

REvil ransomware gang's web sites mysteriously shut down

bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/

Lawrence Abrams

By

[Lawrence Abrams](#)

- July 13, 2021
- 10:49 AM
- 7



The infrastructure and websites for the REvil ransomware operation have mysteriously gone offline as of last night.

The REvil ransomware operation, aka Sodinokibi, operates through numerous clear web and dark web sites used as ransom negotiation sites, ransomware data leak sites, and backend infrastructure.

Starting last night, the websites and infrastructure used by the REvil ransomware operation have mysteriously shut down.



Onionsite Not Found



Browser



Network



Onionsite

The most likely cause is that the onionsite is offline. Contact the onionsite administrator.

Details: 0xF0 — The requested onion service descriptor can't be found on the hashing and therefore the service is not reachable by the client.

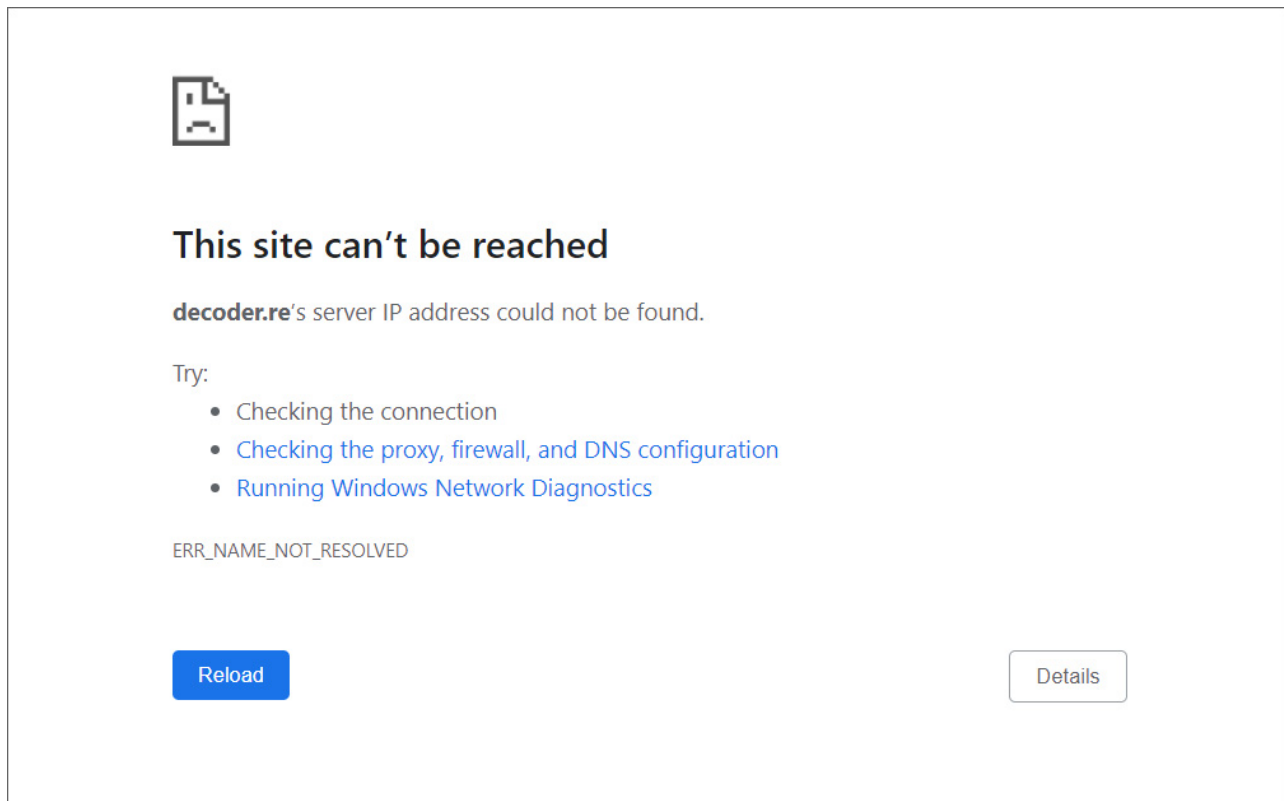
Try Again

REvil Tor site no longer accessible

"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," the Tor Project's AI Smith told BleepingComputer.

While it is not unheard of for REvil sites to lose connectivity for some time, all sites to shut down simultaneously is unusual.

Furthermore, the decoder[.]re clear website is no longer resolvable by DNS queries, possibly indicating the DNS records for the domain have been pulled or that backend DNS infrastructure has been shut down.

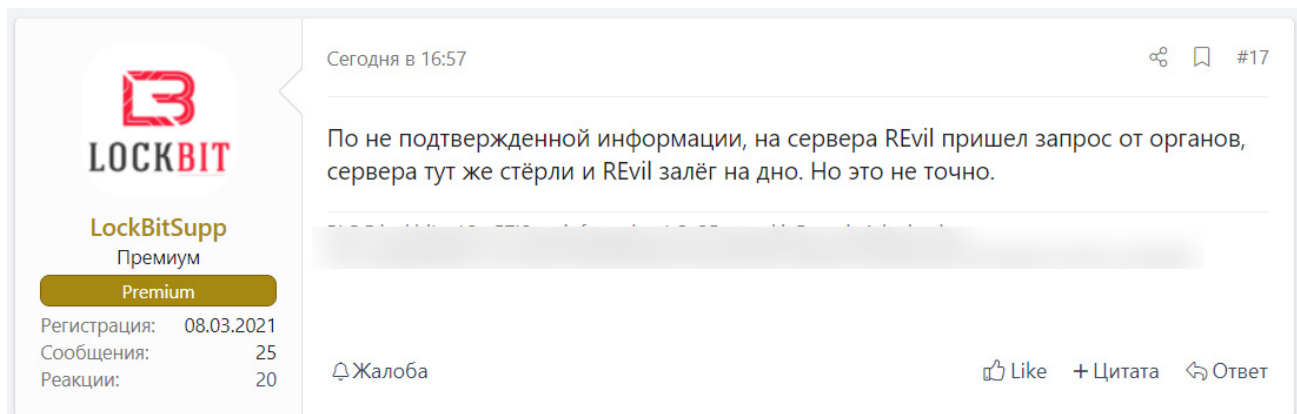


REvil domain no longer resolves to DNS queries

Recorded Future's [Alan Liska](#) said that the REvil web sites went offline at approximately 1 AM EST this morning.

This afternoon, the LockBit ransomware representative posted to the XSS Russian-speaking hacking forum that it is rumored the REvil gang erased their servers after learning of a government subpoena.

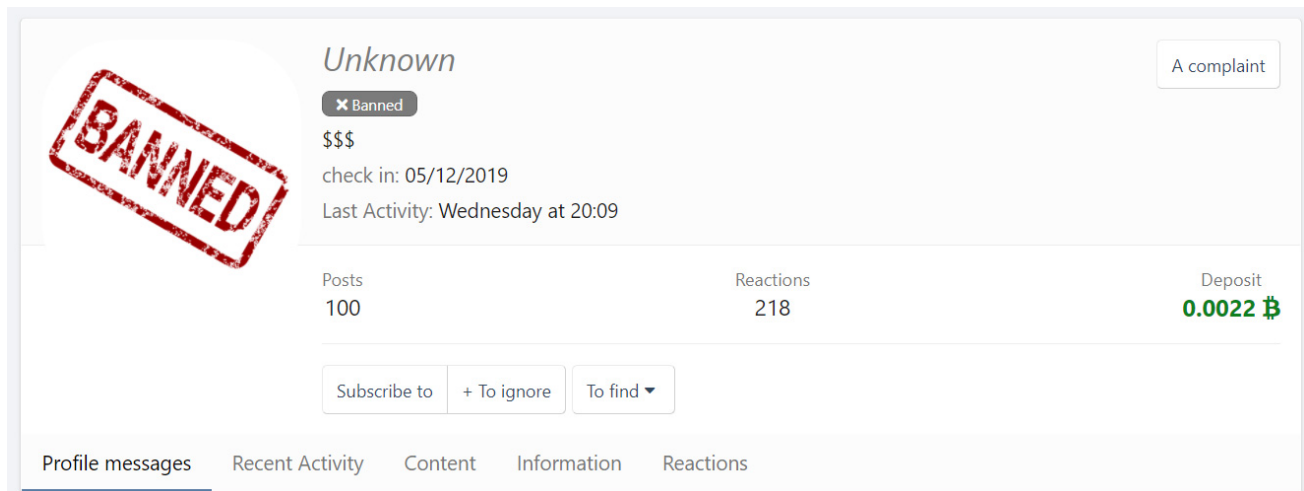
"Upon uncorroborated information, REvil server infrastructure received a government legal request forcing REvil to completely erase server infrastructure and disappear. However, it is not confirmed," the post says in Russian translated to English for BleepingComputer by Advanced Intel's [Vitali Kremez](#).



LockBit forum post about REvil

Soon after, the XSS admin banned REvil's 'Unknown,' the public-facing representative of the ransomware gang, from the forum.

"As a rule of thumb, the administration of the top forums bans its users when they are suspected of being under the police control," explained Kremez.



The screenshot shows a forum profile for a user named 'Unknown'. A large red stamp with the word 'BANNED' is overlaid on the profile picture. The profile information includes: a 'Banned' status tag, a 'check in: 05/12/2019' timestamp, and 'Last Activity: Wednesday at 20:09'. Below this, statistics are shown: 'Posts: 100', 'Reactions: 218', and 'Deposit: 0.0022 ₿'. At the bottom, there are navigation tabs for 'Profile messages', 'Recent Activity', 'Content', 'Information', and 'Reactions'. Action buttons for 'Subscribe to', '+ To ignore', and 'To find' are also visible.

REvil's 'Unknown' banned from hacking forum

If you have first-hand information about the shut down, you can confidentially contact us on Signal at [+16469613731](tel:+16469613731) or on Wire at [@lawrenceabrams-bc](https://t.me/lawrenceabrams-bc).

Feeling the heat

On July 2nd, the REvil ransomware gang encrypted approximately 60 managed service providers (MSPs) and over 1,500 individual businesses using a zero-day vulnerability in the Kaseya VSA remote management software.

As part of these attacks, REvil initially demanded \$70 million for a universal decryptor for all victims but quickly dropped the price to \$50 million.

Since then, the ransomware group has been under increased scrutiny by law enforcement, which did not seem to faze 'Unknown,'

As these ransomware gangs commonly operate out of Russia, President Biden has been in talks with President Putin about the attacks and warned that if Russia did not act upon threat actors in their borders, the USA would take action themselves.

"I made it very clear to him that the United States expects when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is," Biden said after signing an executive order at the White House.

At this point, it is not clear if REvil's shut down of servers is for technical reasons, if the gang shut down their operation, or if a Russian or USA law enforcement operation took place.

Other ransomware groups, such as [DarkSide](#) and [Babuk](#), shut down voluntarily due to the increased pressure by law enforcement.

However, when ransomware groups shut down, the operators and affiliates commonly rebrand as a new operation to continue performing ransomware attacks. This was seen in the past when [GandCrab shut down](#) and many of its [members relaunching as REvil](#).

Babuk also [relaunched as Babuk v2.0](#) after the original group splintered due to differences in how attacks were conducted.

The FBI has declined to comment regarding the shut down of REvil's servers.

This is a developing story.

Update 7/13/21 6:31 PM EST: Added more information about hacking forums.

Related Articles:

[The Week in Ransomware - May 6th 2022 - An evolving landscape](#)

[Conti, REvil, LockBit ransomware bugs exploited to block encryption](#)

[REvil ransomware returns: New malware sample confirms gang is back](#)

[REvil's TOR sites come alive to redirect to new ransomware operation](#)

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

- [Law Enforcement](#)
- [Ransomware](#)
- [REvil](#)
- [Sodinokibi](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments



osct - 10 months ago

-
-

Biden had nothing to do with this. Stay on topic Don't bring politics in this group.



AlfaX - 10 months ago

-
-

"Biden had nothing to do with this. Stay on topic Don't bring politics in this group."

And you know that how? It would seem at this point, no one knows why the sites are down.



TsVkl! - 10 months ago

-
-

The US as a whole is exerting pressure on Russia to stop these attacks, nothing to do with politics. It's gone from harassing people for their pictures to bringing down critical infrastructure, which if was done by a state entity would be an act of war.

It can never be allowed to continue and will result in actual war if allowed to escalate.



[iwangchungeverynight](#) - 10 months ago

-
-

Politics interweaves everything done on this planet in how, when, and where business is conducted, to how public entities provide services, to the provisioning and procurement of goods and services for human survival. The moment the leader of one of the largest economies on the planet uttered the words 'cybersecurity', 'ransomware', and 'executive order', quite literally every single discussion about ransomware became political in nature. To ignore that reality is to avoid uncomfortable conversations but doesn't change the basic fact that everything has political undertones and is maneuvered by those waves of activity and power.



[nicecube](#) - 10 months ago

-
-

Good news, I hope they got pulled over by the Russian police.



[herbman](#) - 10 months ago

-
-

Contrary to what the media insist is the truth the overwhelming majority of cyber attacks are coming from China NOT Russia.

If you're one of those people that actually believe what the media report then you clearly don't have a clue to the truth but let me give you an example and the below is reported from the far left Guardian who eventually decided to come clean about who really colluded with Russia.

"It's Confirmed, John Brennan Colluded with Foreign Spies to Get Trump"

An article in the Guardian last week provides more proof that one side did collude with foreign powers and interfered in the election. It was Hillary's side.

Then-CIA director John Brennan was the ringleader. He colluded with foreign powers in a massive political espionage scheme to defeat Trump according to the Guardian.



I can't speak for malware in general, but I disagree when it comes to ransomware, which this article is about.

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
