Ransomware Giant REvil's Sites Disappear

By Lisa Vaas

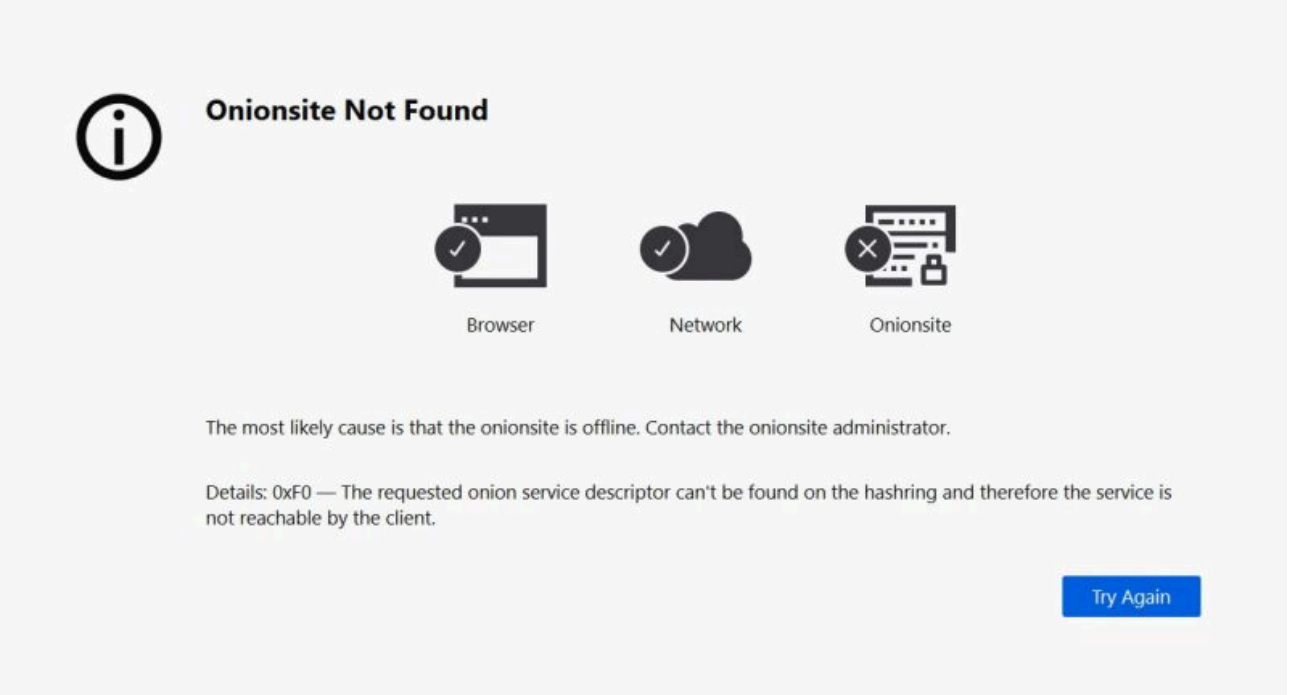
Published: 2021-07-13 · Archived: 2026-04-06 00:05:43 UTC

Just days after President Biden demanded that Russian President Putin shut down ransomware groups, the servers of one of the biggest groups mysteriously went dark.

All of REvil's Dark Web sites slipped offline as of early Tuesday morning, and it's not clear whether it's due to the ransomware gang getting busted or whether the threat actors did it on purpose.

The REvil ransomware operation, a.k.a. Sodinokibi, uses both clear web and Dark Web sites to negotiate ransoms, leak data, support its backend infrastructure and receive payment from its many victimized organizations. That victims list has recently grown with the addition of Kaseya and its many managed service provider (MSP) customers, as well as the global meat supplier JBS Foods,

All of REvil's sites went offline as of around 1 a.m. It doesn't mean that the notorious gang has been shut down, as one cybersecurity expert emphasized – it's just that all its sites were unreachable, up until at least Tuesday at 2:55 p.m. EDT.



"Onionsite not found" message displaying in place of REvil's site. Source: BleepingComputer

One possibility: It could be that the U.S. shut down the servers. Then again, perhaps it was the Russian government. The timing would make sense, given the White House's saber-rattling at Russia over the ransomware plague. The silenced servers come just a few days after President Biden called President Vladimir V. Putin of Russia and demanded that he shut down ransomware groups attacking American targets.

If you don't, we will, Biden said. On Friday, when a pool of reporters asked the president if the U.S. might attack the servers that Russia-linked cybercriminals have used to hijack American networks, he said, "Yes."

Ransomware Gangs Are 'on Borrowed Time'

Jake Williams, co-founder and CTO at BreachQuest, told Threatpost that it's all just speculation at this point, but ransomware gangs operating in Russia "were on borrowed time the second Colonial was hit." He was referring to the ransomware attack on Colonial Pipeline leading up to Memorial Day Weekend: An attack that was attributed to the ransomware-as-a-service (RaaS) player DarkSide.

"The Russian government didn't care about the cybercrime occurring within its borders, but only so long as it didn't impact Russia itself," Williams said in an email. "That has clearly changed – the Russian government can clearly see they are being impacted by the actions of these actors. Whether REvil was taken out of commission by the Russian government, saw the writing on the wall and took infrastructure down, is simply rebranding like so many groups have (likely including REvil itself), or something else, is unknown at this point."

Theories abound. Drew Schmitt, principal threat intelligence analyst for GuidePoint Security, echoed Williams' assertion that the darkened servers could be attributed to a number of things at this point.

"A lack of DNS response is a potential indicator of law enforcement involvement, but it's not enough to determine whether the threat group changed their URL, is doing maintenance, or something similar," he told Threatpost on Tuesday via email.

"An unresolved DNS response over a short period of time is not necessarily a strong indicator without correlating evidence, statements, etc.," he expounded. "It could be a short outage, however, we would need more time and evidence to tell what actually may be going on."

This isn't the first time, at any rate: Last week, REvil's site went down for a short while, according to Schmitt.

It could be that REvil chose to fade away, or it could be that its servers were seized a la DarkSide. In the DarkSide server shutdown, the threat actor posted on an underground forum that it had lost access to the public part of its infrastructure: Specifically, the servers for its blog, payment processing and denial-of-service (DoS) operations had been seized.

The Tor Project's Al Smith told BleepingComputer that the "Onionsite Not Found" message could mean a few things: "In simple terms, this error generally means that the onion site is offline or disabled. To know for sure, you'd need to contact the onion site administrator," he was quoted as saying.

The sites have recently been active. But as of Tuesday afternoon, visitors were being greeted with messages saying that "A server with the specified hostname could not be found."

A 'Planned' Takedown

Another cybersecurity expert, John Hultquist of Mandiant Threat Intelligence, told CNBC that it looks like this was an intentional, orderly takedown, though we don't know yet who's behind it: "The situation is still unfolding, but evidence suggests REvil has suffered a planned, concurrent takedown of their infrastructure, either by the operators themselves or via industry or law enforcement action," he said.

REvil's Usually Up and Humming

At any rate, the inaccessibility of the REvil ransomware group's websites is unusual, according to the Photon research team at Digital Shadows. The team told Threatpost that REvil's infrastructure "has historically been more stable than that of other ransomware groups."

They suggested that the outage could be caused by temporary technical issues or upgrades, or it could signify a law-enforcement disruption of the group's operations. But they did note that as of Tuesday, REvil's representatives "have not appeared on high-profile Russian-language cybercriminal forums for several days."

This Is Likely Not REvil's Last Hurrah

The Photon team added that, while chatter about the outage is limited due to some Russian-language forums' "hostile attitude towards discussing ransomware," some threat actors have speculated that even if law-enforcement agencies have successfully targeted REvil, it won't spell the end of the group's activities. Some threat actors predicted that the group will reappear under another name or split into smaller groups to attract less attention, the team said via email.

Meanwhile, the ripples of ransomware attacks by the likes of REvil can spread for months. That was evidenced by an attack on the Guess fashion label that compromised the personal and banking data of 1,300 victims. That data spill came after a February ransomware attack inflicted on Guess and attributed to DarkSide.

Guess has started sending letters to 1,300 employees and contractors who had their personal and banking data exposed during the breach.

But Hurray Nonetheless?

Regardless of whether it's a permanent shutdown or a temporary shut-up, REvil's darkened servers are cause for celebration, some said.

Katie Nickels, director of intelligence for Red Canary, commented on Twitter: "I don't know what this means, but regardless, I'm happy! If it's a government takedown – awesome, they're taking action. If the actors voluntarily went quiet – excellent, maybe they're scared."

Does it matter either way? Nickels thinks not: "It's still important to remember that this doesn't solve ransomware."

Check out our free upcoming live and on-demand webinar events – unique, dynamic discussions with cybersecurity experts and the Threatpost community.
