REvil ransomware gang's web sites mysteriously shut down

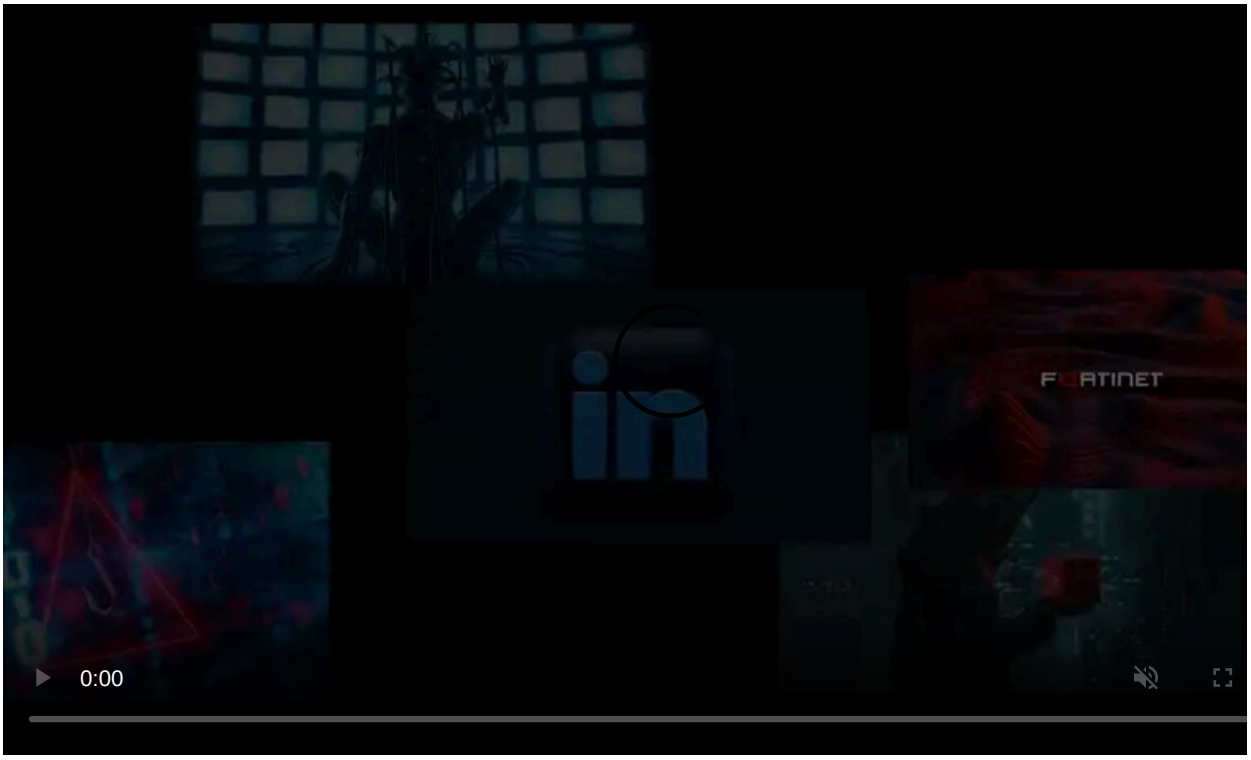
By Lawrence Abrams

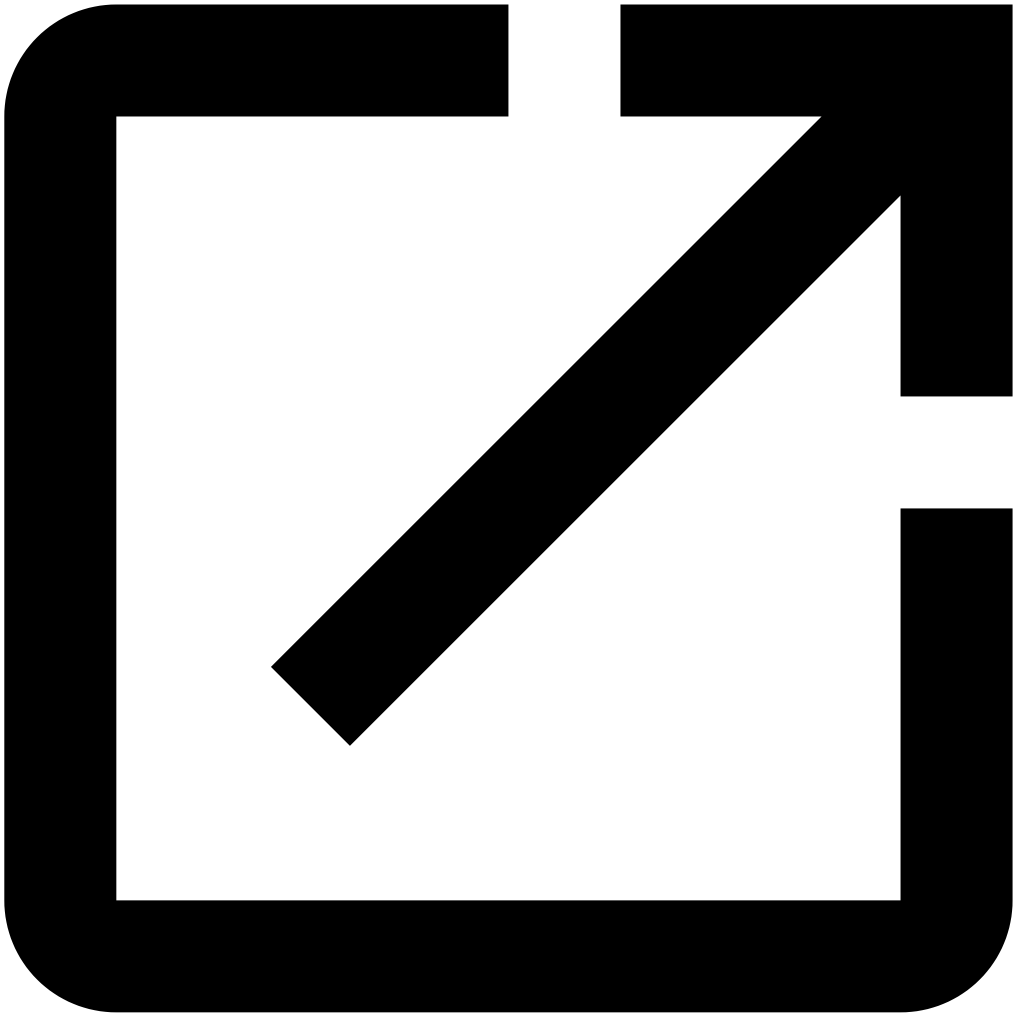
Published: 2021-07-13 · Archived: 2026-04-05 20:22:51 UTC

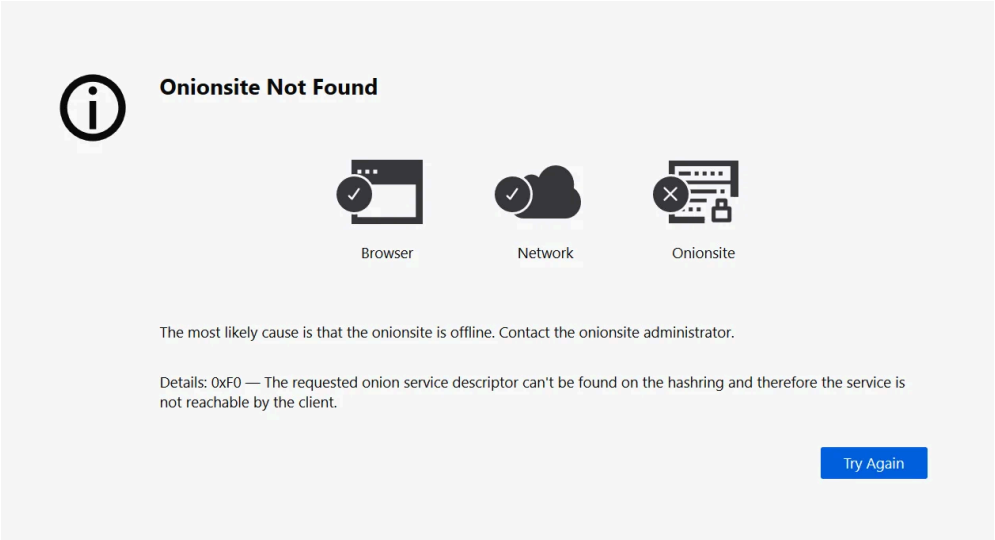
The infrastructure and websites for the REvil ransomware operation have mysteriously gone offline as of last night.

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.


FORTINET
0:00



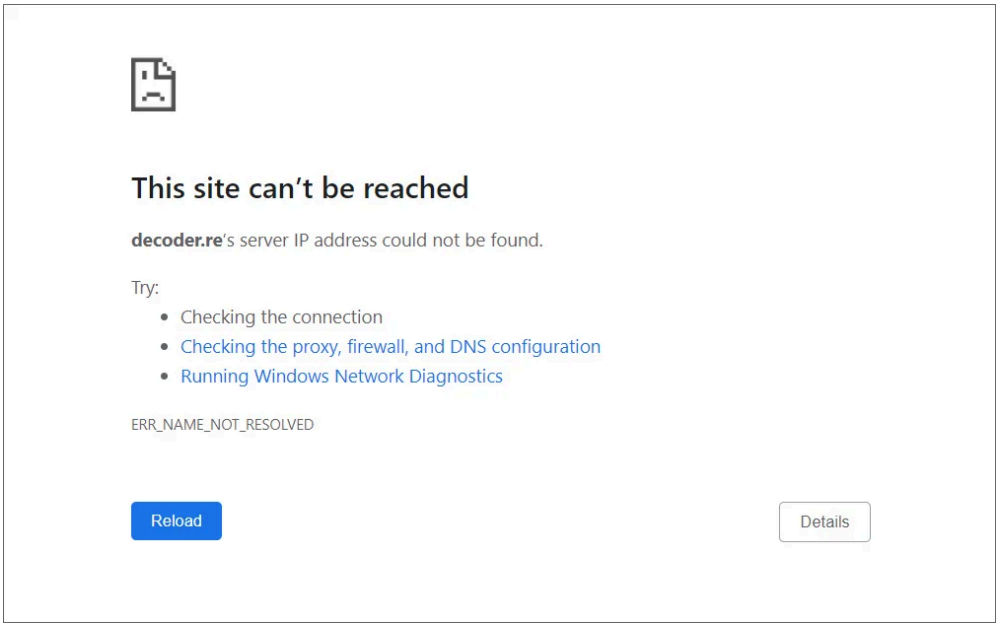


REvil Tor site no longer accessible

"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 Al 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.

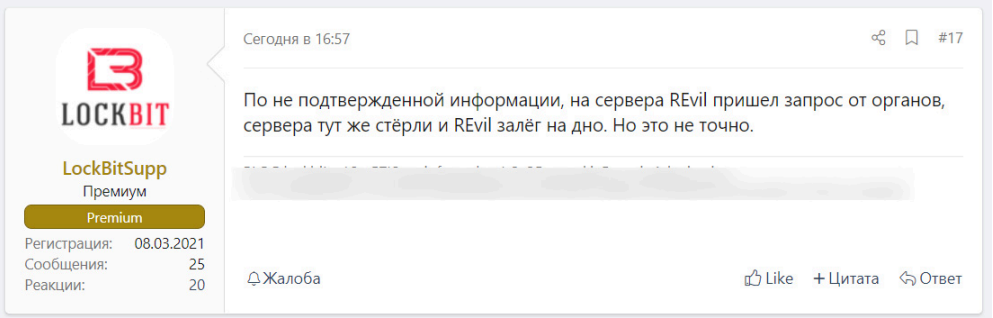


REvil domain no longer resolves to DNS queries

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.

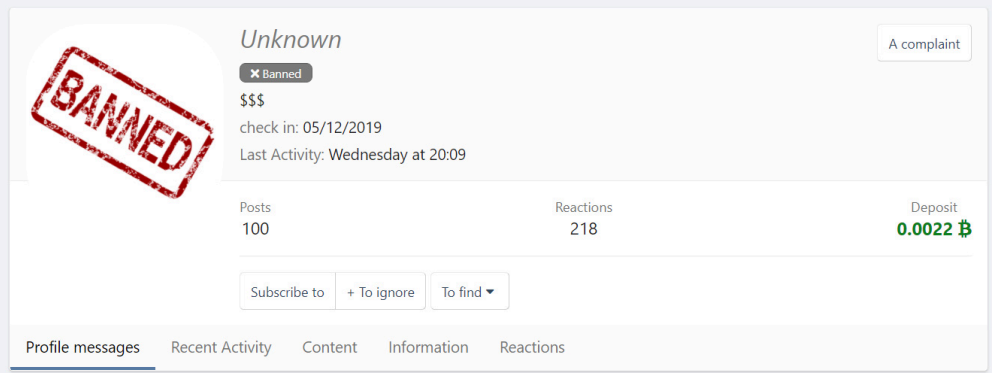
"Upon uncorroborated information, REvil server infrastructure received a government legal request forcing REvil to completely erase server infrastructure and disappear. However, it is not confirmed," the post says in Russian translated to English for BleepingComputer by Advanced Intel's Vitali Kremez.



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.



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 or on Wire at @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.

Source: https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/