BLEEPINGCOMPUTER

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

By Ionut Ilascu

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

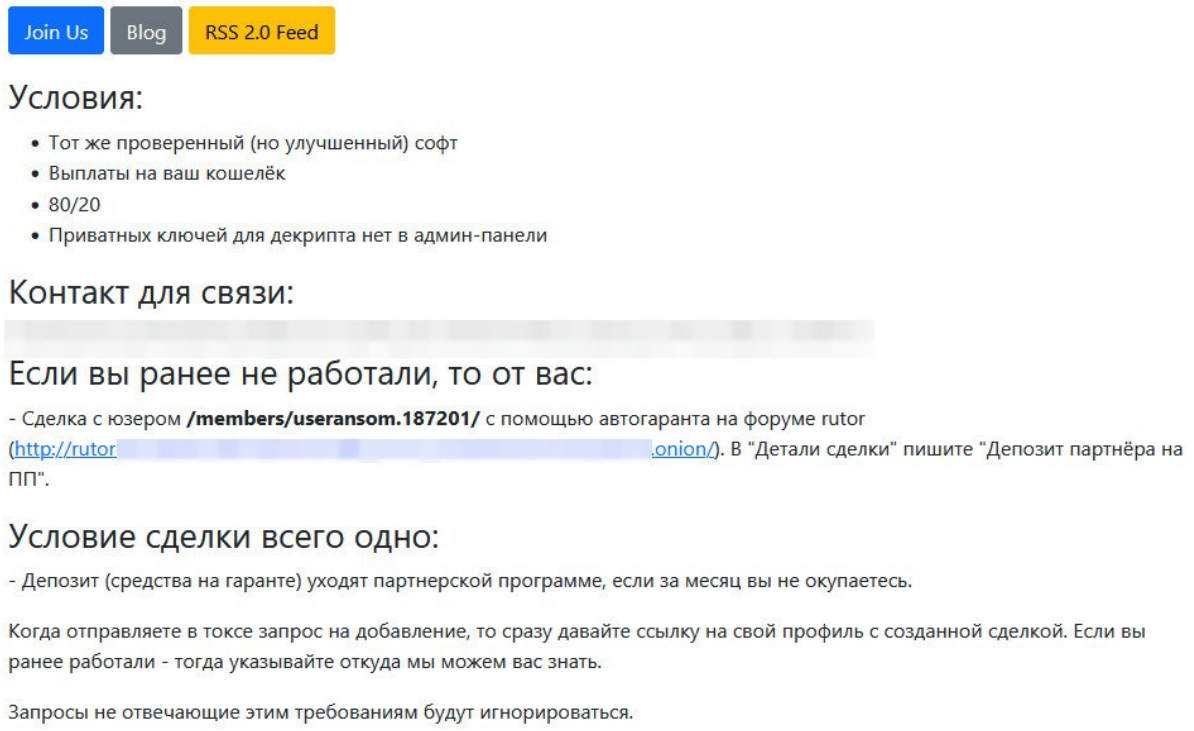
It is unclear who is behind the new REvil-connected operation but the new leak site lists a large catalog of victims from past REvil attacks plus two new ones.

New RaaS in the making

A few days back, however, security researchers pancak3 and Soufiane Tahiri noticed the new REvil leak site being promoted on RuTOR, a forum marketplace that focuses on Russian-speaking regions.

The new site is hosted on a different domain but leads to the original one REvil used when active, BleepingComputer confirmed today, while the two researchers captured the redirect.

The leak site provides details on the conditions for affiliates, who allegedly get an improved version of REvil ransomware and an 80/20 split for affiliates collecting a ransom.



source: BleepingComputer

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.

Security researcher MalwareHunterTeam in January, a couple of weeks after 14 alleged members of the gang were arrested in Russia, said that starting mid-December last year they noticed activity from a a different ransomware gang (Ransom Cartel) that was related to REvil's encryptor, although no connection was evident.

source: MalwareHunterTeam

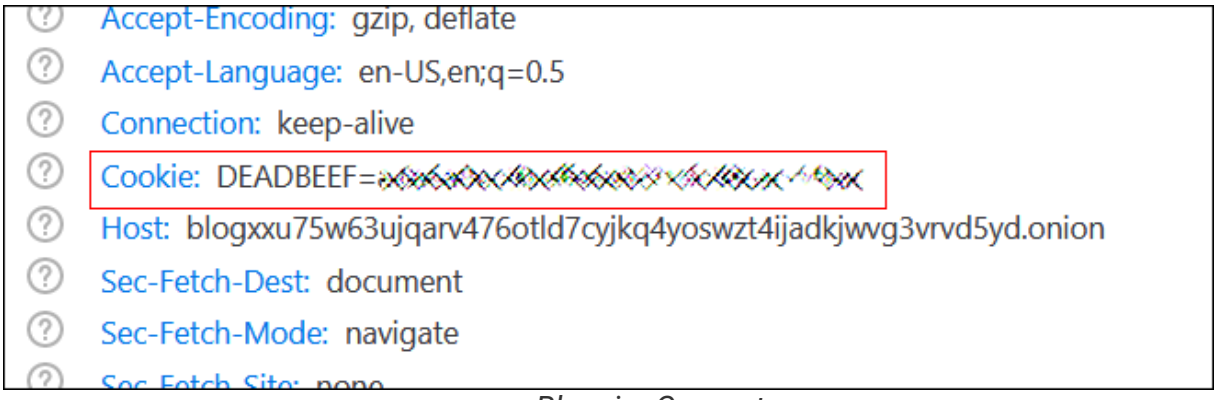
The researcher later observed the current REvil-related leak site being up between April 5 and April 10 but with no content and it started to be populated about a week after.

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

```
−<rss version="2.0">
  −<channel>
      <title>Corp Leaks</title>
      <description/>
      <copyright> 2022</copyright>
      <generator>AwesomeSoftware Name</generator>
      <a10:link title="CorpLeaks.com" href="https://corpleaks.com/"/>
    −<item>
       <guid isPermaLink="false">d300ab07-28e5-4fc0-b400-0a493354044a</guid>
      −<link>
          https://corpleaks.com/DirectLink/d300ab07-28e5-4fc0-b400-0a493354044a
       </link>
```

source: BleepingComputer

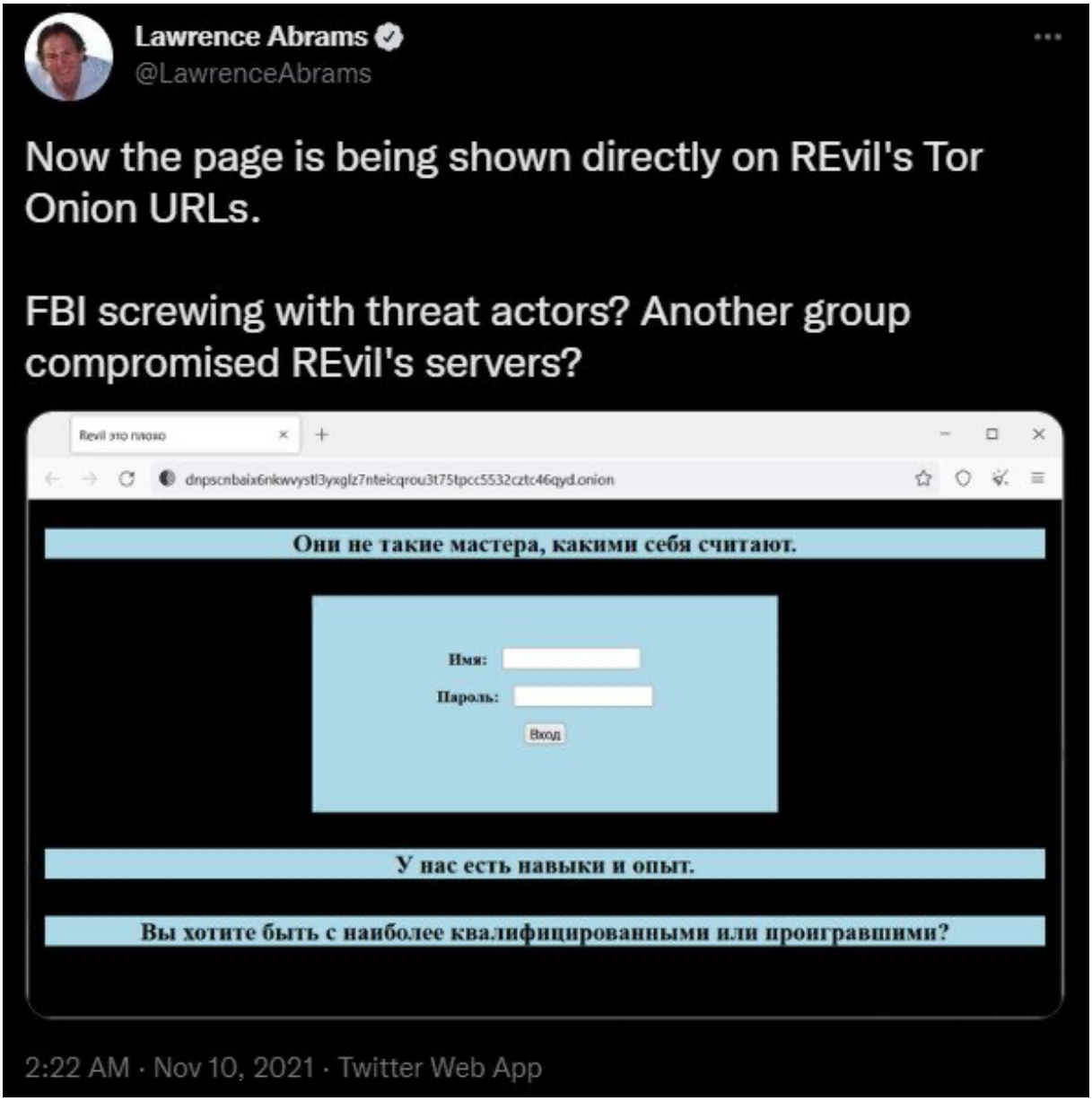
The blog and payment sites are up and running on different servers. Looking at the former, BleepingComputer noticed that the new ransomware operation's blog drops a cookie named DEADBEEF, a computer term that was used as a filemarker by the TeslaCrypt ransomware gang.



source: BleepingComputer

A connection to a ransomware threat actor is not possible at this time 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.

While under control of the FBI in November 2021, REvil's data leak and payment sites showed a page titled "*REvil is bad*" and a login form, initially via TOR gateways and at the .Onion location.



source: *Lawrence Abrams*

The mystery of the redirects, both recent and from last year, 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.

There are multiple ransomware operations that either use patched REvil encryptors or are impersonating the original group.

These include LV, which was using REvil's encryptor before law enforcement shut them down and Ransom Cartel, which appears to be connected to REvil but the link is unclear.

REvil's fall

REvil ransomware had a long run that 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 and also led to their demise last year as law enforcement around the world 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 members of the gang and arresting 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 from the name Puzyrevsky and an IP address transmitted by the United States as belonging to the group's main hacker.

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.