REvil's TOR sites come alive to redirect to new ransomware operation

By Ionut Ilascu

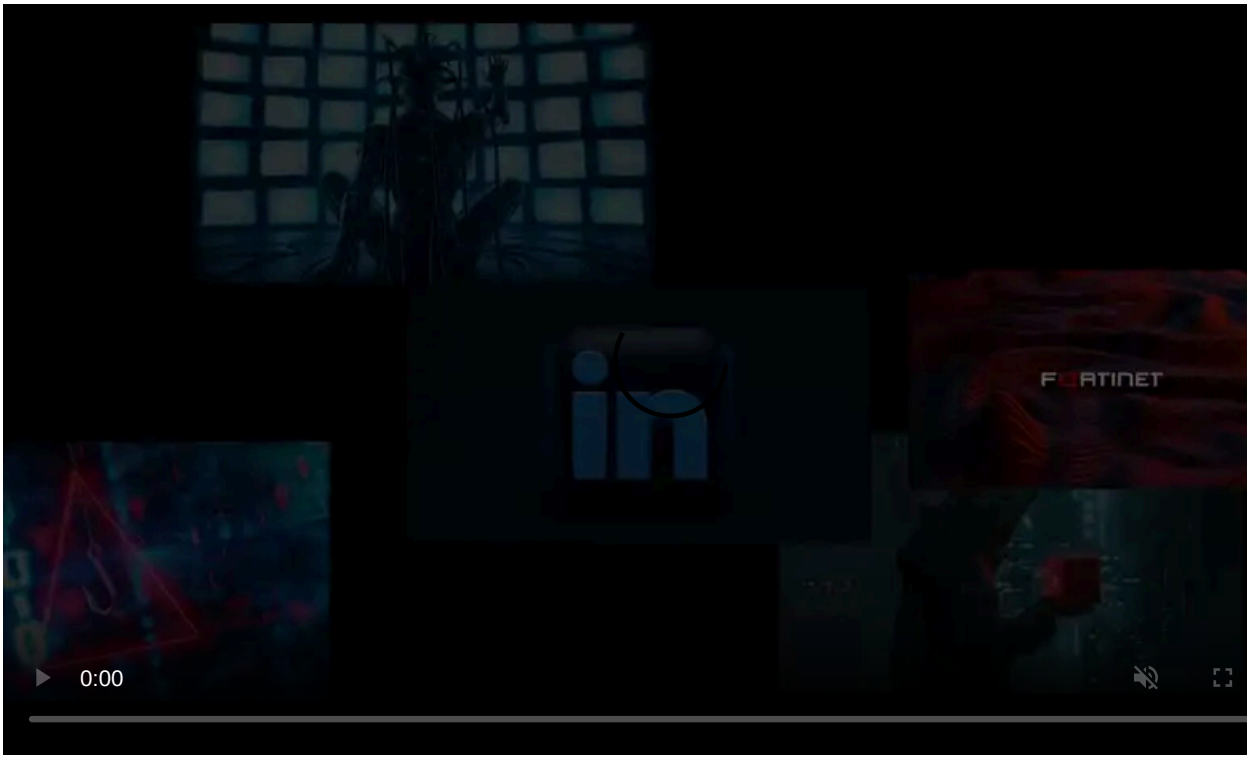
Published: 2022-04-20 · Archived: 2026-04-05 19:14:32 UTC

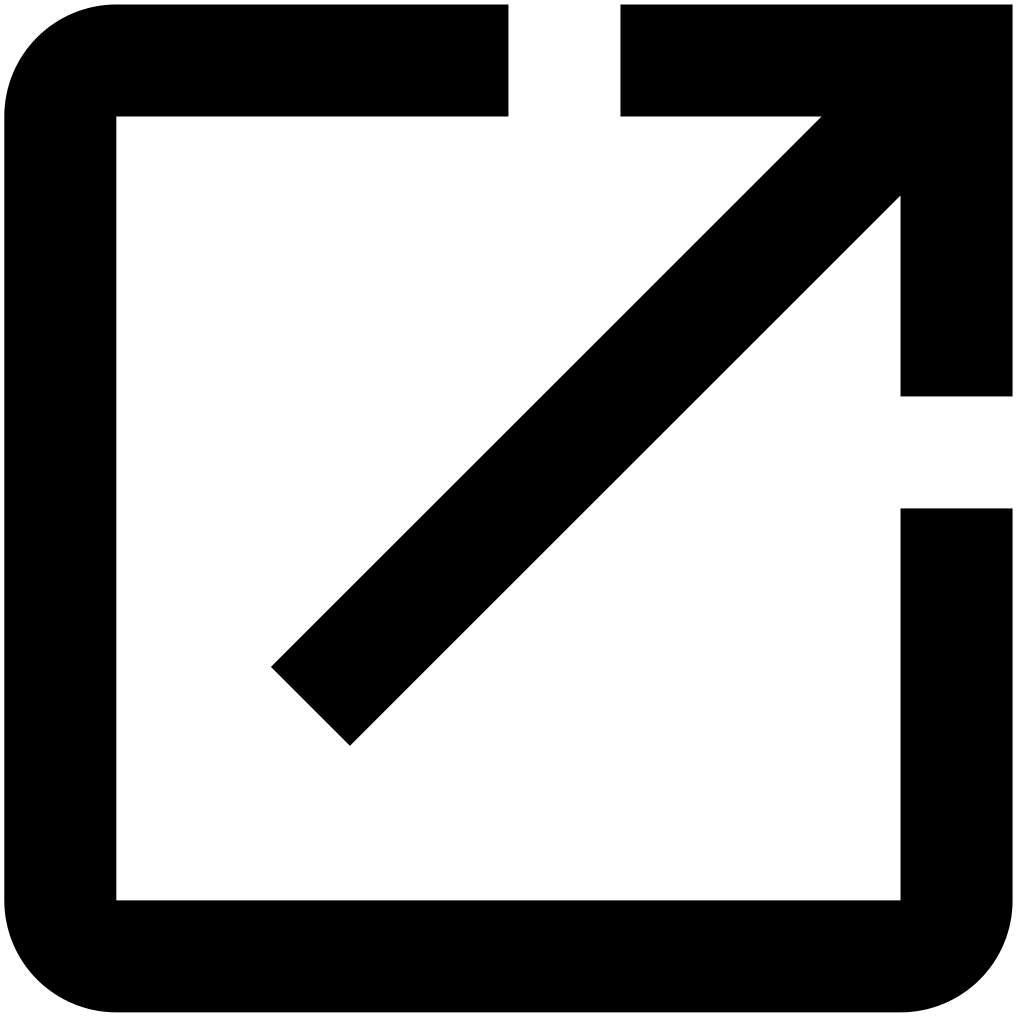
REvil ransomware's servers in the TOR network are back up after months of inactivity and are now redirecting to a new operation that launched recently.

It is unclear who is behind the new REvil-connected operation, but the new leak site lists a large catalog of victims from past REvil attacks, plus two new ones.

New RaaS in the making

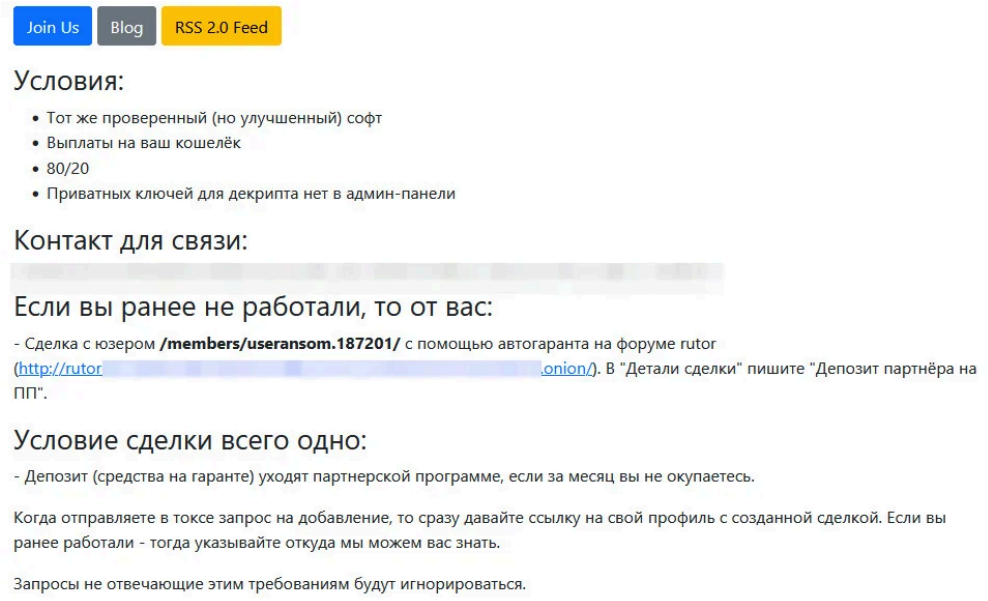
A few days ago, security researchers pancak3 and Soufiane Tahiri noticed a new ransomware operation promoted on RuTOR, a forum marketplace focusing on Russian-speaking regions.


0:00



The promotion included a link to a new Tor data leak site that contained information on how to join the group as an affiliate, claiming to be "The same proven (but improved) software."

This leak site, shown below, provides details on how to become an affiliate and who allegedly gets an improved version of REvil ransomware and an 80/20 split for affiliates collecting a ransom.



source: BleepingComputer

Security researcher MalwareHunterTeam observed this same leak site between April 5 and April 10 but with no content. However, a few days later, the researcher saw it become populated with a mixture of old REvil victims' data and some new victims.

The site lists 26 pages of victims, most of them from old REvil attacks, and just the last two appear to be related to the new operation. One of them is Oil India.

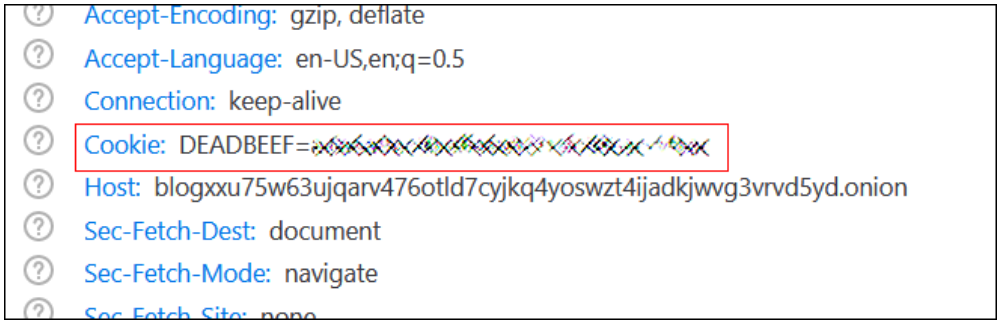
Today, we received proof that this new operation is tied to REvil, as REvil's original Tor sites are now redirecting to this new operation's data leak site, as illustrated by security researchers and independently confirmed by BleepingComputer.

Another observation from MalwareHunterTeam is that the source for the new operation's RSS feed shows the string Corp Leaks, which has been used by the now-defunct Nefilim ransomware gang [1, 2].

source: BleepingComputer

The new operation's blog and payment sites are up and running on different servers.

Looking at the former, BleepingComputer noticed that the new ransomware operation's blog drops a cookie named DEADBEEF, a computer term that was also used as a filemarker by the TeslaCrypt ransomware gang.



source: BleepingComputer

Other than the redirects, a connection to a ransomware threat actor is impossible as samples of the new REvil-based payload have to be analyzed, and whoever is behind the new leak site has not claimed any name or affiliation yet.

To make it more confusing, multiple ransomware operations now use patched REvil encryptors or are linked to the original group in some manner.

MalwareHunterTeam tweeted in January that another ransomware gang launched in December 2021 named Ransom Cartel, also related to REvil's encryptor.

In addition to Ransom Cartel, another group known as LV has been patching REvil's encryptor for some time to encrypt victims using their own encryption keys.

Mysterious case of redirects

While under the control of the FBI in November 2021, REvil's data leak and payment sites began showing a page titled "*REvil is bad*" and a login form. These pages were initially only shown when accessing the page via TOR gateways, but later at the .onion URL as well.

The mystery of the recent redirects deepens, as this suggests that someone other than law enforcement has access to the TOR private keys that allowed them to make changes for the .Onion site.

On a popular Russian-speaking hacker forum, users are speculating between the new operation being a scam, a honeypot, or a legit continuation of the old REvil business that lost its reputation and has a lot to do to earn it back.

REvil's fall

REvil ransomware's long run started in April 2019 as a continuation of the GandCrab operation, the first that established the ransomware-as-a-service (RaaS) model.

In August 2019, the gang hit multiple local administrations in Texas and demanded a collective ransom of $2.5 million - the highest at that time.

The group is responsible for the Kaseya supply-chain attack that affected about 1,500 businesses. However, this massive attack also led to their demise as law enforcement worldwide intensified their collaboration to bring the gang down.

Soon after hitting Kaseya, the gang took a two-month break, not knowing that law enforcement agencies had breached their servers. When REvil restarted the operation, they restored systems from backups, oblivious of the compromise.

In mid-January, Russia announced that it shut down REvil after identifying all of the operation's members and arrested 14 individuals.

“As a result of the joint actions of the FSB and the Ministry of Internal Affairs of Russia, the organized criminal community ceased to exist, the information infrastructure used for criminal purposes was neutralized” Russia’s Federal Security Service

In an interview with Rossiyskaya Gazeta, the Deputy Secretary of the Security Council of the Russian Federation, Oleg Khramov, said that the Russian law enforcement agency started its investigation into REvil after the name 'Puzyrevsky' and

an IP address was shared by the United States.

At the moment, the U.S. has stopped collaborating with Russia on cybersecurity threats - attacks on critical infrastructure in particular, as a direct result of Russia invading Ukraine.

Update (April 21): Article updated to make it clear that the ransomware gang redirecting from the original REvil leak site to the new one appears to be different from other groups that used a patched REvil payload in the past, and that the redirect was observed on April 20.
Update (10/15/22): Parts of article rewritten to make it clearer.

Source: https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/