REvil's "Cryptobackdoor" Con: Ransomware Group's Tactics Roil Affiliates, Sparking a Fallout

By Flashpoint Intel Team

Published: 2021-09-28 · Archived: 2026-04-05 17:43:34 UTC

How REvil allegedly cuts out affiliates according to… its former affiliates

REvil, a sophisticated Russian-speaking ransomware group, frequently works with affiliates who provide them with access to networks—and negotiate with victims on REvil's behalf—for a cut of the ransom. REvil affiliates can collect up to 70 percent of the ransom payment while REvil operators collect the rest. This is how REvil has historically operated its ransomware-as-a-service model.

REvil's tactics have recently come under renewed scrutiny. Threat actors operating on XSS and Exploit are currently reacting to evidence that REvil included a secret backdoor in its ransomware code—allegedly enabling the ransomware group to steal illicit ransom proceeds from its affiliates.

On September 20, a threat actor allegedly unearthed a "cryptobackdoor" in REvil's sample code and posted the finding on Exploit, an illicit high-tier Russian-language forum. The backdoor code enables REvil the capability of restoring encrypted files on its own—without the involvement of the affiliates it originally hired.

Flashpoint analysts note that the backdoor was likely exposed months ago. However, the September 20 leak represents what appears to be the first time concrete evidence of REvil's tactics have been made public.

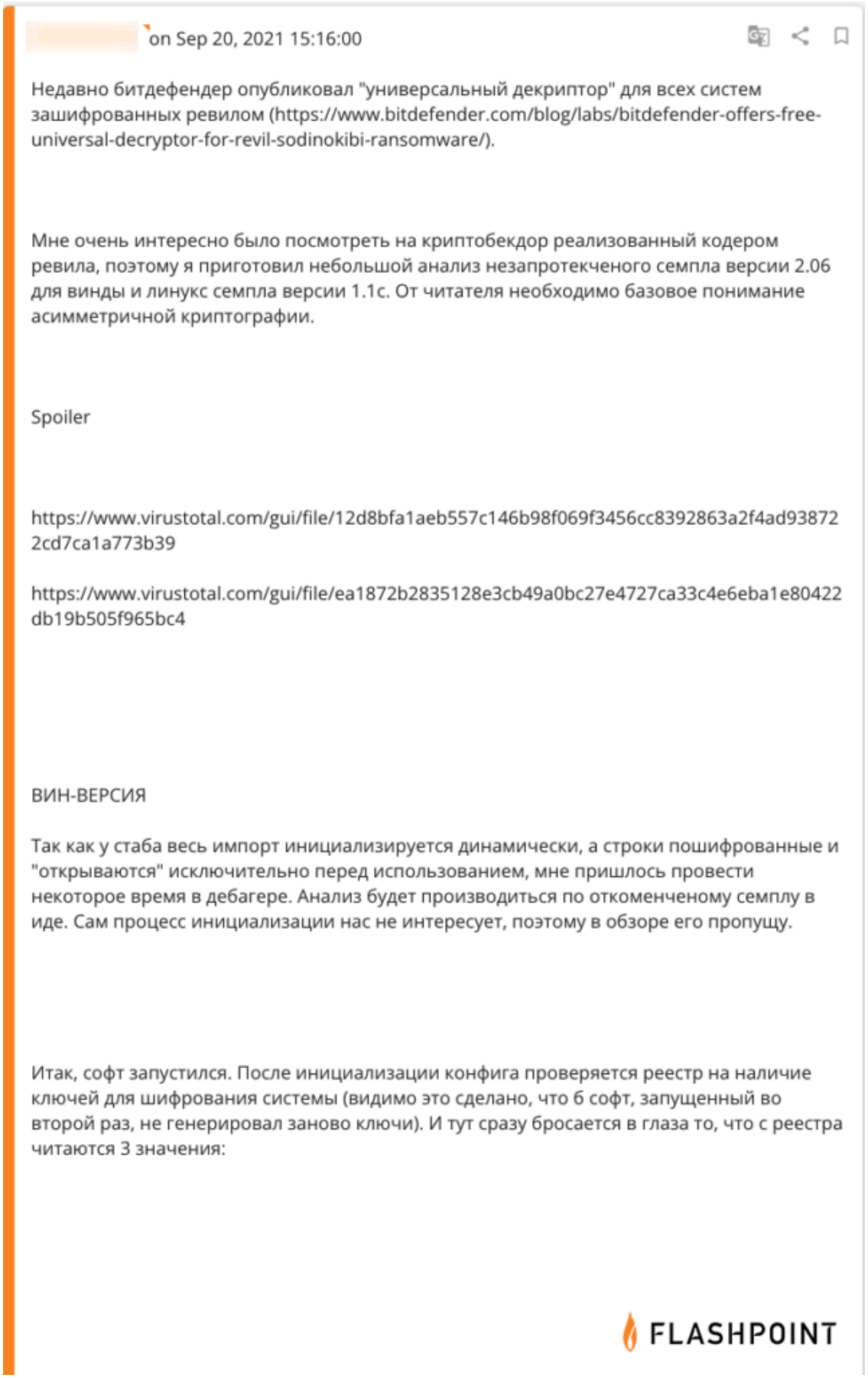
REvil can also allegedly hijack chats with victims and cut off discussions with its affiliates in order to collect full shares of the ransom without sharing the proceeds.

The subsequent fallout within the threat actor community offers the very organizations and individuals they target a window into the types of important chatter that can arise in the cybercriminal underground; insights into evolving relationships and behavioral codes among threat actors; and lens into whether arbitration is a realistic and viable possibility when dealing with major ransomware groups.

Making sense of the chatter

The threat actor Signature—who had previously requested US $7 million in an arbitration dispute on Exploit—re-hashed their argument after the REvil backdoor was revealed.

As a result, Signature started a new Exploit thread, saying that they knew all along about REvil's scamming tactics and claiming the revelations lend credence to Signature's arbitration claim. With the revelation of the parallel chat and the code backdoor, it is possible that an REvil operator had logged into the Signature chat posing as the victim company and abruptly ended the negotiations to collect all the ransom on their parallel chat, just as Signature alleged in May.



Exploit post outlining REvil's "cryptobackdoor," taken from the Flashpoint platform. (*Image: Flashpoint*)

LockBitSupp, the LockBit ransomware representative on Exploit, chimed in to say that many REvil affiliates share suspicion towards REvil.

Some illicit community members reacted with derision to the new evidence presented against REvil, pointing to a greater internal fissure growing between groups of affiliated threat actors.

One Exploit user said that this is the first time the are hearing of major ransomware groups stealing profits from their alleged partners. The user compared REvil's behavior to scamming methods used by low level carders.

Another Exploit user said they were tired of "lousy partner programs" used by ransomware collectives "you cannot trust" and further speculated that REvil would survive and thrive regardless of whether their reputation takes a real hit among fellow threat actors.

Cybersecurity analysts at Flashpoint note that animosity towards ransomware-involved threat actors has been ongoing since high-profile ransomware attacks caused increased law enforcement scrutiny toward cybercriminal communities.

Arbitration

Other users have also expressed pessimism regarding the underground community's ability to handle REvil's alleged behavior. One threat actor on XSS said that "the Devil himself will not be able to figure out" arbitration cases against REvil since the matter has gotten too complicated—and that arbitration might be prohibited anyway because some forums have purportedly instituted a ransomware ban.

Another threat actor echoed these sentiments that opening up arbitration cases against REvil would be useless, like "arbitrat[ing] against Stalin."

Reduce ransomware risk and see Flashpoint intelligence in action

When organizations, such as financial institutions and law enforcement agencies, gain insight into the operational dynamics of malicious cybercriminal communities, they can better understand threat actor TTPs; access potentially vital observations in real-time; leverage that information to thwart a ransomware attack.

Sign up for your risk-free 90-day trial and see how Flashpoint can provide you with the actionable threat intelligence you and your entire team need to identify and respond to threats targeting your organization. When equipped with Flashpoint Intelligence, your team has immediate access to collections across illicit online communities ranging from private forums and illicit marketplaces to encrypted chat services channels to gain insight into threat-actor activity on a global scale.
