REvil ransomware's servers mysteriously come back online

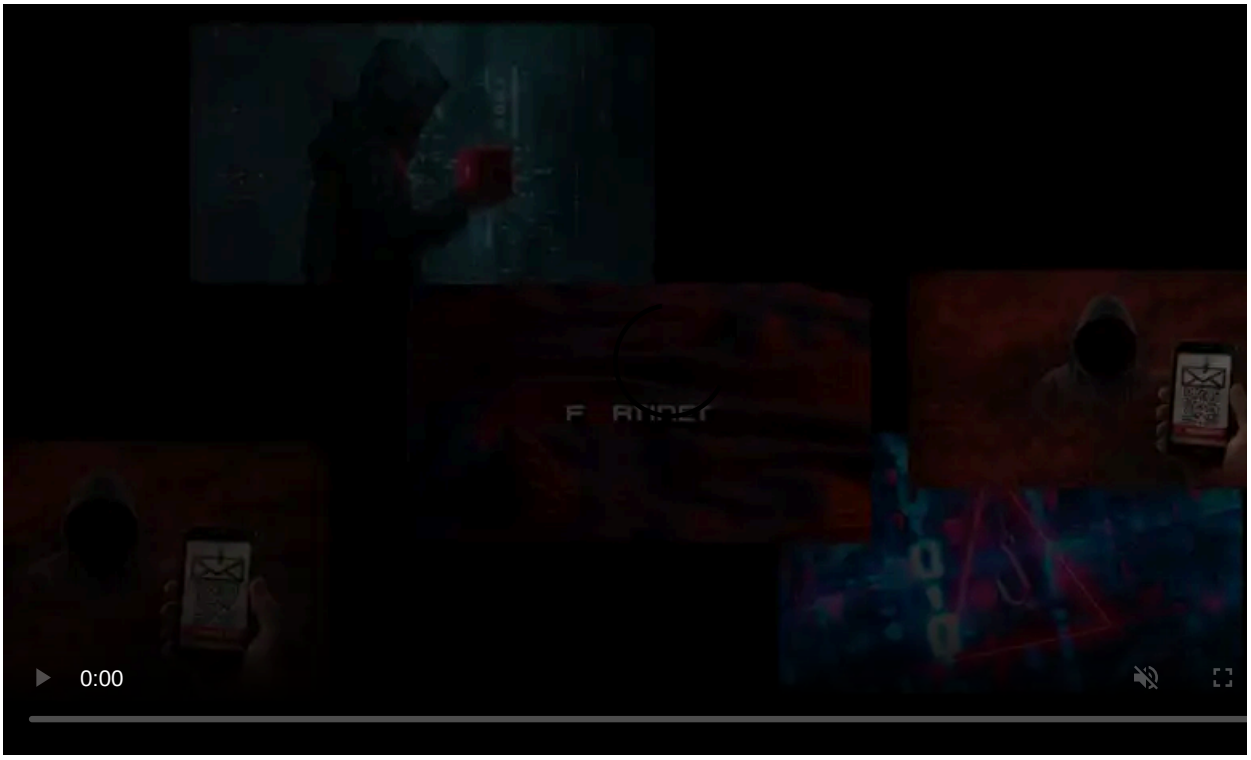
By Lawrence Abrams

Published: 2021-09-07 · Archived: 2026-04-05 22:32:31 UTC

The dark web servers for the REvil ransomware operation have suddenly turned back on after an almost two-month absence. It is unclear if this marks their ransomware gang's return or the servers being turned on by law enforcement.

On July 2nd, the REvil ransomware gang, aka Sodinokibi, used a zero-day vulnerability in the Kaseya VSA remote management software to encrypt approximately 60 managed service providers (MSPs) and over 1,500 of their business customers.

REvil then demanded $5 million from MSPs for a decryptor or $44,999 for each encrypted extension at the individual businesses.


0:00

The gang also demanded $70 million for a master decryption key to decrypt all Kaseya victims but soon dropped the price to $50 million.

After the attack, the ransomware gang faced increasing pressure from law enforcement and the White House, who warned that the USA would take action themselves if Russia did not act upon threat actors in their borders.

Soon after, the REvil ransomware gang disappeared, and all of their Tor servers and infrastructure were shut down.

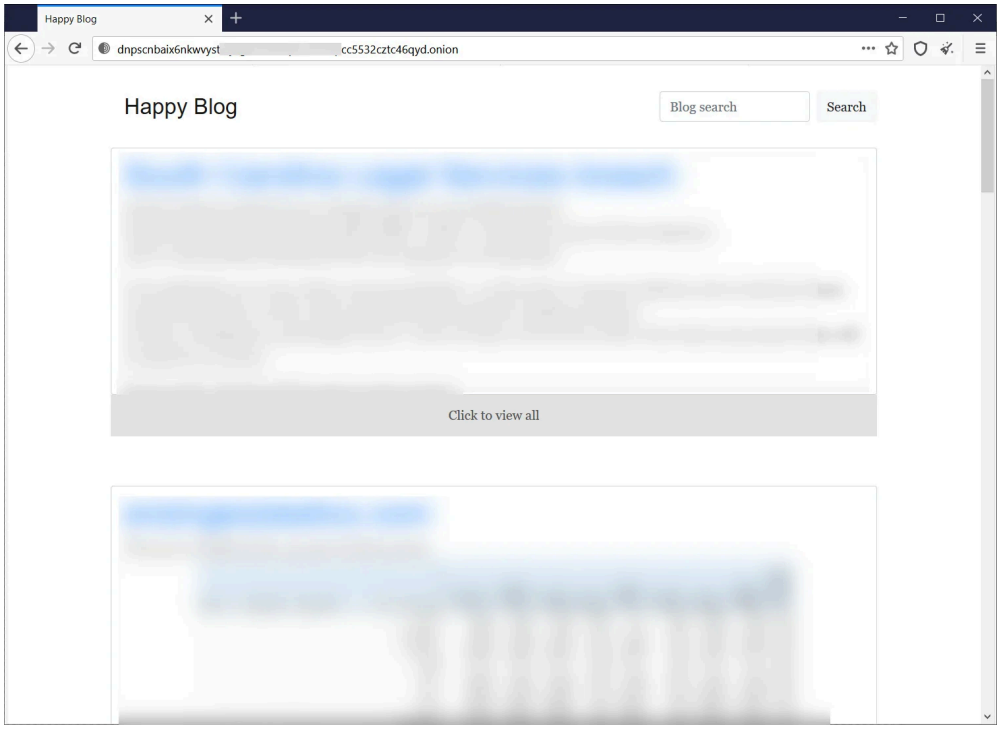
To this day, it is not clear what happened, but it left ransomware victims who wished to negotiate unable to do so and without the ability to restore files.

Mysteriously, Kaseya later received the master decryption key for the attack victims and stated it was from a trusted third party. It is believed that Russian intelligence received the decryption key from the threat actors and passed it along to the FBI as a gesture of goodwill.

REvil infrastructure suddenly turns back on

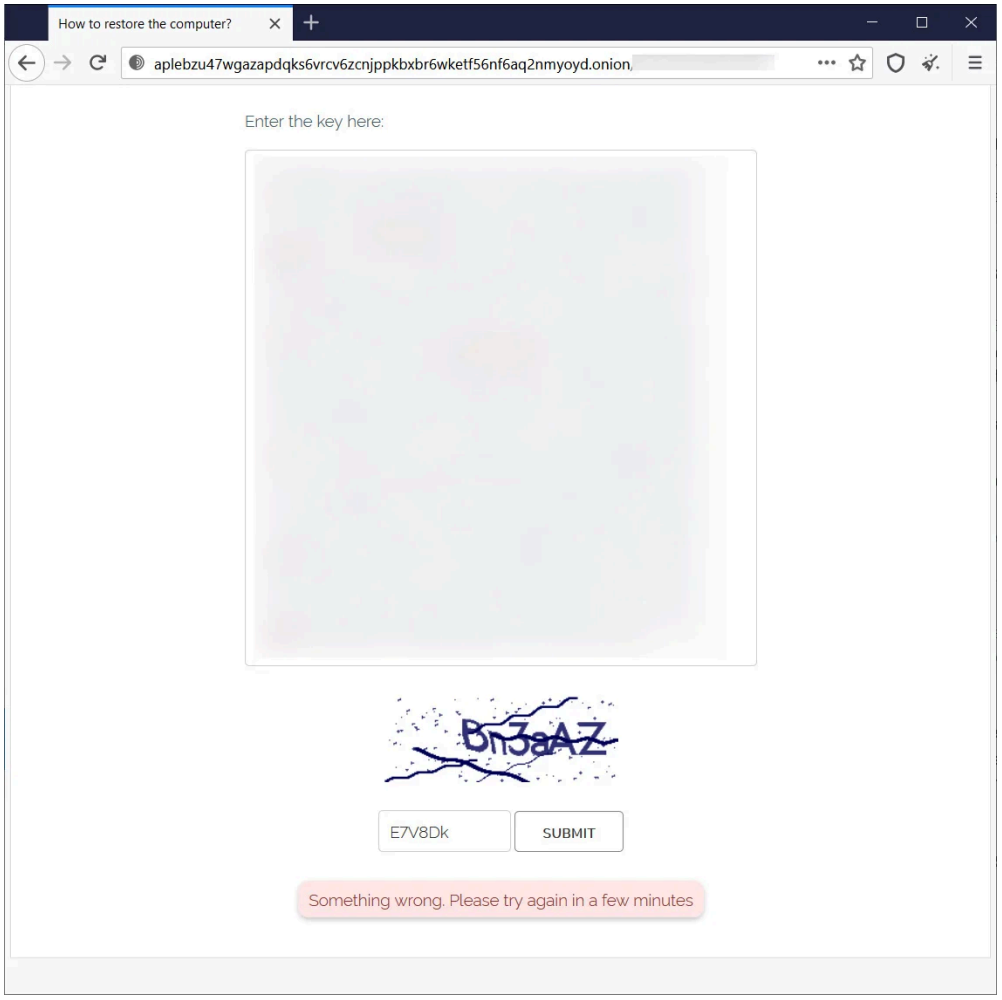
Today, both the Tor payment/negotiation site and REvil's Tor 'Happy Blog' data leak site suddenly came back online.

The most current victim on the REvil data leak site was added on July 8th, 2021, just five days before REvil's mysterious disappearance.



REvil's Happy Blog data leak site

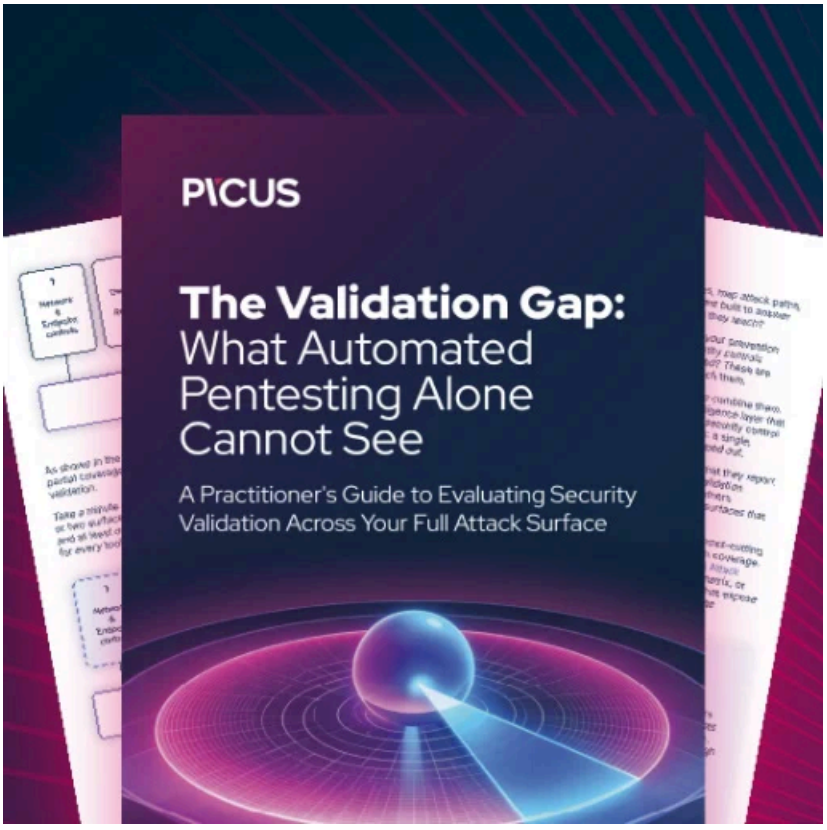
Unlike the data leak site, which is functional, the Tor negotiation site does not appear to be fully operational yet. While it shows the login screen, as seen below, it does not allow victims to log into the site.



REvil Tor negotiation site

The gang's http://decoder.re/ is still offline at this time.

It is unclear at this time whether the ransomware gang is back in operation, the servers have been turned back on by mistake, or it is due to the actions of law enforcement.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/