REvil ransomware returns: New malware sample confirms gang is back

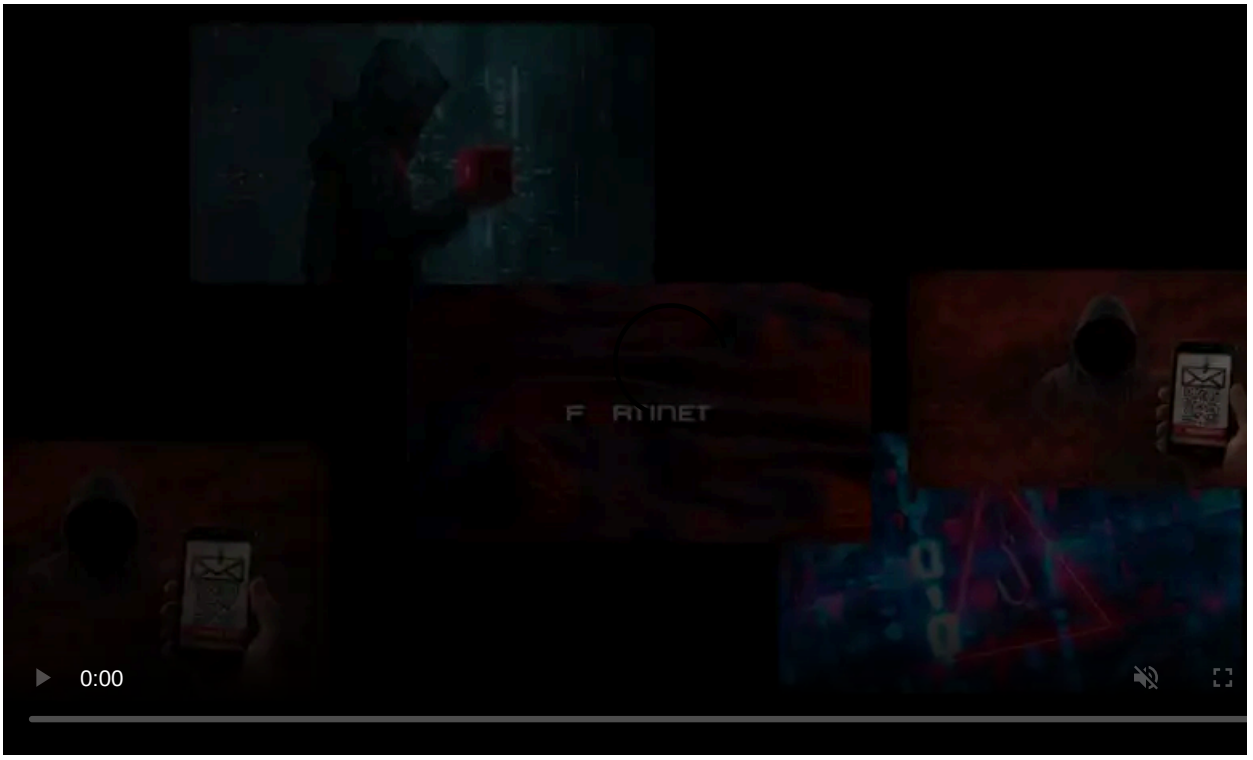
By Lawrence Abrams

Published: 2022-05-01 · Archived: 2026-04-05 21:20:00 UTC

The notorious REvil ransomware operation has returned amidst rising tensions between Russia and the USA, with new infrastructure and a modified encryptor allowing for more targeted attacks.

In October, the REvil ransomware gang shut down after a law enforcement operation hijacked their Tor servers, followed by arrests of members by Russian law enforcement.

However, after the invasion of Ukraine, Russia stated that the US had withdrawn from the negotiation process regarding the REvil gang and closed communications channels.


0:00

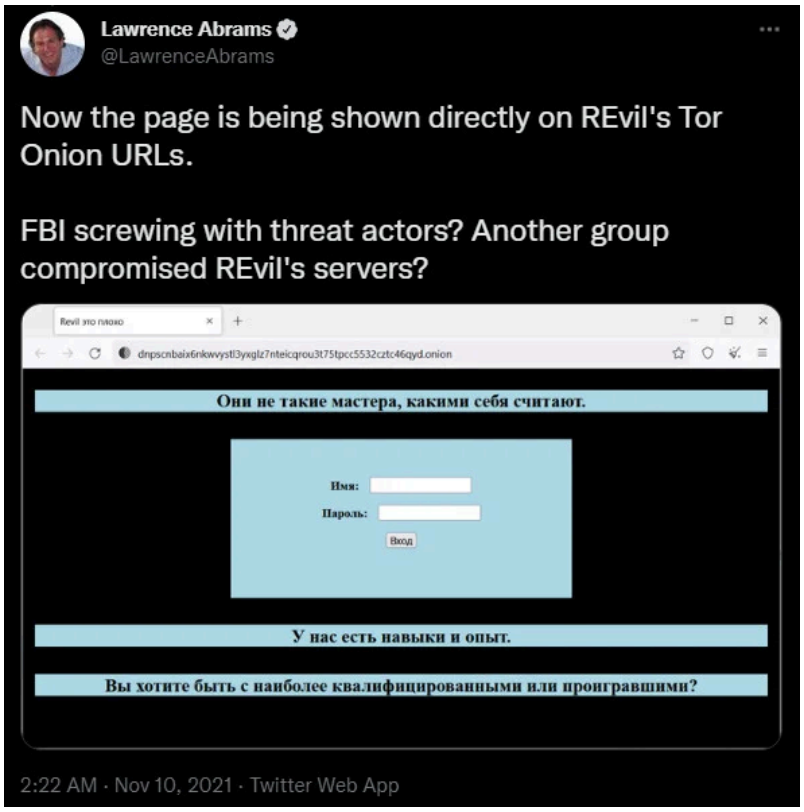
REvil's Tor sites come back to life

Soon after, the old REvil Tor infrastructure began operating again, but instead of showing the old websites, they redirected visitors to URLs for a new unnamed ransomware operation.

While these sites looked nothing like REvil's previous websites, the fact that the old infrastructure was redirecting to the new sites indicated that REvil was likely operating again. Furthermore, these new sites contained a mix of new victims and data stolen during previous REvil attacks.

While these events strongly indicated that REvil rebranded as the new unnamed operation, the Tor sites had also previously displayed a message in November stating that "REvil is bad."

This access to the Tor sites meant that other threat actors or law enforcement had access to REvil's TOR sites, so the websites themselves were not strong enough proof of the gang's return.



REvil's tor sites are defaced with an anti-REvil message
Source: BleepingComputer

The only way to know for sure whether REvil was back was to find a sample of the ransomware encryptor and analyze it to determine if it was patched or compiled from source code.

A sample of the new ransomware operation's encryptor was finally discovered this week by AVAST research Jakub Kroustek and has confirmed the new operation's ties to REvil.

Ransomware sample confirms return

While a few ransomware operations are using REvil's encryptor, they all use patched executables rather than having direct access to the gang's source code.

However, BleepingComputer has been told by multiple security researchers and malware analysts that the discovered REvil sample used by the new operation is compiled from source code and includes new changes.

Security researcher R3MRUM has tweeted that the REvil sample has had its version number changed to 1.0 but is a continuation of the last version, 2.08, released by REvil before they shut down.

```
snwprintf(
  v3,
  0x20000,
  v7,
  0x100,                                // <--- version 1.00
  dword_415F50,
  dword_415F50,
  dword_415F64,
  dword_415F68,
  dword_415F6C,
  dword_415F70,
  dword_415F74,
  dword_415F78,
  dword_415F7C,
  dword_415F80,
  dword_415FEC,
  dword_415F84,
  dword_415F60 + 2);
```

Version change in new REvil encryptor

In discussion with BleepingComputer, the researcher said he could not explain why the encryptor doesn't encrypt files but believes it was compiled from source code.

"Yes, my assessment is that the threat actor has the source code. Not patched like "LV Ransomware" did," R3MRUM told BleepingComputer.

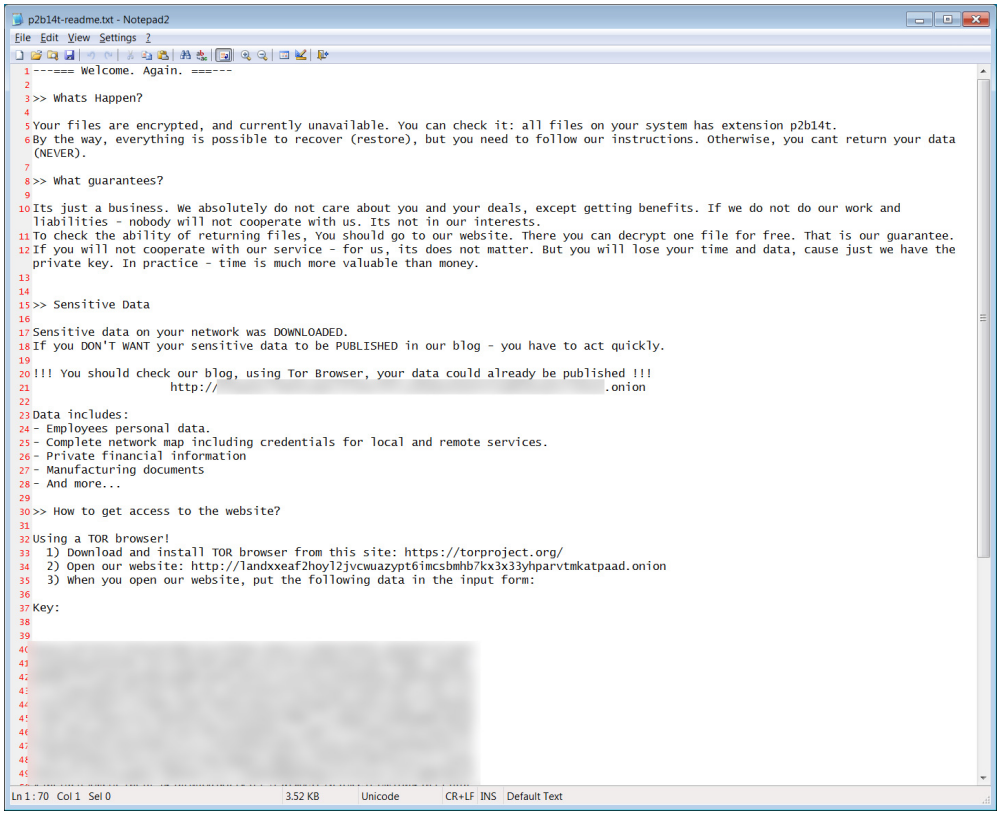
Advanced Intel CEO Vitali Kremez also reverse-engineered the REvil sample this weekend and has confirmed to BleepingComputer that it was compiled from source code on April 26th and was not patched.

Kremez told BleepingComputer that the new REvil sample includes a new configuration field, 'accs,' which contains credentials for the specific victim that the attack is targeting.

Kremez believes that the 'accs' configuration option is used to prevent encryption on other devices that do not contain the specified accounts and Windows domains, allowing for highly targeted attacks.

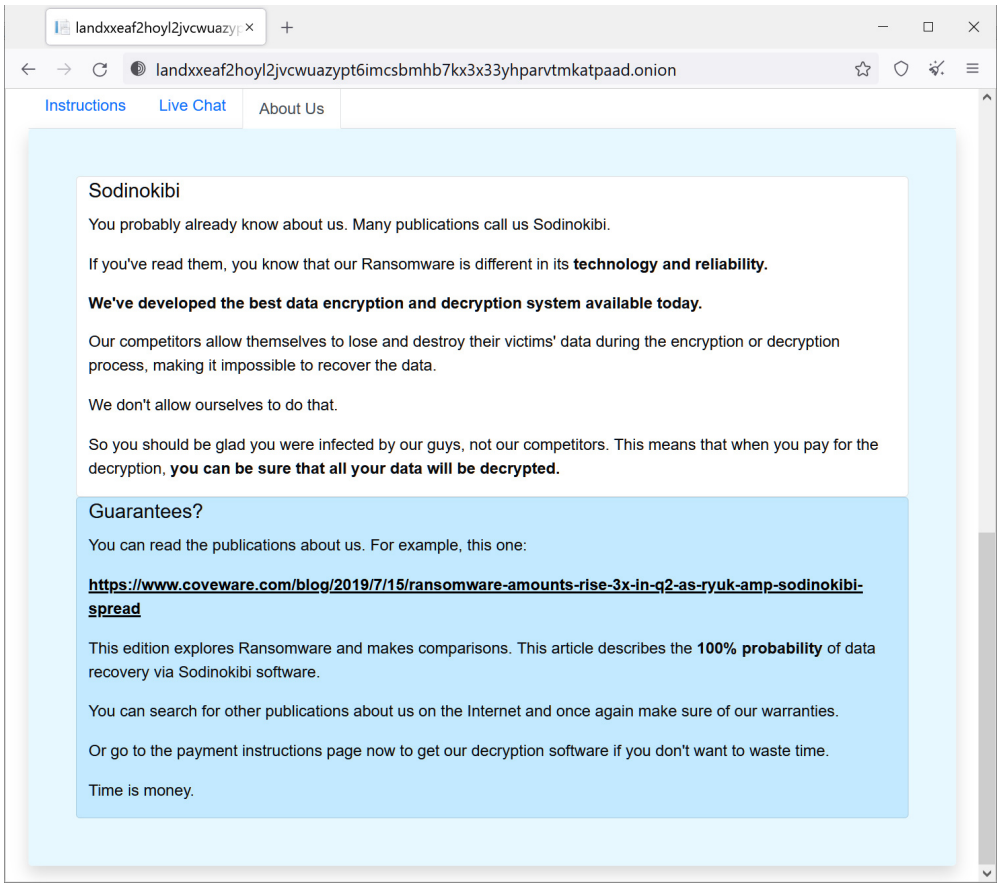
In addition to the 'accs' option, the new REvil sample's configuration has modified SUB and PID options, used as campaign and affiliate identifiers, to use longer GUID-type values, such as '3c852cc8-b7f1-436e-ba3b-c53b7fc6c0e4.'

BleepingComputer also tested the ransomware sample, and while it did not encrypt, it did create the ransom note, which is identical to REvil's old ransom notes.



REvil ransom note

Furthermore, while there are some differences between the old REvil sites and the rebranded operation, once a victim logs into the site, it is almost identical to the originals, and the threat actors claim to be 'Sodinokibi,' as shown below.



New ransomware operation claiming to be Sodinokibi
Source: BleepingComputer

While the original public-facing REvil representative known as 'Unknown' is still missing, threat intelligence researcher FellowSecurity told BleepingComputer that one of REvil's original core developers, who was part of the old team, relaunched the ransomware operation.

As this was a core developer, it would make sense that they also had access to the complete REvil source code and potentially the Tor private keys for the old sites.

It's not surprising that REvil has rebranded under the new operation, especially with the declining relations between USA and Russia.

However, when ransomware operations rebrand, they typically do it to evade law enforcement or sanctions preventing the payment of ransoms.

Therefore, it is unusual for REvil to be so public about their return, rather than trying to evade detection like we have seen in so many other ransomware rebrands.
