REvil ransomware is back in full attack mode and leaking data

By Lawrence Abrams

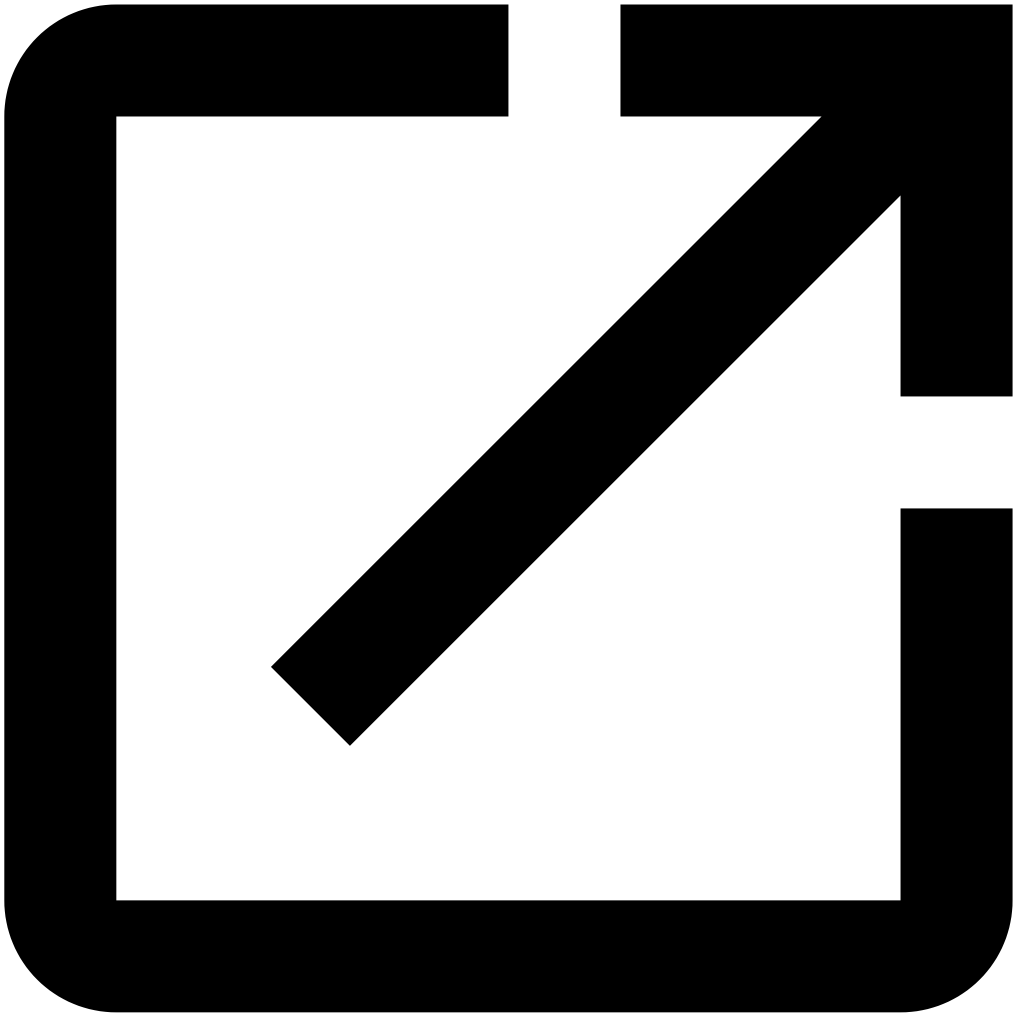
Published: 2021-09-11 · Archived: 2026-04-05 13:22:16 UTC

The REvil ransomware gang has fully returned and is once again attacking new victims and publishing stolen files on a data leak site.

Since 2019, the REvil ransomware operation, aka Sodinokibi, has been conducting attacks on organizations worldwide where they demand million-dollar ransoms to receive a decryption key and prevent the leaking of stolen files.

While in operation, the gang has been involved in numerous attacks against well-known companies, including JBS, Coop, Travelex, GSMLaw, Kenneth Cole, Grupo Fleury, and others.

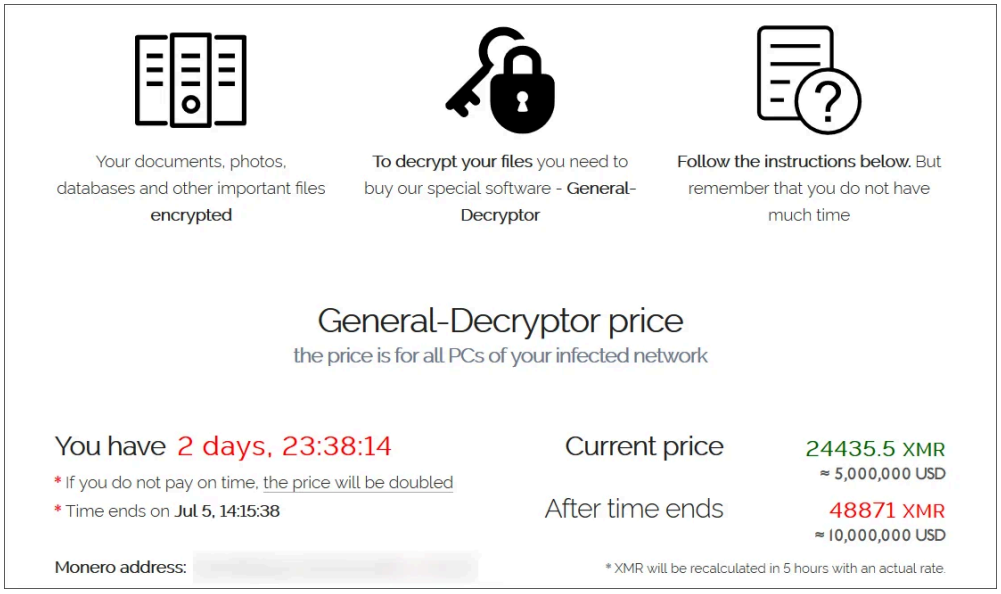

DIE LINKE.
0:00



REvil's disappearance act

REvil shut down their infrastructure and completely disappeared after their biggest caper yet - a massive attack on July 2nd that encrypted 60 managed service providers and over 1,500 businesses using a zero-day vulnerability in the Kaseya VSA remote management platform.

REvil then demanded $50 million for a universal decryptor for all Kaseya victims, $5 million for an MSP's decryption, and a $44,999 ransom for individual file encryption extensions at affected businesses.



REvil ransom demand for an encrypted MSP

This attack had such wide-ranging consequences worldwide that it brought the full attention of international law enforcement to bear on the group.

Likely feeling pressure and concerns about being apprehended, the REvil gang suddenly shut down on July 13th, 2021, leaving many victims in a lurch with no way of decrypting their files.

The last we had heard of REvil, was that Kaseya received a universal decryptor that victims could use to decrypt files for free. It is unclear how Kaseya received the decryptor but stated it came from a "trusted third party."

REvil returns with new attacks

After their shutdown, researchers and law enforcement believed that REvil would rebrand as a new ransomware operation at some point.

However, much to our surprise, the REvil ransomware gang came back to life this week under the same name.

On September 7th, almost two months after their disappearance, the Tor payment/negotiation and data leak sites suddenly turned back on and became accessible. A day later, it was once again possible to log in to the Tor payment site and negotiate with the ransomware gang.

All prior victims had their timers reset, and it appeared that their ransom demands were left as they were when the ransomware gang shut down in July.

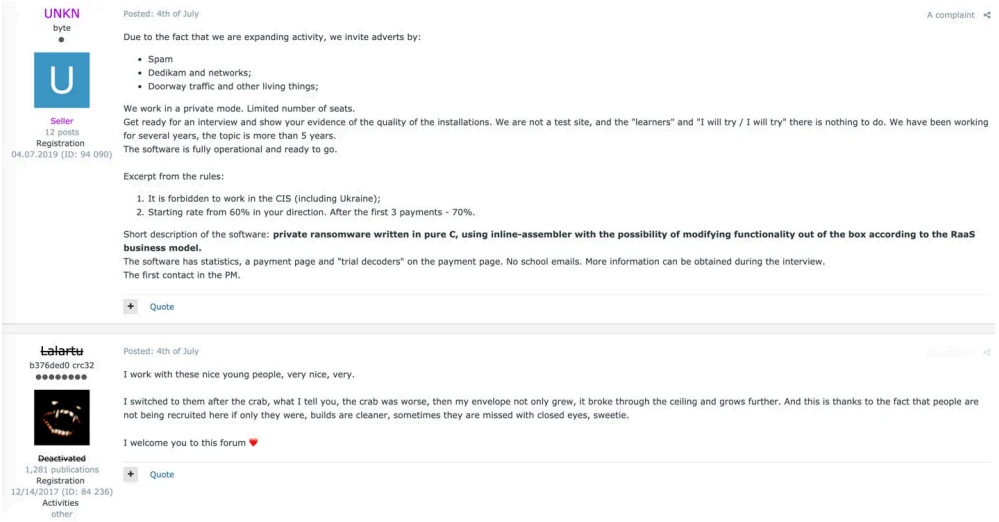
However, there was no proof of new attacks until September 9th, when someone uploaded a new REvil ransomware sample compiled on September 4th to VirusTotal.

Today, we have seen further proof of their renewed attacks as the ransomware gang has published screenshots of stolen data for a new victim on their data leak site.

If you have first-hand information about REvil's return, you can confidentially contact us on Signal at +16469613731, Wire at @lawrenceabrams-bc, or Jabber at lawrence.abrams@anonym.im.

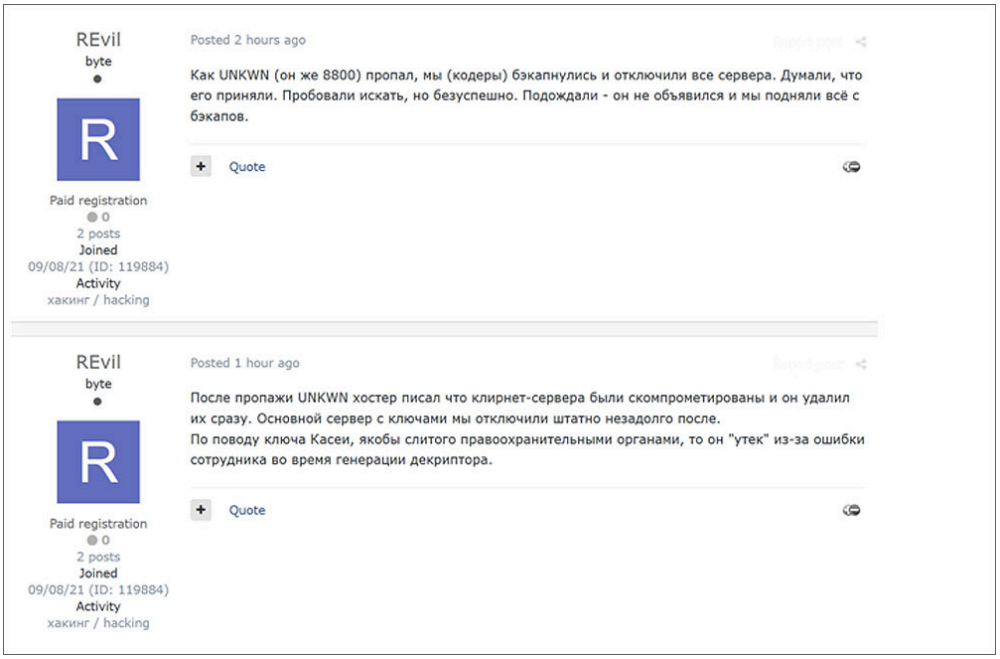
New REvil representative emerges

In the past, REvil's public representative was a threat actor known as 'Unknown' or 'UNKN,' who frequently posted at hacking forums to recruit new affiliates or post news about the ransomware operation.



Forum post by REvil's UNKN

On September 9th, after the return of the ransomware operation, a new representative simply named 'REvil' had begun posting at hacking forums claiming that the gang briefly shut down after they though Unknown was arrested and servers were compromised.



REvil post to Russian-speaking hacking forum
Source: Advanced Intel

This translation of these posts can be read below:

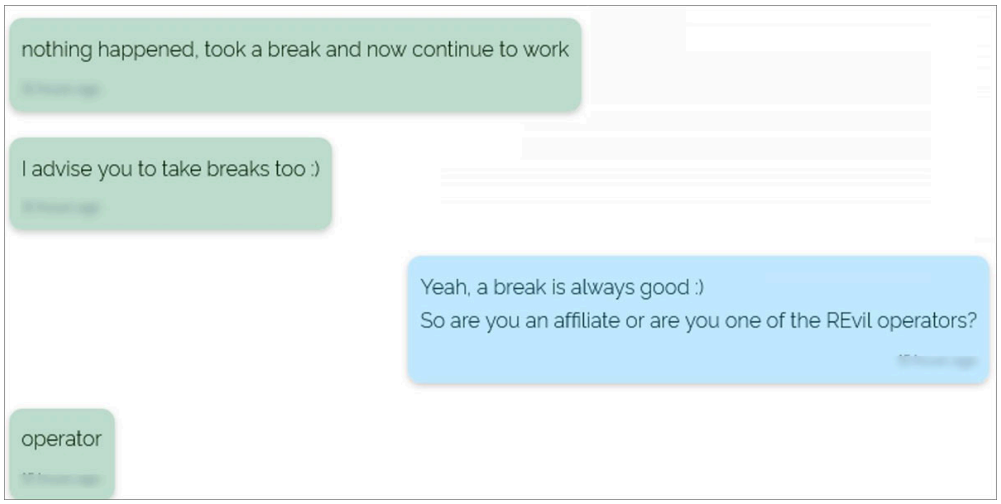
> "As Unknown (aka 8800) disappeared, we (the coders) backed up and turned off all the servers. Thought that he was arrested. We tried to search, but to no avail. We waited - he did not show up and we restored everything from backups.

> After UNKWN disappeared, the hoster informed us that the Clearnet servers were compromised and they deleted them at once. We shut down the main server with the keys right afterward.
>
> Kaseya decryptor, which was allegedly leaked by the law enforcement, in fact, was leaked by one of our operators during the generation of the decryptor." - REvil

Based on these claims, Kaseya's universal decryptor was obtained by law enforcement after they gained access to some of REvil's servers.

However, BleepingComputer has been told by numerous sources that REvil's disappearance surprised law enforcement as much as everyone else.

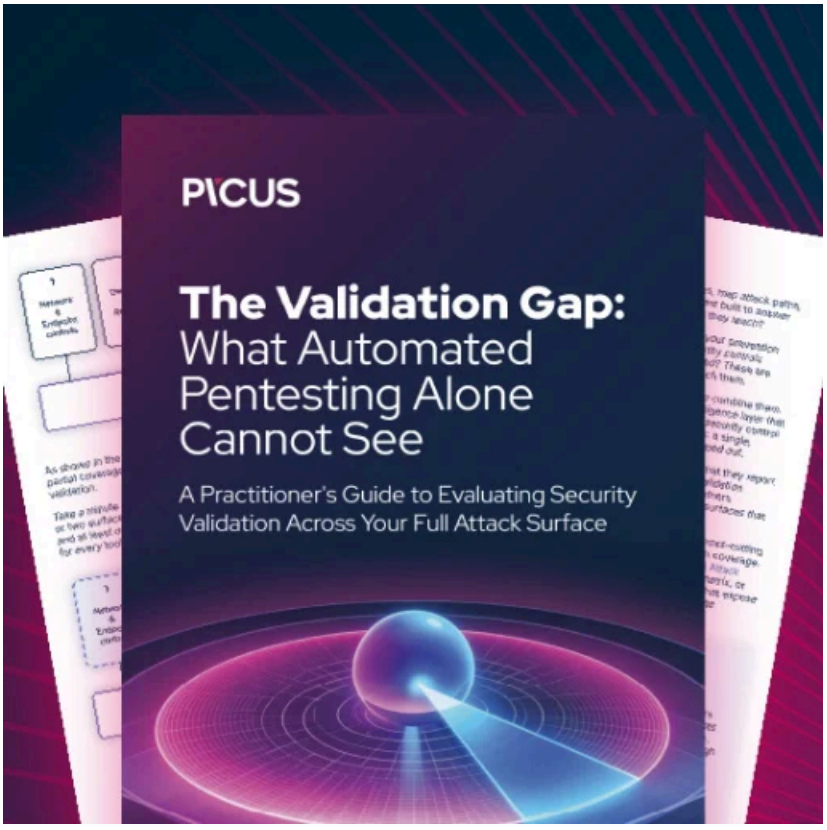
A chat between what is believed to be a security researcher and REvil, paints a different story, with an REvil operator claiming they simply took a break.



Chat between a researcher and REvil about their disappearance

While we may never know the real reason for the disappearance or how Kaseya obtained the decryption key, what is most important is to know that REvil is back to targeting corporations worldwide.

With their skilled affiliates and ability to perform sophisticated attacks, all network admins and security professionals must become familiar with their tactics and techniques.



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-ransomware-is-back-in-full-attack-mode-and-leaking-data/