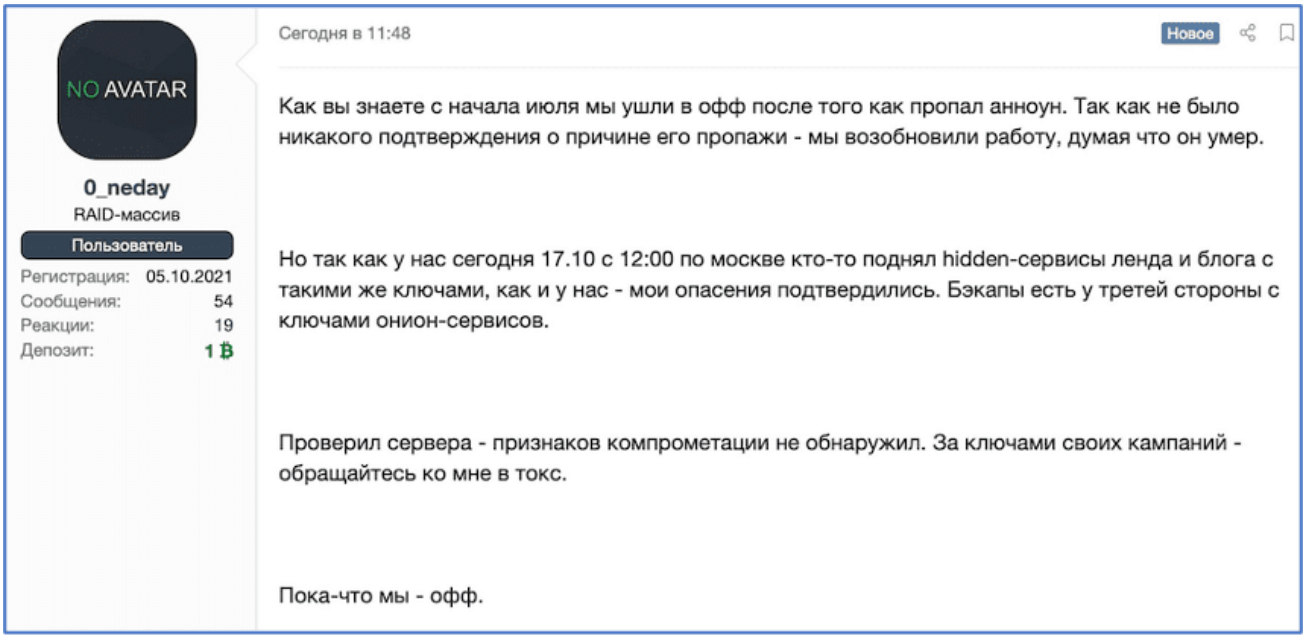
“Page Not Found”: REvil Darknet Services Offline After Attack Last Weekend

darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend

October 20, 2021

Last weekend, REvil’s “Happy Blog” went offline for the second time in less than six months. Instead of the blog Tor service simply not responding to an HTTP request, the page instead displayed the default 404 error displayed by the nginx webserver. According to a REvil representative the ransomware-as-a-service (RaaS) organization’s Tor domain was “hijacked” using the private keys of the domain held by REvil’s previously public-face “Unknown” (who also operates as “UNKN”).

DarkOwl reviewed the group’s history and latest posts about the hijacking and determined that since returning, REvil’s reputation was in jeopardy and many darknet users and RaaS community members suspected the group had been compromised by the FBI.



“This Page Is Not Found”

Last weekend, Tor users anticipating to connect to the legendary Happy Blog hosted by the infamous REvil RaaS gang, received the default 04 error page for nginx webservers on Fedora, indicating the Tor onion services run by the REvil operation were compromised and corrupted instead of simply taken offline by disconnecting the servers from the network.

The page read:

```
"nginx error! The page you are looking for is not found. Website Administrator
Something has triggered missing webpage on your website. This is the default 404
error page for nginx that is distributed with Fedora. It is located
/usr/share/nginx/html/404.html You should customize this error page for your own
site or edit the error_page directive in the nginx configuration file
/etc/nginx/nginx.conf."
```

An Insider Job?

In a post titled, "**У REvil угнали домены"** [Translated: REvil's domains were stolen"], REvil's current spokesperson – the persona behind the moniker *0_neday* on the darknet underground forum XSS – stated the server had compromised using UNKN's (a.k.a. Unknown and REvil's previous representative) private Tor service keys. "*To be precise they deleted the path to my hidden service in the torrc file and raised their own so I would go there".*

0_neday went on to further state that the group presumed Unknown had "died" earlier in the summer, when the group went offline in mid-July shortly after the Kaseya supply chain attack successfully encrypted thousands of networks when its ransomware spread through a software auto-update.

There are a number of conflicting theories why REvil disappeared less than a month later.

REvil's Mysterious Disappearance in July

REvil's services mysteriously shutoff the Tuesday following a late "Friday phone-call" between US President Biden and Russian President Vladmir Putin, during which REvil and the global ransomware epidemic was reportedly a subject of their conversation. The information security community has theorized any number of reasons the services disappeared after this call:

a. The US launched an offensive cyber campaign directly against REvil – possibly using sophisticated intelligence or USCYBERCOM resources – and brought the gang's services offline.

b. President Putin directed REvil to shut down their operations in response to the conversation he had directly with Biden, where Biden stated he would hold Russia responsible for aiding and abetting the threat actor's actions on Russian soil.

c. REvil was feeling the "heat" and international pressure after a series of high-profile attacks, some of which included US military targets. Perhaps the group's operators voluntarily "took a break" from their ransomware operation.

d. REvil leader, UNKN "exit scammed" emptying the gang and their affiliate's cryptocurrency accounts and disabled their Tor services using their administrator privileges.

Reporting from the Washington Post suggested the US was not behind the July shutdown, as some had hypothesized, citing government sources. No “seizure banner” was evident when the Tor services went offline as has historically been the case when law enforcement take down darknet marketplaces. The FBI’s Director, Christopher Wray testified in front of Congress stating how they do not make decisions unilaterally but work directly with allies and other agencies on such matters. The FBI was strongly criticized for their delay in providing a universal decrpytor key for the REvil ransomware after the Kaseya attack they had allegedly obtained.

> “These are complex . . . decisions, designed to create maximum impact, and that takes time in going against adversaries where we have to marshal resources not just around the country but all over the world.”

— FBI Director Testimony

The FBI provided the key to Kaseya nineteen (19) days after their networks were compromised and a week after the REvil infrastructure went dark. The key was reportedly obtained through direct access to the servers of the REvil operation.

In mid-September, BitDefender announced they had developed a “free universal decrpytor” for the REvil/Sodin ransomware strain in circulation prior to July 13th. According to BitDefender’s blog and social media posts, the decrpytor was “created in collaboration with a trusted law enforcement partner.”

This announcement was the source of many a controversial discussion across darknet malware forums.

REvil’s Return in September

According to the DarkOwl Vision darknet data records, REvil’s Happy Blog returned after their summer hiatus the first week in September 2021. Shortly after the blog was back online, new victims were quickly announced.

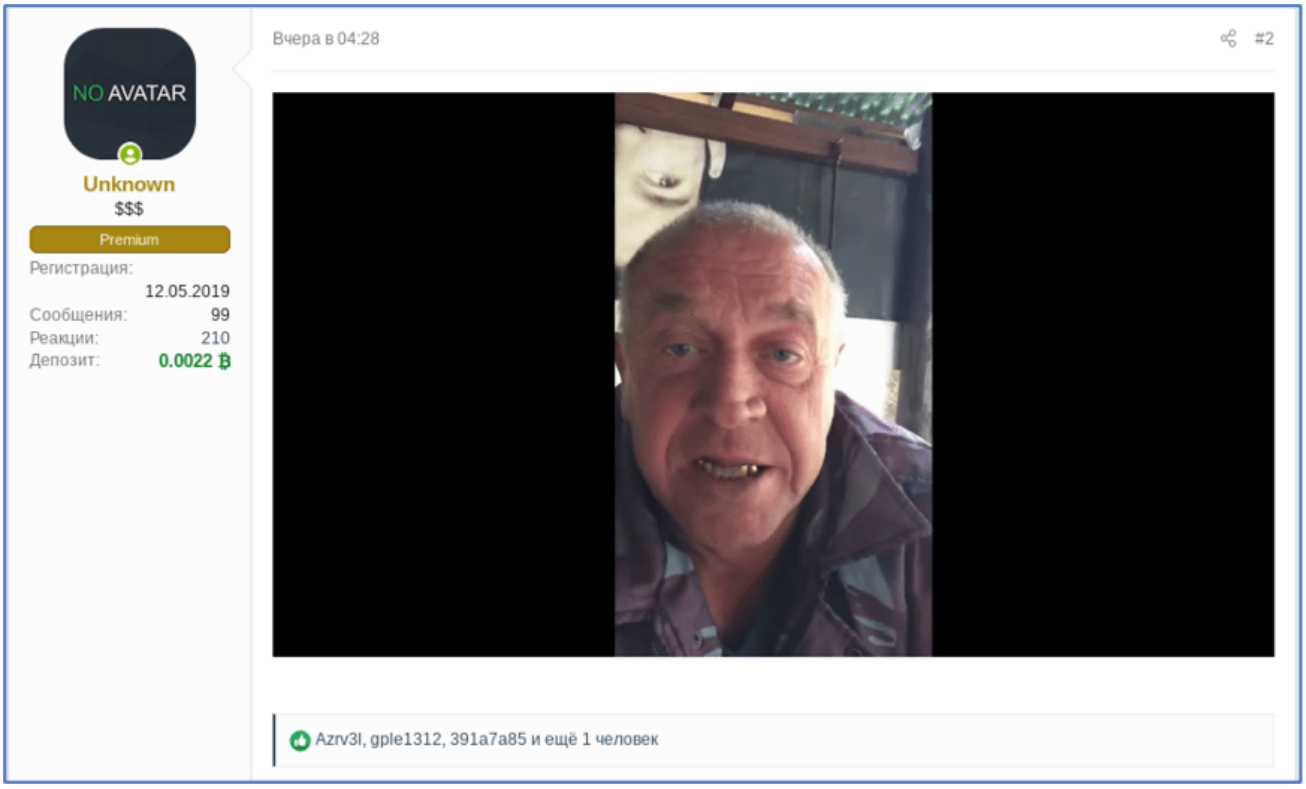
Surprisingly, in early October, DarkOwl analysts observed the REvil team sharing a link to RAMP – another ransomware focused forum – announcing that REvil was active on the new Groove ransomware backed forum. RAMP, hosted on a Tor domain previously owned and operated by the Babuk RaaS gang, emerged after many darknet underground forums “banned” ransomware related discussions last summer.

This behavior was noteworthy as REvil had historically not shown any affiliation with other RaaS groups, making their endorsement of RAMP unusual to many in the darknet.

Complex Cast of Characters

Unknown/UNKN

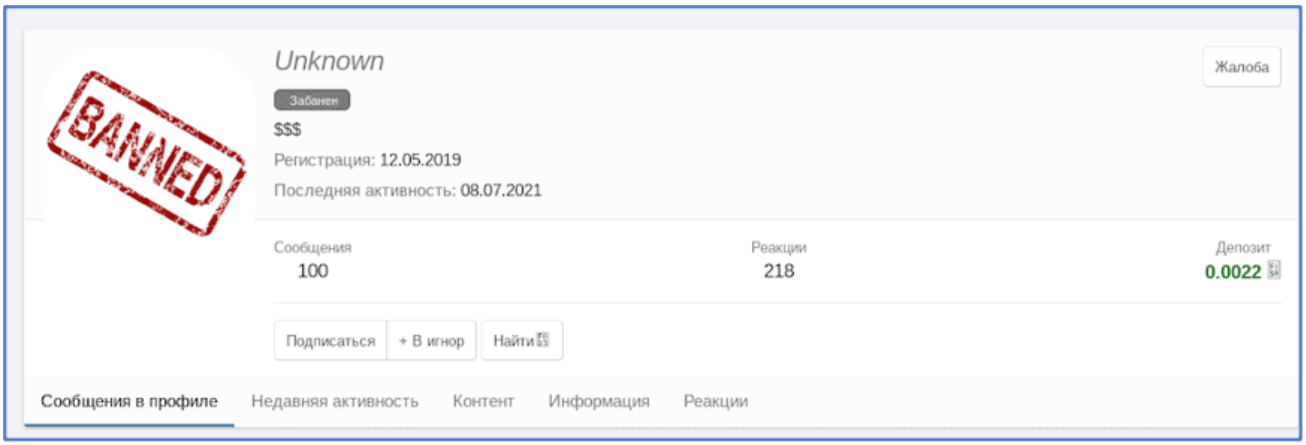
Unknown/UNKN was the original spokesperson for the REvil gang when they first branded as Sodinokibi in early 2019. They spoke with measured cadence and subtle humor. One of their last posts was early July after the Kaseya attack, where they simply shared a video of a typical older, angry Russian gentleman.



The admin from XSS banned Unknown's forum account on July 8th, the week in between the Kaseya attack and the REvil servers were shutdown in July. It's unclear if the justification was retribution for ransomware (as the topic was banned from the forum at that time), or the admin knew something else was awry.

In May, Unknown announced they were going to leave XSS, have limited activity on their account on exploit.in, and move their discussions to "private."

At the time of their account ban, *Unknown* had 0.0022 Bitcoin in escrow on XSS.



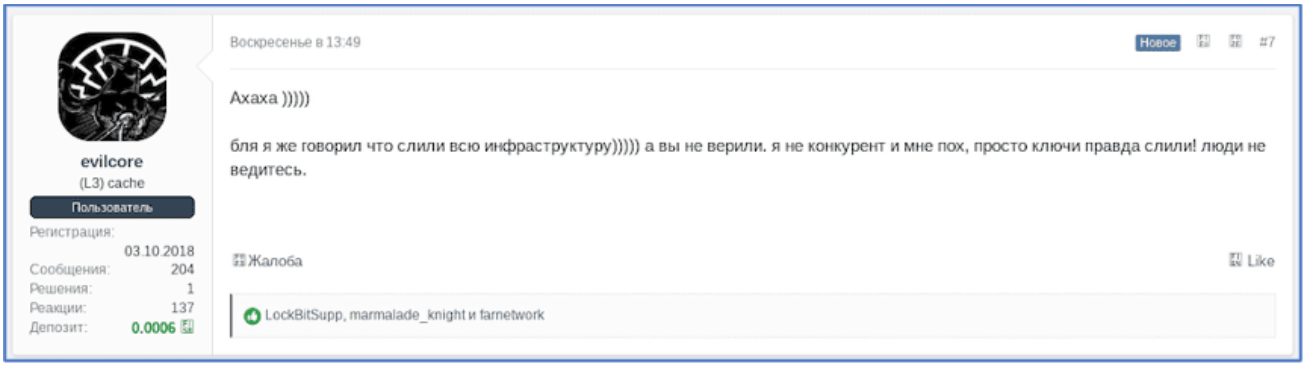
0_neday

0_neday emerged as a representative of REvil on XSS after users *evilcore* and *Lockbitsupp* challenged the origination of the REvil decryptor key released by Bitdefendor on the public forum. They created their account earlier this month on October 5, 2021, depositing a significant amount of Bitcoin (i.e. account value of 1 BTC in escrow or approximately $50,800 USD on 10/5/2021) to legitimize their status. On October 12th, *0_neday* posted on *evilcore's* XSS member profile, "my boss agreed to offer you a 10% discount" suggesting 0_neday is a front for someone much more authoritative in the REvil gang. This contrasts with a claim they made a few days later that only he and Unknown had private keys to the Tor onion service domains. As of 19 October, *0_neday* indicated they were leaving the forum, signing their last post with

```
[Translated] "Good luck everyone, I'm off."
```

evilcore

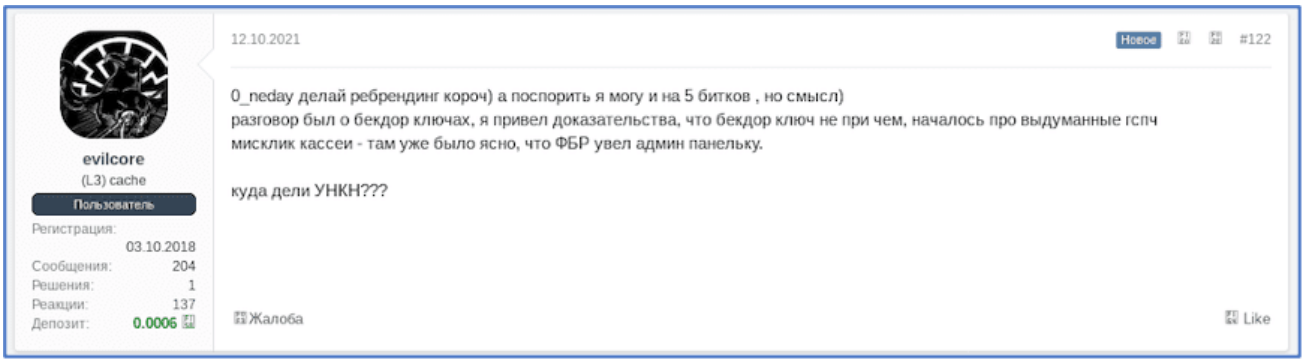
evilcore is a relatively long-time user of XSS with registration on the forum in late 2018. They claim they have no connection to any ransomware gang, but vocal in criticizing the operations of the groups, especially most recently REvil. They posted a comment to *0_neday's* thread this week about REvil's domains getting stolen suggesting the leak of the decryption key was intentional and the entire infrastructure was merged and not compromised by *Unknown* as indicated, with a bit of "told you so" attitude and stark warning for users not to get fooled.




```
[Translated] "Ahaha)))))

fuck, I told you that they merged the entire infrastructure))))) and you didn't
believe. I'm not a competitor and I don't care, they just really leaked the keys!
people don't get fooled."
```

evilcore have been vocal against the legitimacy of REvil since they reappeared in September and the story that supposed a REvil developer "misclicked" accidently releasing the decryptor key. In a comment on a thread titled, "**Атака вымогателей на больницу привела к гибели ребенка"** [Translated: "The ransomware attack on the hospital led to the death of a child"], evilcore closes with [Translated: "where is UNKN?"] after claiming the FBI likely had control of REvil's admin panel.



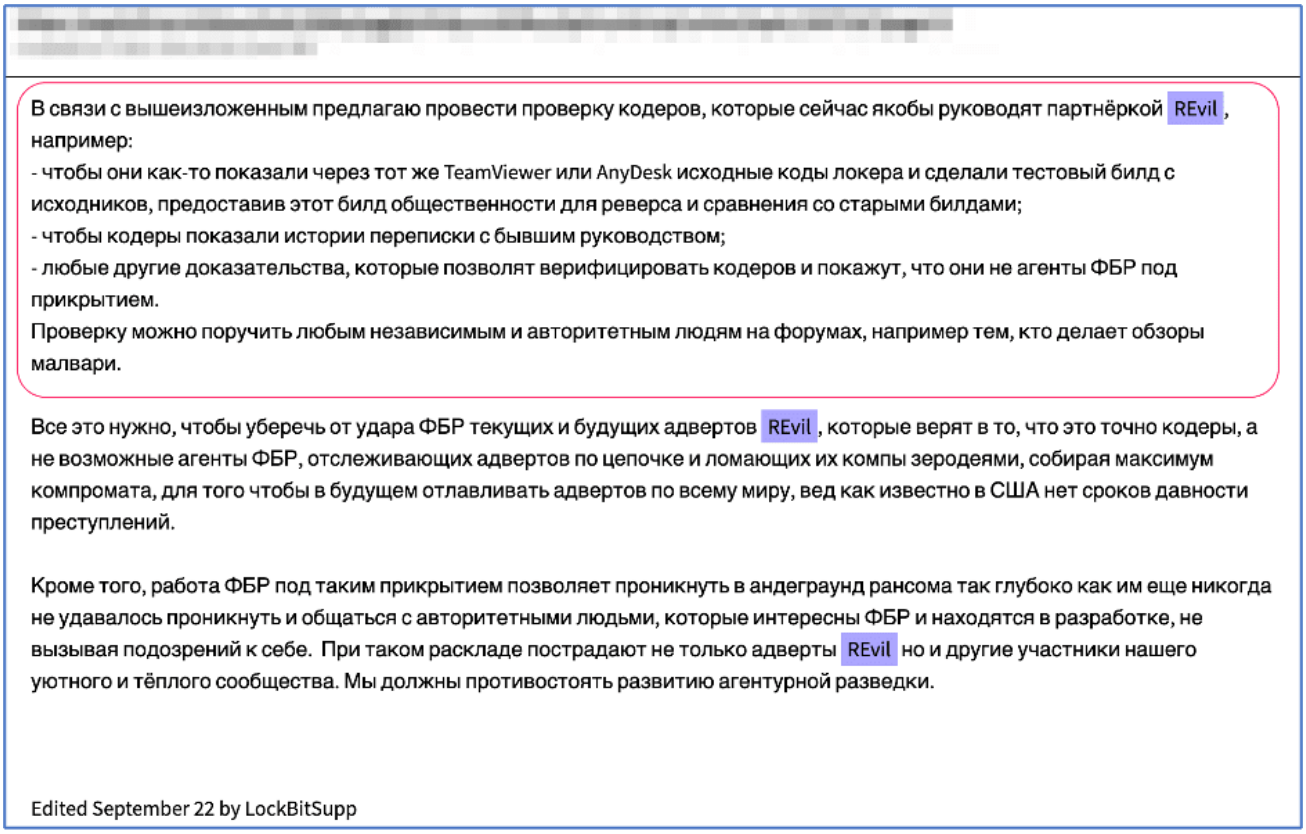

```
[Translated] "0_neday do the rebranding:) and I can bet on 5 bits, but the point is)
the conversation was about backdoor keys, I gave evidence that the backdoor key had
nothing to do with it, it started about fictional gspch misklik checkout and - there
it was already clear that the FBI had taken the admin panel.

Where is UNKN going???"
```

The controversial October 12 thread continued with bickering between directly between *0_neday* and *evilcore*, with LockBit's forum representative, *LockBitSupp, and forum users, 1MG, and ev4ng3liya*, chiming in including critiques of REvil's desperation to draw in affiliates with a 90/10 percent split – unheard of in the RaaS industry. *evilcore* eventually even accused *0_neday* of being FBI.

LockBitSupp

LockBitSupp is competitive RaaS gang, LockBit 2.0's public representative on the XSS forum. This alias is also active for the same group on another darknet forum, exploit.in and highly critical of REvil, stating they had recruited many REvil affiliates due to their lousy partner programs (PP). On exploit, they added lengthy posts with concerns that REvil had been compromised by the FBI and that the current REvil coders and affiliates needed to be checked to verify their allegiance to the RaaS industry:



В связи с вышеизложенным предлагаю провести проверку кодеров, которые сейчас якобы руководят партнёркой REvil, например:
- чтобы они как-то показали через тот же TeamViewer или AnyDesk исходные коды локера и сделали тестовый билд с исходников, предоставив этот билд общественности для реверса и сравнения со старыми билдами;
- чтобы кодеры показали истории переписки с бывшим руководством;
- любые другие доказательства, которые позволят верифицировать кодеров и покажут, что они не агенты ФБР под прикрытием.
Проверку можно поручить любым независимым и авторитетным людям на форумах, например тем, кто делает обзоры малвари.

Все это нужно, чтобы уберечь от удара ФБР текущих и будущих адвертов REvil, которые верят в то, что это точно кодеры, а не возможные агенты ФБР, отслеживающих адвертов по цепочке и ломающих их компы зеродеями, собирая максимум компромата, для того чтобы в будущем отлавливать адвертов по всему миру, вед как известно в США нет сроков давности преступлений.

Кроме того, работа ФБР под таким прикрытием позволяет проникнуть в андеграунд рансома так глубоко как им еще никогда не удавалось проникнуть и общаться с авторитетными людьми, которые интересны ФБР и находятся в разработке, не вызывая подозрений к себе. При таком раскладе пострадают не только адверты REvil но и другие участники нашего уютного и тёплого сообщества. Мы должны противостоять развитию агентурной разведки.

Edited September 22 by LockBitSupp

```
[Translated] "In connection with the above, I propose to check the coders who are
now allegedly running the REvil affiliate program, for example:

- so that they somehow showed the locker source codes through the same TeamViewer or
AnyDesk and made a test build from the source, providing this build to the public
for reverse and comparison with old builds;

- so that the coders show the history of correspondence with the former management;

- any other evidence that will allow us to verify the coders and show that they are
not undercover FBI agents.

Verification can be entrusted to any independent and authoritative people on the
forums, for example, those who do reviews of malware."
```

They concluded their post with the realization that **if the FBI has infiltrated** the REvil RaaS gang or their affiliates, that the damage to the advertisers was far less than the suffering caused to "**our cozy and warm community**."

REvil brand trustworthiness continues to decline

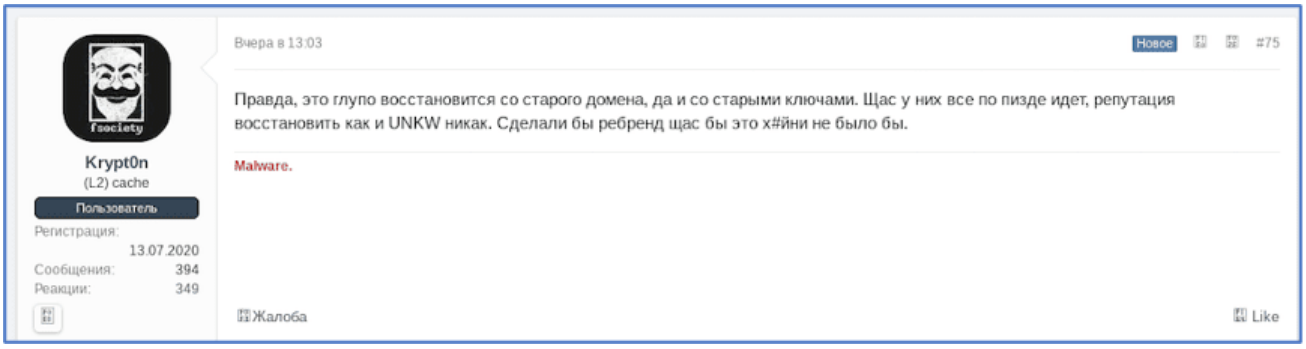
In late September, darknet forum users began expressing concerns over REvil's unpredictable and scandalous behavior. One exploit user, *Signature*, claimed they had evidence that REvil had installed a "cryptobackdoor" which allowed REvil operators to take over negotiations between their affiliates and their victims, usurping ransomware payments

thereby scamming money from their affiliates. It's unclear how long this backdoor existed – some researchers state the backdoor was present for months, but removed from the September codebase.

Signature had launched a previous dispute on the forum with REvil's UNKN in May 2021, when they claimed they had been contracted to provide network access to REvil victims, Quanta and Apex, and was never paid their 7 Million USD for the work provided. The thread resulted in a gross airing of RaaS dirty laundry to the public with private chats from qTox shared on the forum thread.

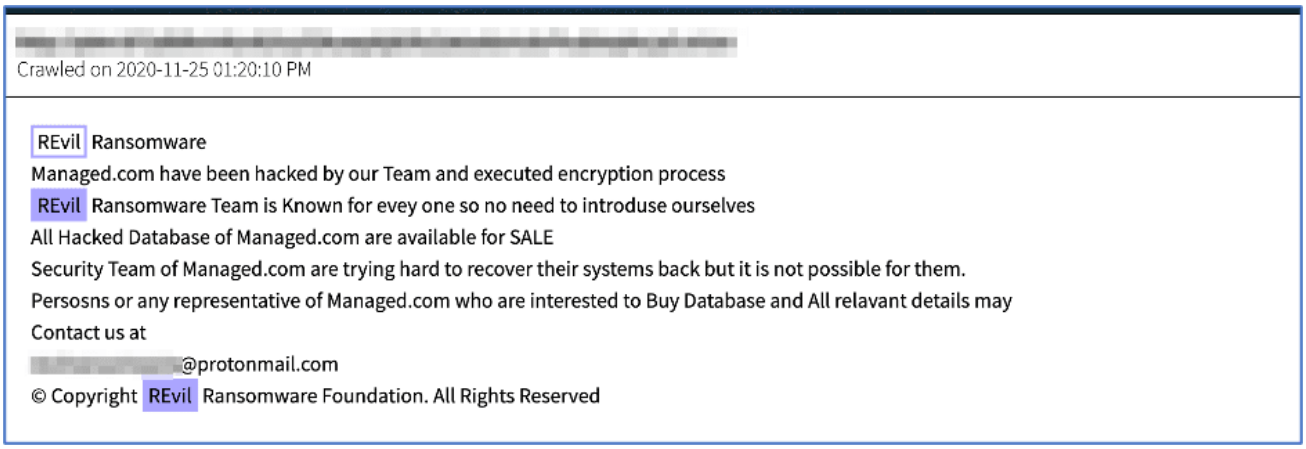
Up until last weekend, REvil had been active on the same Tor v3 domain address for over 22 months, excluding their summer vacation and active in the ransomware market since April 2019. Most RaaS groups change addresses regularly and even rebrand with new logos and aliases to maintain their operational security.

EvilCorp RaaS gang''s representative on the XSS forum suggested REvil should have rebranded a long time ago. In the most recent thread of the REvil domain hijacking, user Krypt0n, admittedly late to the conversation, stated it was stupid for REvil to return in September to the same Tor domain address with the same keys. They added there was no way for REvil to restore their reputation and status achieved by UNKN.



Despite the fact elite hacker forum members can easily spot law enforcement and rippers, REvil's brand is renowned and other copycat services will likely emerge in their likeness. In November last year, DarkOwl detected a non-REvil related domain advertising they were the "REvil Team" and were offering to sell Managed.com's website hosting company's database.

The REvil imposters included a protonmail.com e-mail address for contacting them and the domain was online for barely a month.



DarkOwl will continue to monitor this situation as it develops.

Curious about something you've read? Contact us to learn how darknet data applies to your use case

---