REvil Actor Accuses Russia of Planning 2021 Kaseya Attack

By Alexander Culafi

Published: 2025-08-11 · Archived: 2026-04-05 12:50:50 UTC

Source: Alexander Culafi via Dark Reading

A convicted REvil affiliate accused the Russian government of planning the 2021 supply chain attack against Kaseya.

Jon DiMaggio, chief intelligence strategist at Analyst1, and John Fokker, head of threat intelligence at Trellix, discussed the ransomware-as-a-service (RaaS) gang REvil during an Aug. 9 session at DEF CON 33. REvil is an infamous gang with a number of large-scale victims under its belt, including Acer and meat processing giant JBS S.A., but the talk covered REvil's most notorious strike: the July 2021 ransomware attack against Kaseya, which specialized in remote IT management software and services.

REvil targeted a vulnerability in Kaseya's remote monitoring software VSA in a supply chain attack that compromised more than 1,000 companies.

In November of that year, the US Department of Justice (DOJ) unsealed documents against two alleged REvil operators, Russian national Yevgeniy Polyanin and Yaroslav Vasinskyi, the latter of which had been arrested in Poland the month before.

Related:Not Toying Around: Hasbro Attack May Take 'Weeks' to Remediate

The DEF CON session, "Ghosts of REvil: An Inside Look with the Hacker Behind the Kaseya Ransomware Attack," primarily concerns Vasinskyi, who was extradited to the US in early 2022. In 2024, he was sentenced to more than 13 years in prison and fined more than $16 million for, as the DOJ put it, "his role in conducting over 2,500 ransomware attacks and demanding over $700 million in ransom payments."

A Look Inside REvil

Loading...

Fokker began with an overview of REvil's operation, explaining that the group began in 2019 as a successor to the GandCrab ransomware group. When GandCrab reached about 150 affiliates, the scope of the operation was becoming too large, and so a new group was established to support GandCrab's highest-earning members.

REvil, which is now defunct, had a straightforward ransomware-as-a-service model, with five admins at the top supporting 40 affiliates at any one time. In order to join, Fokker said, an affiliate needed to pass a "strict" interview in order to prove they were REvil material.

"I have to confess, we tried to apply," Fokker said, "but our Russian was not good enough so we were kicked out."

Although REvil was known for its big game attacks, the group also targeted individual consumers. When a ransom paid out, the money would be split between the gang's administration and the affiliate that carried out the attack.

The session highlighted a number of reasons the gang was successful, including an early example of having a dedicated communication platform rather than email negotiations; an early example of using a leak site to publish stolen data (now standard practice for much of the ransomware ecosystem); stable malware and decryptors ("You need to be able to keep your promise if you encrypt something," Fokker said); strict affiliate selection; and smart outsourcing of certain functions like money laundering to third parties.

Related:Bank Trojan 'Casbaneiro' Worms Through Latin America

One other key differentiator between REvil and other gangs was that it was "good at administration."

"Trust only goes so far if you pay people what they are owed. If you do not pay people, then they'll turn their back on you," Fokker said. And for REvil, the group had detailed accounting with IDs marking both affiliates and their campaigns.

REvil eventually fell apart, starting in an international infrastructure takedown operation on Oct. 21, 2021. In January 2022, Russia said it had dismantled REvil and charged several members.

Vasinskyi Speaks

The story got stranger when, in February of this year, DiMaggio received an email from federal prison claiming to be a contact request from Vasinskyi, the REvil operator serving a 13-plus year prison sentence.

At first, DiMaggio said Vasinskyi planned on speaking with a journalist that had much further reach, but due to DiMaggio's technical understanding and previous research of cybercrime forums, the pair established a bond that

continues today. At one point during the session, DiMaggio said he was planning to speak with Vasinskyi 30 minutes after the session ended.

Related:AI-Powered 'DeepLoad' Malware Steals Credentials, Evades Detection

Although one can't take a cybercriminal's word for granted, DiMaggio urged attendees to view the full report of his interactions with the REvil actor, which were published to Analyst1 that day.

"I think there's a lot of value in understanding what a criminal tells you, and you know at this point, he didn't have much to lose. There wasn't really a reason for him to lie to me. He has no chance of parole," DiMaggio said.

DiMaggio said that after the Kaseya attack, then President Biden said the US would respond if it turned out the Russian government was involved, "which is pretty ***** ironic because the first thing Vasinskyi told me was that the Russian government was involved."

Vasinskyi said that not only was the Russian government involved, but it also picked the target and orchestrated the attack, with Vasinskyi acting as the architect to create the relevant zero-day exploit. It's worth noting that Russia has not taken credit for any cybercriminal actions taken during the Kaseya attack.

"Vasinskyi doesn't deny his role in the attack. What he does deny is him being the one who executed it. According to him, he staged everything, got into the network, and staged everything, but he did not execute the ransomware payload itself," DiMaggio said. "According to Vasinskyi the Russian government did that, and that's a pretty big deal if he's telling me the truth now."

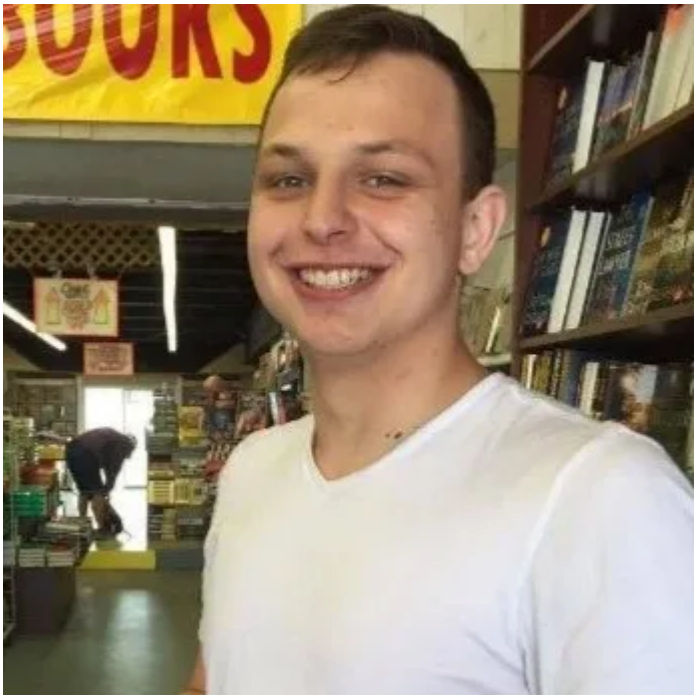
The Russian government's motive for this, Vasinkyi reportedly told DiMaggio, was not to make money but instead for the disruption from the attack to cripple downstream systems, allowing Russia to access critical infrastructure.

Vasinskyi, who is a Ukrainian national, was arrested while crossing the border into Poland. What followed, allegedly, were threats made against him and his family by individuals with supposed ties to Russian intelligence (as detailed in the aforementioned report).

DiMaggio ended the session with an observation: That although Vasinskyi was convicted for crimes he committed, "suddenly we stopped looking for the leadership of REvil." There have been no new indictments nor names of REvil administrators.

"I'm a big believer in chasing bad guys, but we can't stop just because we got one, and since he was sort of the one that was available. He wasn't in Russia, so he was accessible and it was kind of like having this trophy," DiMaggio said. "I'm not saying he shouldn't be in prison. What I'm saying is we should be going after the leadership — the people who made these plans."

About the Author



Senior News Writer, Dark Reading

Alex is an award-winning writer, journalist, and podcast host based in Boston. After cutting his teeth writing for independent gaming publications as a teenager, he graduated from Emerson College in 2016 with a Bachelor of Science in journalism. He has previously been published on VentureFizz, Search Security, Nintendo World Report, and elsewhere. In his spare time, Alex hosts the weekly Nintendo podcast Talk Nintendo Podcast and works on personal writing projects, including two previously self-published science fiction novels.
