# US arrests and charges Ukrainian man for Kaseya ransomware attack

By Catalin Cimpanu

Published: 2022-12-19 · Archived: 2026-04-05 21:31:00 UTC

The US Department of Justice has charged today a 22-year-old Ukrainian national for orchestrating the ransomware attacks on Kaseya servers that took place over the July 4 weekend this year.

The suspect, named Yaroslav Vasinskyi, was detained last month following an arrest warrant issued by the US. He was detained by Polish authorities at a border station while crossing from Ukraine into Poland.

In court documents unsealed today, the DOJ said that Vasinskyi was a long-time collaborator of the REvil (Sodinokibi) ransomware operation.

Officials said that using the hacker alias of MrRabotnik, Vasinskyi breached companies across the world and then deployed a copy of the REvil ransomware to lock victims' computers. To recover their files, victims had to make a ransom payment to the REvil gang, of which Vasinskyi kept a significant percentage.

While the Ukrainian national worked as a REvil "affiliate" since 2019, what led to his arrest was an attack he carried out over the July 4 weekend this year.

On Friday, July 2, Vasinskyi is believed to have used a vulnerability in Kaseya software to gain access to Kaseya servers installed across the world.

Used primarily by managed service providers (MSPs), these servers allowed the suspect to deploy the REvil ransomware inside the internal networks of thousands of companies across the world, which had hired the MSPs to provide remote IT management solutions.

The attack was devastating and led to a meeting of the White House National Security Council, talks between the Russian and US president, and the shutdown of the REvil RaaS a week later.

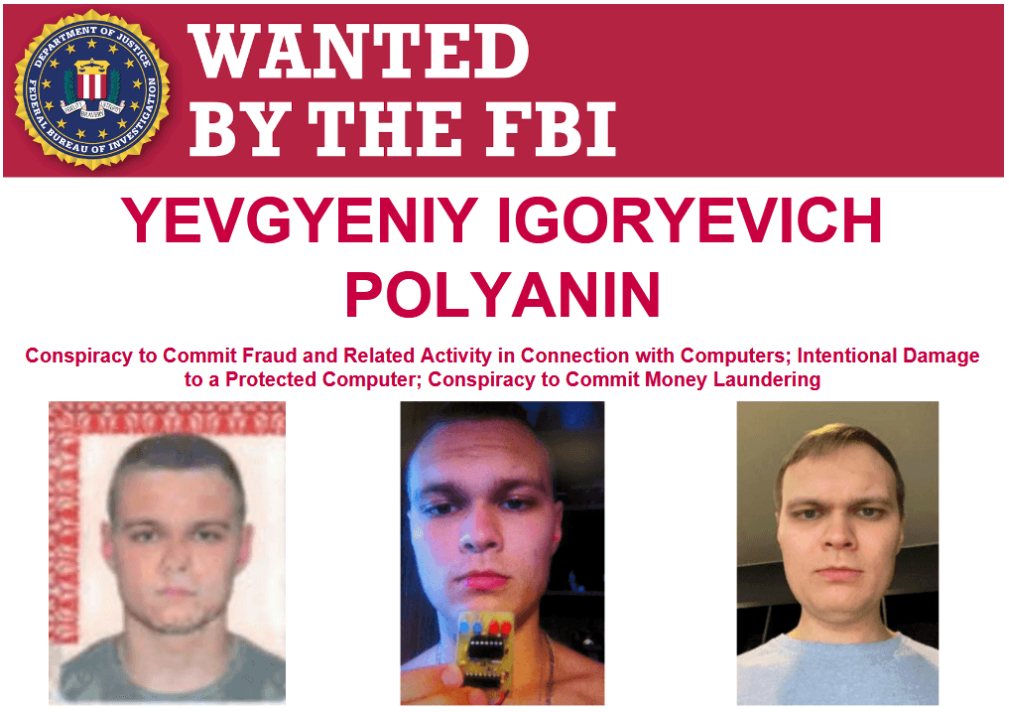
Second suspect charged for REvil attack on Texas municipalities

But besides Vasinskyi, the US has also charged a second suspect that helped the REvil gang deploy its ransomware.

Identified in court documents as Yevgeniy Polyanin, 28, the DOJ said this Russian national also worked as a REvil "affiliate" and performed intrusions on behalf of the REvil gang.

US officials believe that Polyanin is the person who breached the network of TSM Consulting, a Texas-based managed service provider, from where he deployed the REvil ransomware on the internal networks of at least 20 Texas local government agencies on August 16, 2019.

While Polyanin is still at large and wanted by the FBI, the DOJ said it managed to successfully seize $6.1 million worth of cryptocurrency assets that the suspect was holding in an FTX account.




Ransomware crackdown continues

US authorities announced Vasinskyi's arrest today, hours after Europol announced similar arrests in Romania, Kuwait, and South Korea.

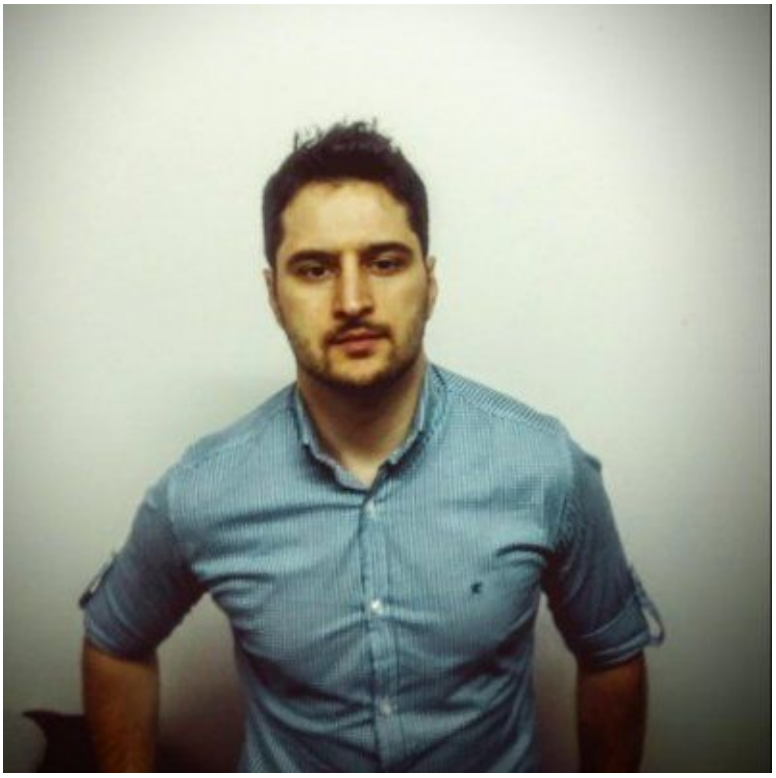
In total, seven "affiliates" who worked with the GandCrab and REvil RaaS programs were detained this year, Europol said.

As part of this operation, the US Treasury has also imposed sanctions on Chatex, a cryptocurrency portal that helped ransomware gangs launder funds in the past. Treasury officials also imposed financial sanctions on Polyanin, who is still at large, and believed to be residing in Russia.

In addition, the US State Department also announced a bounty program for any information that may lead to the identification and/or arrest of members of the REvil (Sodinokibi) ransomware group:

$10 million – for information on REvil key leaders$5 million – for information on REvil partners (affiliates)





Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

---