REvil Affiliates Confirm: Leadership Were Cheating Dirtbags

By Lisa Vaas

Published: 2021-09-23 · Archived: 2026-04-05 19:03:26 UTC

After news of REvil's rip-off-the-affiliates backdoor & double chats, affiliates fumed, reiterating prior claims against the gang in "Hackers Court."

A day after news broke about REvil having screwed their own affiliates out of ransomware payments – by using double chats and a backdoor that let REvil operators hijack ransom payments – those affiliates took to the top Russian-language hacking forum to renew their demands for REvil to fork over their pilfered share of ransom payments.

Advanced Intelligence, the threat intelligence firm that disclosed the backdoor and double chats, told Threatpost on Thursday that a high-profile actor with an established reputation on the top Russian language hacking forum – Exploit – used AdvIntel's report findings to revitalize a claim filed in May against REvil on the Russian underground.

The way that ransomware-as-a-service (RaaS) operations such as REvil or DarkSide work is that affiliates do all the dirty work of network compromise, in exchange for (in the case of the original REvil RaaS) 70 percent of whatever ransom that victims fork over.

REvil leadership was supposed to pocket the remaining 30 percent – and only that much – of ransom payments, in exchange for providing the ransomware payload that the affiliates use to seize control of victims' data and systems.

But when negotiations suddenly, mysteriously collapse and the affiliates are left in the lurch, they start to get suspicious, and they turn to the underground's version of arbitration.

You can see why: Ransomware and other types of cyber attacks are, after all, big business.

Ransomware attacks spiked by 350 percent between 2018 and May 2021. When money goes missing, the underground community takes a businesslike approach to seeking redress. Namely, the underground has its own versions of "People's Court" – or, as the case may be, "Hacker's Court."

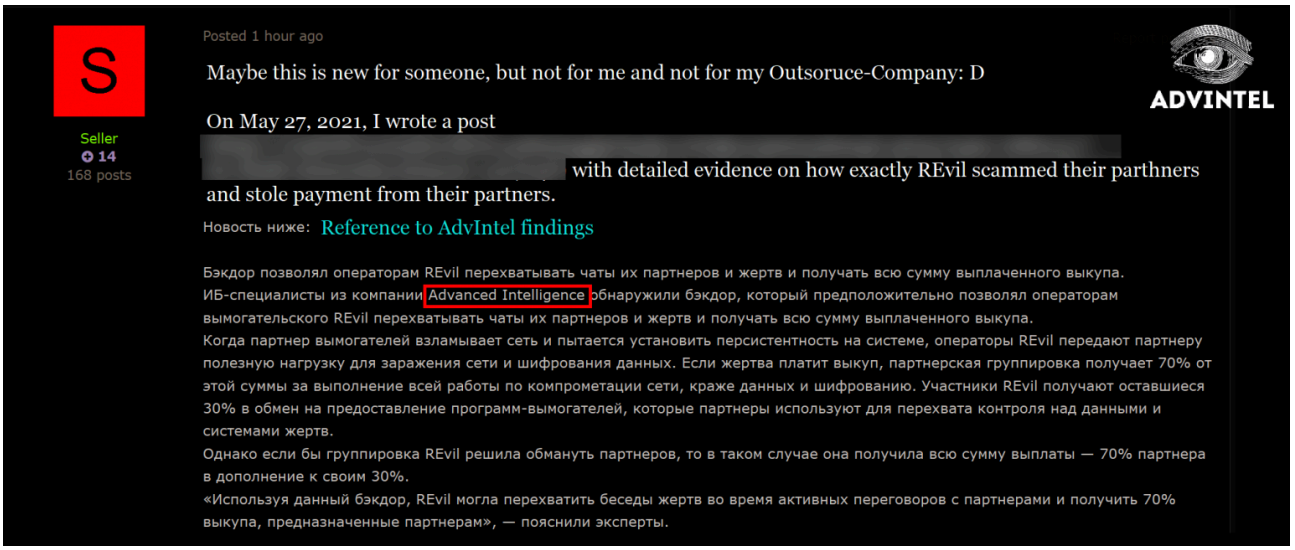
That's what happened with DarkSide, responsible for the Colonial Pipeline attack: Affiliates had a tough time getting paid for their work after DarkSide's servers were shut down in May, so they turned to admins of the group's Dark Web criminal forum to sort things out.

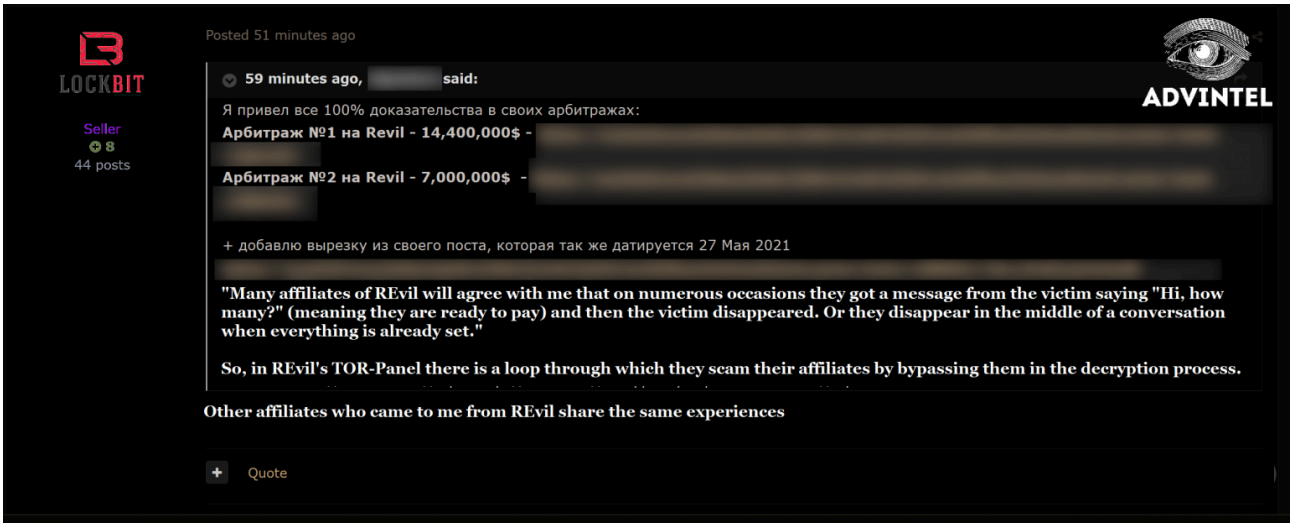
According to AdvIntel's Yelisey Boguslavskiy – head of research at the cyber risk prevention firm – aggravated, scammed affiliates had taken that route in May 2021, seeking to recoup $21.5 million USD from REvil for

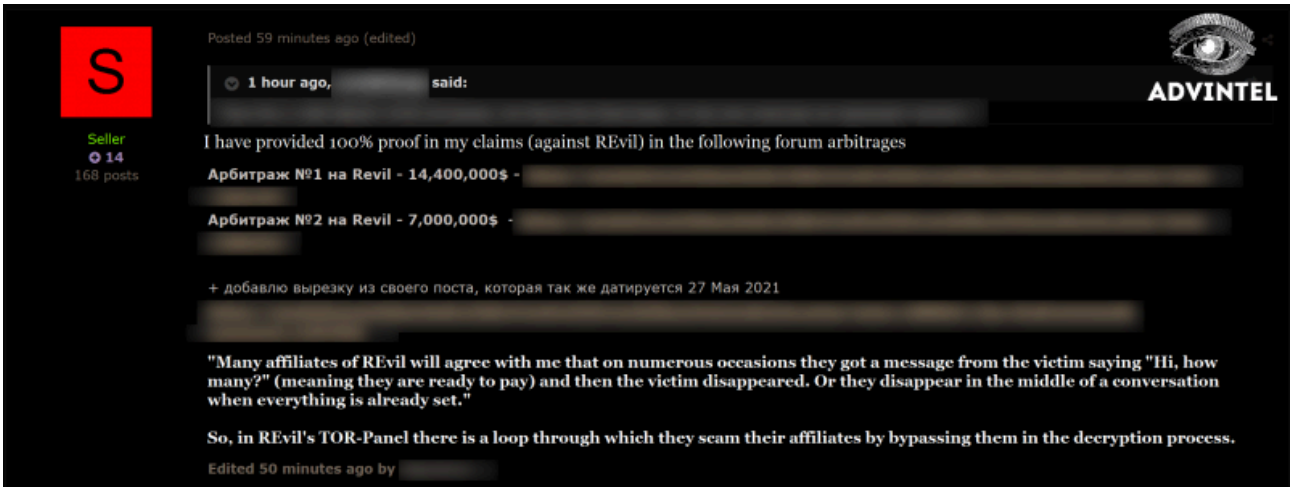
allegedly scamming them.

Ripped-Off Affiliates Fume

Below are screen captures of the actor reiterating the claim from May 2021 on the Exploit criminal forum on Thursday. The threat actor's reiteration confirmed AdvIntel's assumption: REvil leadership did indeed create a backdoor that enabled them to cut off ransom negotiations between victims and the gang's own affiliates, to run a double chat that enabled leadership to pose as victims who threw in the towel mid-negotiation, and to then step in to resume the negotiations, cut the affiliates out of the deal, and pocket the entire ransom payment.







Source: AdvIntel.

‘See? Told You So’

“While repeating this claim, the actor confirmed our assumption about the use of the backdoor, and, most importantly, about the use of double chats,” Boguslavskiy told Threatpost.

It wasn’t just the aggrieved affiliate who confirmed how slimy the REvil slimebags were, Boguslavskiy added: “Moreover, the representative of #LockBit also joined the discussion and stated that former REvil affiliates shared with them that they were scammed due to the double chat scheme.”

LockBit 2.0 is an extremely prolific RaaS gang that’s been proliferating like happy bunny rabbits, as evidenced by Herjavec Group’s LockBit 2.0 profile and its long list of LockBit 2.0’s victims. In other words, the gang’s reps probably know whereof they speak. When one of the gang confirms that REvil ripped off its own affiliates, there’s a fair chance they’re telling the truth.

Will This Cripple REvil?

Now that REvil has kind of, sort of sputtered back to life, with a new representative (but with little respect or trust on the criminal underground’s behalf), Boguslavskiy is hoping that confirmation of REvil’s comfort with screwing its own affiliates via a backdoor and double chats will lead to the gang being shunned on the underground, potentially weakening their ties and ability to recruit and collaborate within the community.

“Ideally, the revitalization of this May 2021 [claim] will lead to further bans against rebranded REvil on forums, which can further complicate their ability to interact with the community,” he suggested.
