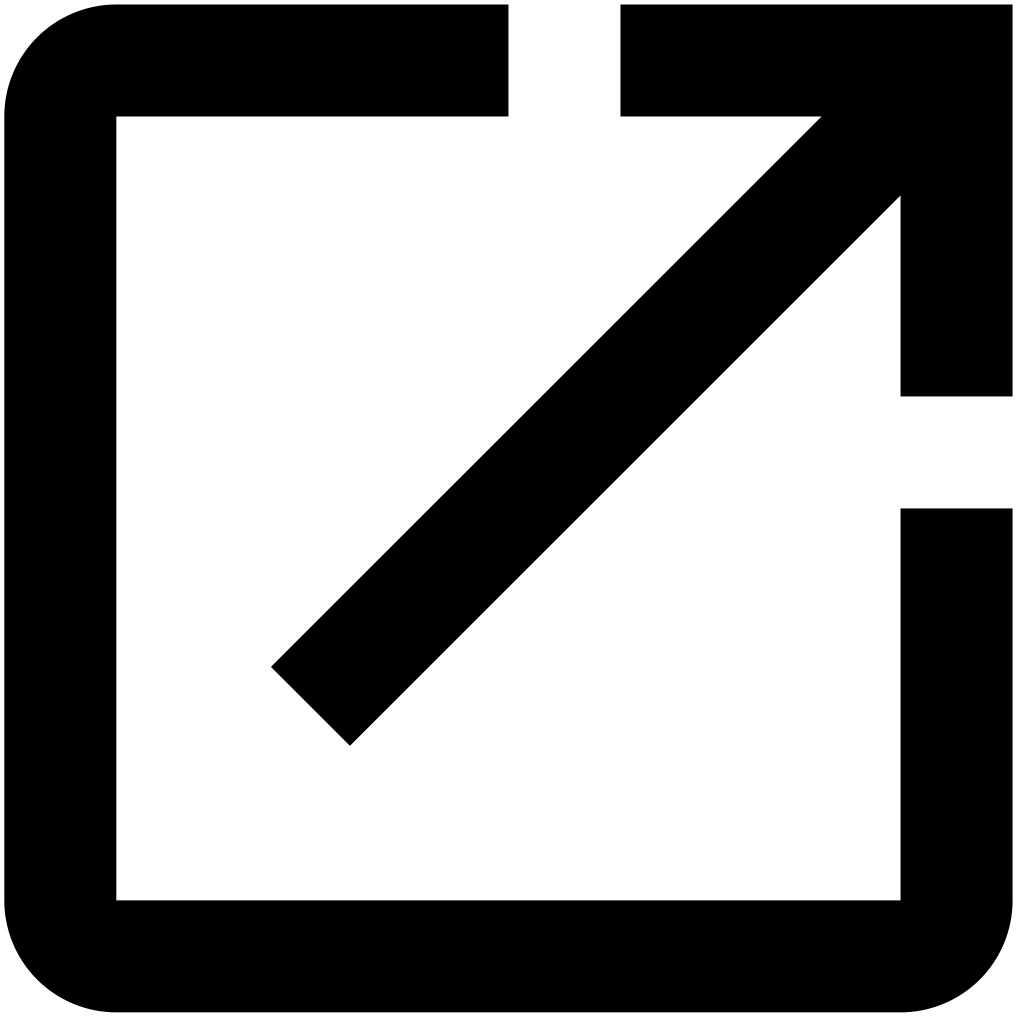
Published: 2024-10-25 · Archived: 2026-04-05 16:26:09 UTC

Russia has sentenced four members of the REvil ransomware operation to over 4 years in prison for distributing malware and illegal circulation of means of payment.

REvil ransomware (aka Sodin and Sodinokibi) was launched in April 2019 as a direct successor of the GandCrab operation.

In less than a year, the gang became the most prolific ransomware group, asking for some of the highest ransom payments at the time and earning over $100 million in a year.


0:00



However, in July 2021, when Revil hit over 1,500 businesses worldwide in a Kaseya supply chain attack, things took a turn for the worse for the ransomware gang.

In response to the attack, President Biden asked President Putin to take action against cybercriminals residing in Russia; otherwise, the U.S. would take action on its own.

Feeling the pressure from international law enforcement, the REvil operation took a break and then resumed operations two months later. However, they did not know that US law enforcement and international partners had breached their servers before the breach. When the cybercriminals restored from backups, the criminals also restored machines controlled by law enforcement.

At the request of the US government, Russia's Federal Security Service (FSB) disrupted the REvil ransomware gang in January 2022 after an international law enforcement operation identified and arrested members of ransomware operations, including the affiliate behind the Kaseya attack.

The FSB's action in 2022 led to the arrest of 14 members of the ransomware gang, raids at 25 addresses, and the seizure of $6.6. million.

"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 said in a press statement at the time.

As reported by The Record, eight members were ultimately tried, with Artem Zayets, Alexey Malozemov, Daniil Puzyrevsky, and Ruslan Khansvyarov sentenced today and four others put into a separate proceeding.

According to Russian media Kommersant, Zayets was sentenced today to 4.5 years, Malozemov to 5 years, Khansvyarov to 5.5 years, and Puzyrevsky to 6 years.

The court found all four guilty of illegal circulation of means of payment, with Khansvyarov and Puzyrevsky also found guilty of distributing malware.

The other four members, Andrey Bessonov, Mikhail Golovachuk, Roman Muromsky, and Dmitry Korotayev, will now be tried in a separate proceeding for illegal access to computer information.

Source: https://www.bleepingcomputer.com/news/security/russia-sentences-revil-ransomware-members-to-over-4-years-in-prison/