US seizes $6 million from REvil ransomware, arrest Kaseya hacker

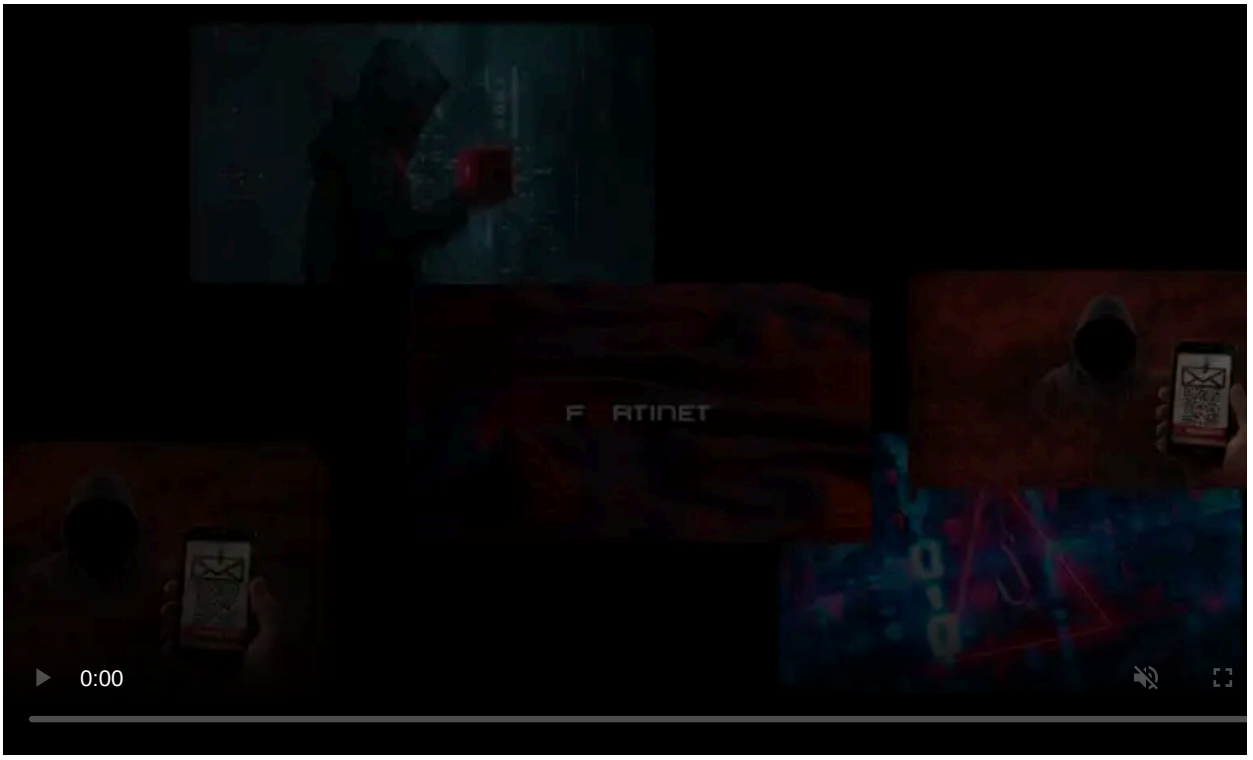
By Ionut Ilascu

Published: 2021-11-08 · Archived: 2026-04-06 03:18:33 UTC

The United States Department of Justice today has announced charges against a REvil ransomware affiliate responsible for the attack against the Kaseya MSP platform on July 2nd and seizing more than $6 million from another REvil partner.

The suspect is 22-year old Ukrainian national Yaroslav Vasinskyi, arrested for cybercriminal activity on October 8 at the behest of the U.S. when trying to enter Poland from his native country.

Vasinskyi is known by several aliases (Profcomserv, Rabotnik, Rabotnik_New, Yarik45, Yaraslav2468, and Affiliate 22). He is one of the seven REvil ransomware affiliates that have been apprehended so far, in ample international efforts to combat the ransomware threat.


F RTINET
0:00

Ransom demands of over 760 million

While the news of Vasinskyi getting arrested did not go unnoticed, the exact reason was unclear until his indictment and arrest warrant were unsealed on November 5.

In a press conference today, the DoJ announced the charges against Vasinskyi, underlining his involvement in the Kaseya attack that impacted around 1,500 businesses worldwide.

REvil ransomware, also known as Sodinokibi, is the successor of GandCrab and had an initial test run in April 2019 in an attack that exploited a vulnerability in WebLogic Server.

According to the indictment, Vasinskyi is a long-time affiliate of the REvil ransomware operation, being part of it since at least March 1st, 2019, and deployed about 2,500 attacks against businesses worldwide.

The investigation revealed that Vasinskyi's ransom demands amounted to $767 million but victims paid only $2.3 million. The operator is believed to have deployed ransomware on the networks of at least nine companies in the U.S.

In contrast, the entire REvil ransomware operation received more than $200 million since it started activity and encrypted at least 175,000 computers.

Of all the companies attacked, the one on Kaseya managed service provider (MSP) was the biggest, the ransom demand being $70 million to decrypt all the systems.

This incident acted as a catalyst for the U.S. to start an ample operation against the ransomware threat in cooperation with law enforcement across the world.

The U.S. is now requesting Vasinskyi's extradition and has unsealed the charges against him.

Seizing ransomware money

The DoJ also announced that law enforcement seized $6.1 million from another REvil ransomware affiliate, Russian national Yevgeniy Polyanin, who is currently at large.

Previously, the U.S. has recovered $4.4 million of the ransomware payment that Colonial Pipeline paid to the DarkSide ransomware gang following an attack that lead to temporary gas shortages.

Polyanin (a.k.a. LK4D4, Damnating, damn2Life, Noolleds, Antunpitre, Affiliate 23) is believed to have perpetrated about 3,000 ransomware attacks against various organizations, including multiple U.S. government entities and private-sector companies, extorting around $13 million from victims.

According to the indictment, Polyanin accessed and encrypted the networks of 13 government entities in Texas around August 16, 2019.

If the date sounds familiar it's because that's when 22 local governments had their systems locked in a REvil ransomware attack that leveraged flaws in software from an MSP.

While the hackers asked for a collective ransom of $2.5 million, one of the largest at the time, they got nothing as a coordinated state and federal response recovered the systems.

As part of the strategy to counter the ransomware threat, the U.S. Department of Treasury today announced sanctions against both Polyanin and Vasinskyi, blocking all property and interests in their property falling under the U.S. jurisdiction.

"Additionally, any entities 50 percent or more owned by one or more designated persons are also blocked. In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action" - U.S. Treasury

The charges against Polyanin are the same as for Vasinskyi:

- conspiracy to commit fraud and related activity in connection with computers (one count for each defendant)
- intentional damage to a protected computer (nine counts for Vasinskyi, 12 for Polyanin)
- conspiracy to commit money laundering (one count for each defendant)

In about five months, the DoJ's efforts have resulted in arresting seven affiliates of the REvil ransomware operation.

On November 4, authorities in Romania arrested two alleged REvil ransomware partners. A GandCrab affiliate was arrested on the same day in Kuwait. The other three individuals were apprehended in February, April, and October.

"The arrest of Yaroslav Vasinskyi, the charges against Yevgeniy Polyanin and seizure of $6.1 million of his assets, and the arrests of two other Sodinokibi/REvil actors in Romania are the culmination of close collaboration with our international, U.S. government and especially our private sector partners," - FBI Director Christopher Wray

Apprehending these REvil affiliates was possible through coordinated efforts from investigators and prosecutors from several jurisdictions:

- Romania's National Police and the Directorate for Investigating Organised Crime and Terrorism

- Canada’s Royal Canadian Mounted Police

- France’s Court of Paris and BL2C (anti-cybercrime unit police)

- Dutch National Police

- Poland’s National Prosecutor’s Office, Border Guard, Internal Security Agency, and Ministry of Justice

- the governments of Norway and Australia

Update [November 8, 14:50 EST]: Added more information from Polyanin's indictment and the DoJ press release.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
