REvil ransomware shuts down again after Tor sites were hijacked

By Lawrence Abrams

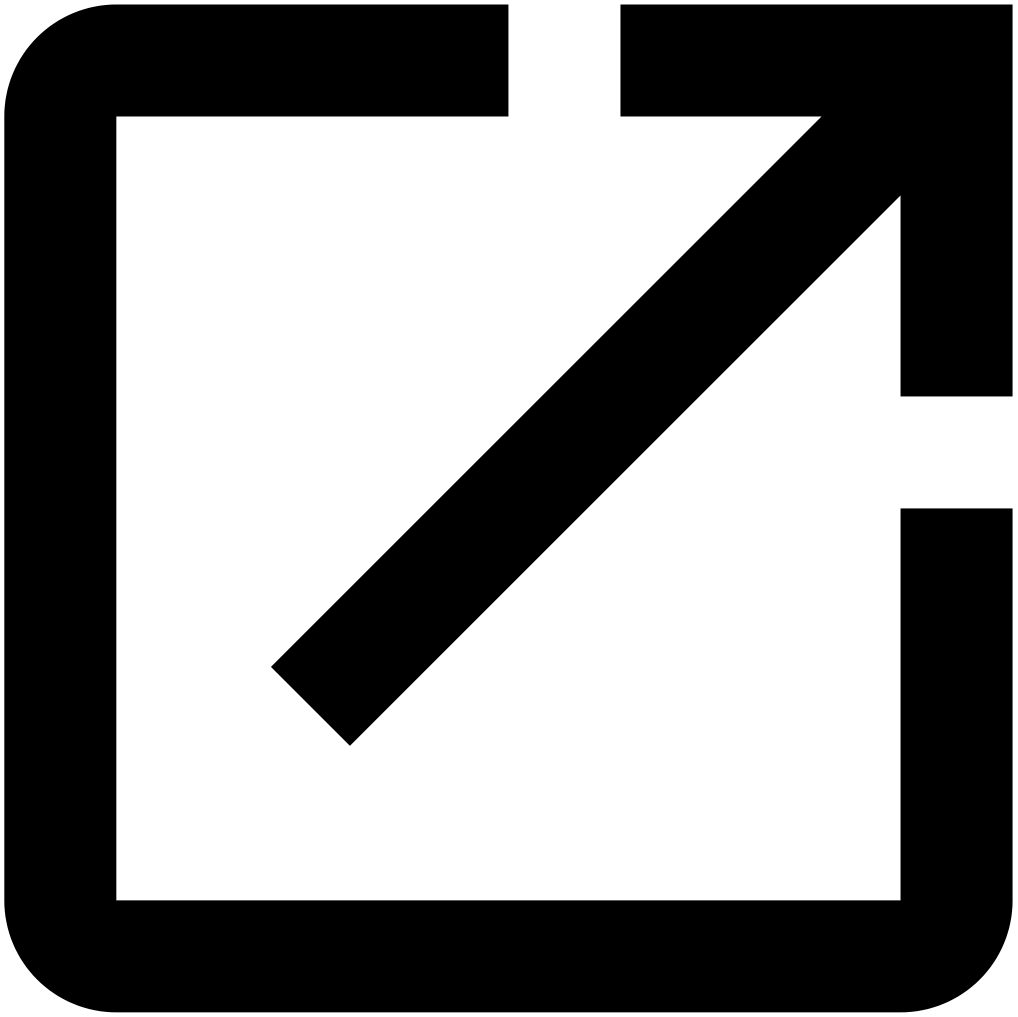
Published: 2021-10-17 · Archived: 2026-04-05 14:38:45 UTC

The REvil ransomware operation has likely shut down once again after an unknown person hijacked their Tor payment portal and data leak blog.

The Tor sites went offline earlier today, with a threat actor affiliated with the REvil operation posting to the XSS hacking forum that someone hijacked the gang's domains.

The thread was first discovered by Recorded Future's Dmitry Smilyanets, and states that an unknown person hijacked the Tor hidden services (onion domains) with the same private keys as REvil's Tor sites and likely has backups of the sites.

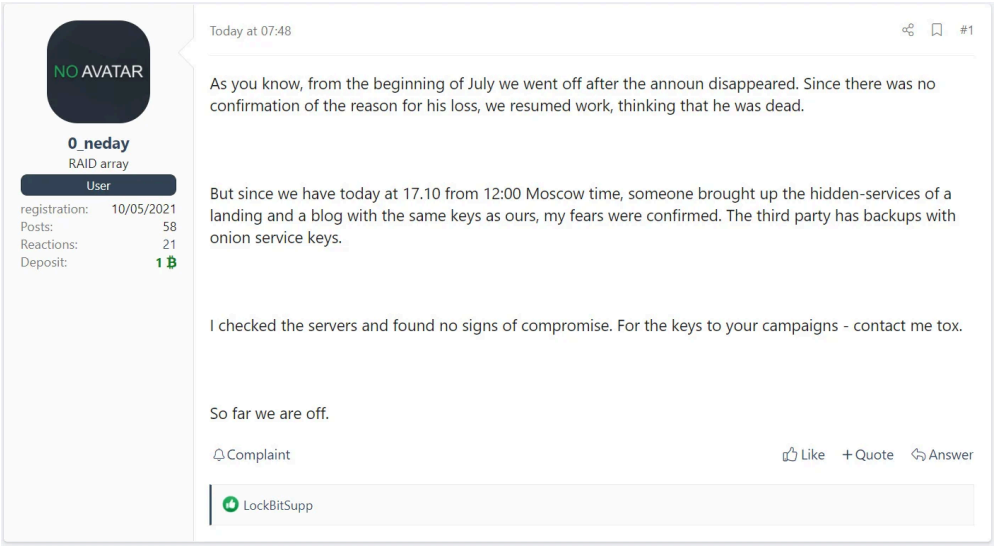

DIE LINKE.
0:00



"But since we have today at 17.10 from 12:00 Moscow time, someone brought up the hidden-services of a landing and a blog with the same keys as ours, my fears were confirmed. The third party has backups with onion service keys," a threat actor known as '0_neday' posted to the hacking forum.

The threat actor went on to say that they found no signs of compromise to their servers but will be shutting down the operation.

The threat actor then told affiliates to contact him for campaign decryption keys via Tox, likely so affiliates could continue extorting their victims and provide a decryptor if a ransom is paid.



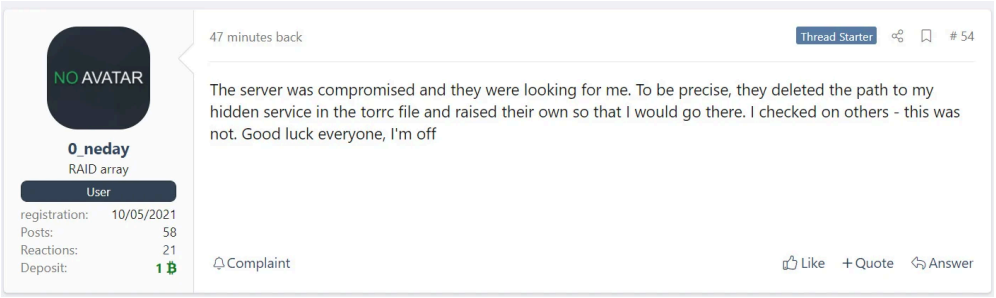
XSS forum topic about REvil sites being hijacked

To launch a Tor hidden service (an .onion domain), you need to generate a private and public key pair, which is used to initialize the service.

The private key must be secured and only accessible to trusted admins, as anyone with access to this key could use it to launch the same .onion service on their own server.

As a third party was able to hijack the domains, it means they too have access to the hidden service's private keys.

This evening, 0_neday once again posted to the hacking forum topic, but this time saying that their server was compromised and that whoever did it was targeting the threat actor.



Forum post stating the REvil server was compromised

At this time, it is unknown who compromised their servers.

As Bitdefender and law enforcement gained access to the master REvil decryption key and released a free decryptor, some threat actors believe that the FBI or other law enforcement have had access to the servers since they relaunched.

As no one knows what happened to Unknown, it is also possible that the threat actor is trying to regain control over the operation.

REvil likely shut down for good

After REvil conducted a massive attack on companies through a zero-day vulnerability in the Kaseya MSP platform, the REvil operation suddenly shut down, and their public-facing representative, Unknown, disappeared.

After Unknown did not return, the rest of the REvil operators launched the operation and websites again in September using backups.

Since then, the ransomware operation has been struggling to recruit users, going as far as to increase affiliate's commissions to 90% to entice other threat actors to work with them.

With this latest mishap, the operation in its current forum will likely be gone for good.

However, no good thing lasts forever when it comes to ransomware, and we will likely see them rebrand as a new operation shortly.

Thx to @_TheEmperors_ for the tip!
