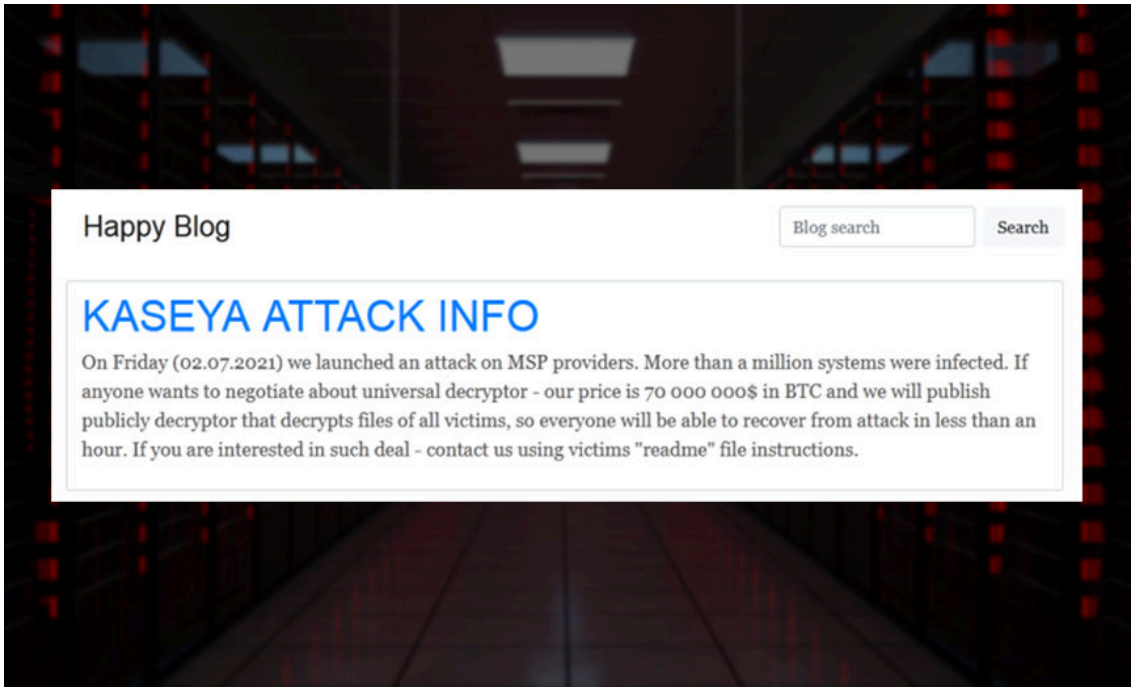
REvil's Cybercrime Reputation in Tatters - Will It Reboot?

By Mathew J. Schwartz

Archived: 2026-04-05 20:09:11 UTC

3rd Party Risk Management , Business Continuity Management / Disaster Recovery , Critical Infrastructure Security

Rebranding Remains Easy for Ransomware Groups, While Affiliates Already Come and Go (euroinfosec) • October 27, 2021



REvil's data-leak site (pictured) and payment portal disappeared after its July attack against Kaseya, only to reappear without explanation in September, before being hijacked earlier this month

Will the notorious ransomware operation known as REvil, aka Sodinokibi, reboot once again after someone apparently messed with its infrastructure?

See Also: How AI Expands Risk Across Enterprise

REvil first appeared in April 2019 as a spinoff of GandCrab ransomware and quickly established itself as one of the dominant ransomware-as-a-service operations. The operation developed the ransomware and later added a dedicated data leak site to name and shame victims and publish stolen data. It recruited business partners - or affiliates - to take the malware and use it to infect victims, in exchange for partners being promised a 70% cut of every resulting ransom payment.

Over the summer, however, rival DarkSide's hit on Colonial Pipeline, plus REvil's hits on meat processing giant JBS and managed service provider software developer Kaseya - among many others - led the White House to

move to better crack down on ransomware. Reportedly, a consortium of Western law enforcement agencies has been more actively disrupting ransomware operators' infrastructure, including that of REvil.

After going dark in July, REvil's Tor-based sites reappeared without explanation in September, listing fresh victims. Shortly thereafter, researchers at New York-based threat intelligence firm Advanced Intelligence, aka AdvIntel, reported that the Exploit cybercrime forum had published a report from its own malware reverse-engineering specialists, finding that all REvil samples up to July included a backdoor seemingly designed to let administrators decrypt files for a victim without affiliates knowing, so administrators could keep 100% of a ransom payment.

Tor-Based Sites Hijacked

Recently, REvil's sites again went offline, after one of its administrators, 0_neday, committed a basic operational security error and attempted to restore the existing sites from backups, rather than launch new ones. After reporting that the sites had been hijacked, 0_neday announced that the server would be taken offline, warning that someone had apparently been "looking for" him.

Reuters reported that the disruption was tied to a multigovernmental effort, although it published no evidence to back that up. But multiple ransomware operations believe that Western law enforcement or intelligence agencies have stepped up their disruption efforts.

One outstanding question now: Will REvil return, or has the brand been burned? Notably, core administrator UNKN - aka Unknown - hasn't been seen or heard from since July, leading some members of REvil to say they suspect he might be dead.

"REvil as a brand is likely gone for good as affiliates and other threat actors would probably not want to collaborate with an operation that was reportedly compromised by law enforcement," says Brett Callow, a threat analyst at security firm Emsisoft. "Whether the individuals behind REvil are also gone for good is an entirely different matter. Unfortunately, it's not at all unlikely that they'll make a comeback under a new name."

Indeed, cybercrime operations that catch unwanted heat sometimes just rebrand, as DarkSide did by becoming BlackMatter.

REvil's Reputation Fades

REvil has faced increasingly hostile questioning on cybercrime forums since its reappearance in September, says Victoria Kivilevich, director of threat research at Israeli threat intelligence firm Kela. That has included "speculations about UNKN's fate, public clashes of the new representative with other threat actors, including LockBit's administrator, the announcement of recruiting affiliates on RAMP, and publication of six new victims on REvil's blog," she says.

"The most common reaction between threat actors was the prejudice against working with REvil again since they did not provide sufficient explanations about the Kaseya attack, the group's disappearance and reemergence, and - probably the most serious claim - the reason behind using the same infrastructure that could be compromised," she says. "Combined with news about a secret backdoor enabling REvil's creators to scam its affiliates, such discussions significantly disrupted REvil's reputation."

Leadership in Turmoil

The original configuration of REvil appeared to be five or six administrators, each with different roles - two focused on affiliates, two more on the back end, says John Fokker, the principal engineer and head of cyber investigations for Advanced Threat Research at McAfee Enterprise.

He notes that Unknown's disappearance - whereabouts still unknown - might explain why 0_neday was behind the attempt to restore REvil's Tor-based data leak site and payment portal. But 0_neday made a rookie mistake by failing to launch the site with a new private key, leading to a new .onion address that he could have announced via Pastebin or another free text-sharing site.

Chatter on the XSS cybercrime forum about 0_neday's botched attempt to restore REvil's Tor sites (Source: John Fokker, McAfee; click to enlarge)

REvil doesn't appear to be operating at full strength. Even so, key to disrupting the likes of REvil will be not just arresting administrators but also the affiliates that take the crypto-locking malware and use it to infect victims, Fokker says.

According to cybercrime intelligence firm Intel 471, affiliates regularly work with multiple ransomware operations, sometimes at the same time, meaning the most experienced ones wouldn't hesitate to work with the likes of Conti or LockBit 2.0 - if they aren't already - if they believe REvil to be burned.

As that highlights, REvil is of course only one operation, and numbers suggest its disappearance isn't having a big impact.

Not all ransomware operations run data leak sites or blogs, which makes it difficult to count the total number of ransomware victims. But of the groups that do, including REvil, Kela reports that they collectively listed 205 victims in June. In August, after REvil's disappearance, such sites listed 248 new victims, growing to 251 in September.

"One can see that the ransomware groups' activities are steadily growing," Kela's Kivilevich says. "The disappearance of one group does not significantly influence the overall ransomware threat, as also could be seen from the shutting down of DarkSide, Avaddon and other groups active this year."

Arresting Affiliates Remains Challenging

No doubt law enforcement is seeking to unmask and arrest REvil's administrators, if they haven't already started to do so. But Fokker of McAfee Enterprise says police need to better identify and arrest affiliates, since they're so integral to the ransomware business model and are not beholden to REvil or any other group.

"If the ransomware name goes away, you still have these people doing 99% of the whole intrusion," Fokker says. "They're skilled, and they'll move to something else. Heck, they can use BitLocker, from Microsoft, to lock

somebody's computer, and they can still earn money."

Even as groups come and go, the opportunity for easy, safe profits continues to attract new players as well.

"The fact that they can make so much money and have such a small chance of being caught - they're not going to stop," Fokker says. "It's real simple: The money is too addictive. They're not going to stop."
