# More Conti ransomware source code leaked on Twitter out of revenge

By Lawrence Abrams

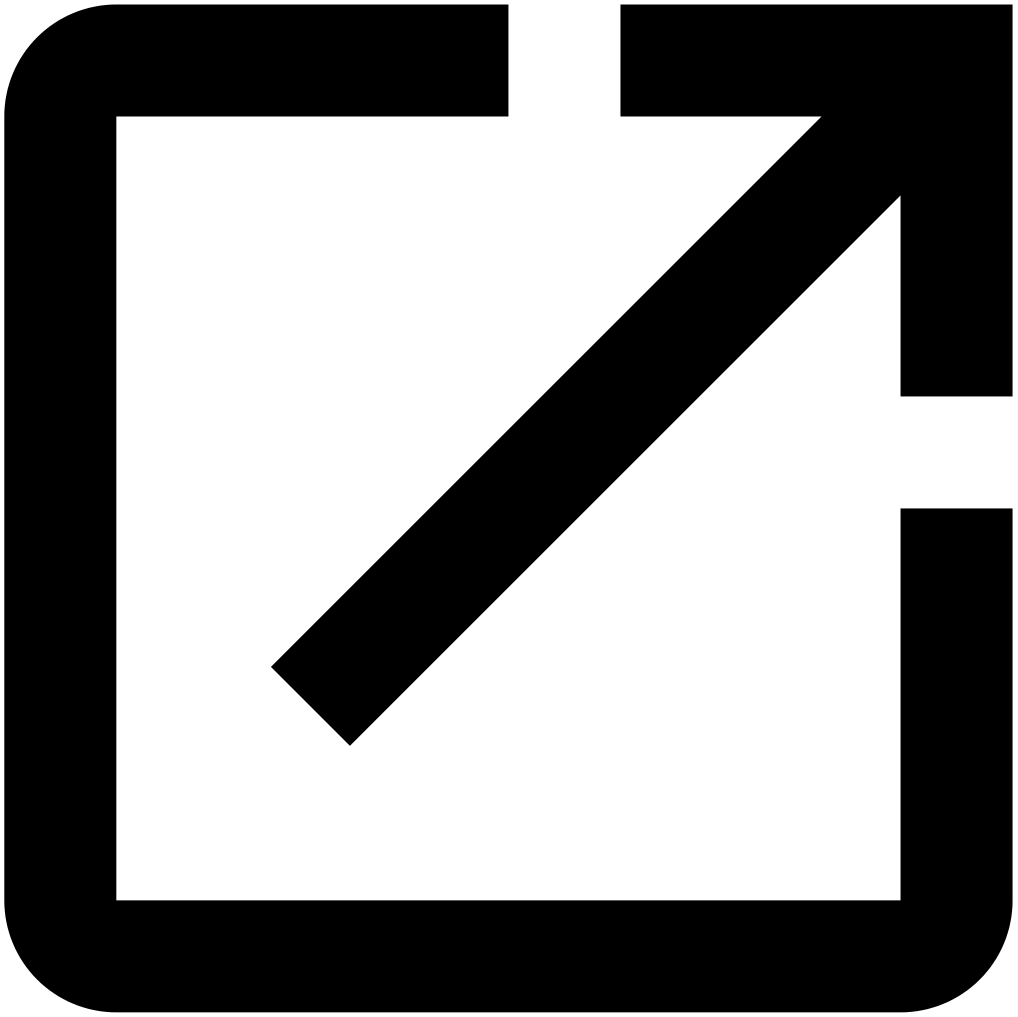
Published: 2022-03-20 · Archived: 2026-04-05 14:19:13 UTC


A Ukrainian security researcher has leaked newer malware source code from the Conti ransomware operation in revenge for the cybercriminals siding with Russia on the invasion of Ukraine.

Conti is an elite ransomware gang run by Russian-based threat actors. With their involvement in developing numerous malware families, it is considered one of the most active cybercrime operations.

However, after the Conti Ransomware operation sided with Russia on the invasion of Ukraine, a Ukrainian researcher named 'Conti Leaks' decided to leak data and source code belonging to the ransomware gang out of revenge.


DIE LINKE.
0:00




**Conti siding with Russia on the invasion of Ukraine**

*Source: BleepingComputer*

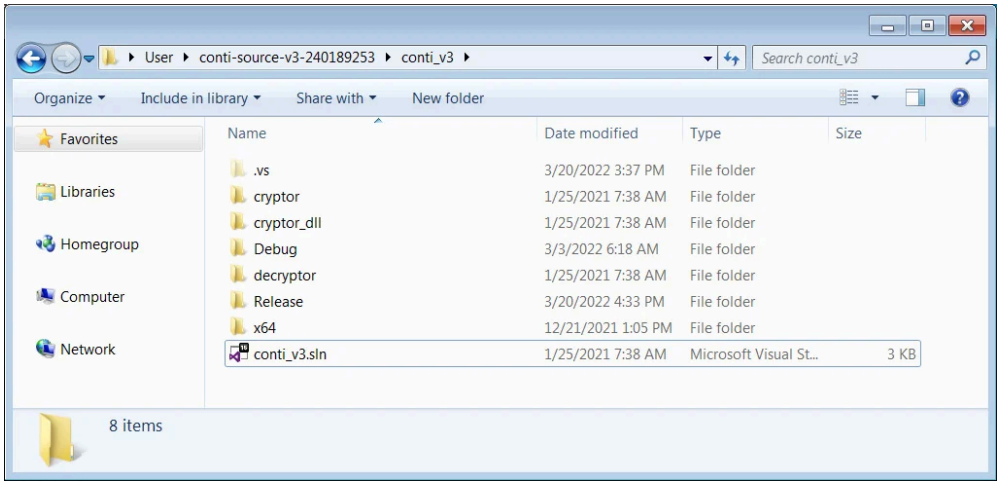
Last month, the researcher published almost 170,000 internal chat conversations between the Conti ransomware gang members, spanning January 21st, 2021, through February 27th, 2022. These chat messages provide detailed insight into the operation's activities and its member's involvement

The researcher later leaked old Conti ransomware source code dated September 15th, 2020. While the code was rather old, it allowed researchers and law enforcement to analyze the malware to understand better how it works.

## More recent Conti source code released

Today, Conti Leaks uploaded the source code for Conti version 3 to VirusTotal and posted a link on Twitter. While the archive is password-protected, the password should be easily determined from subsequent tweets.

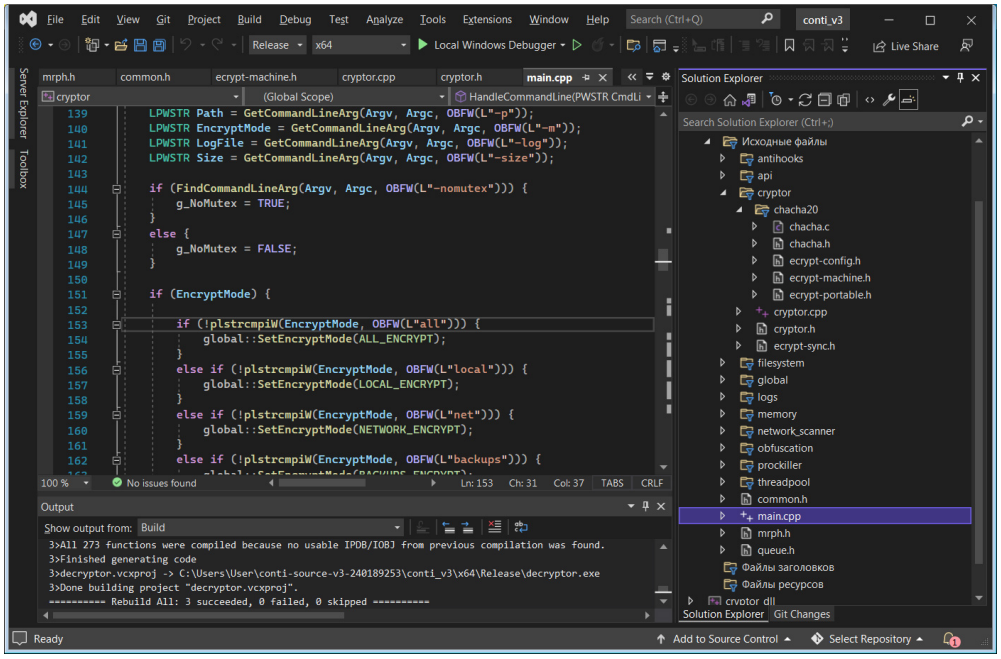
This source code is much newer than the previously released version, with the last modified dates being January 25th, 2021, making it over one year newer than the previously released code.




**Conti Locker version 3 source code**

*Source: BleepingComputer*

Like the previous version, the source code leak is a Visual Studio solution that allows anyone with access to compile the ransomware locker and decryptor.

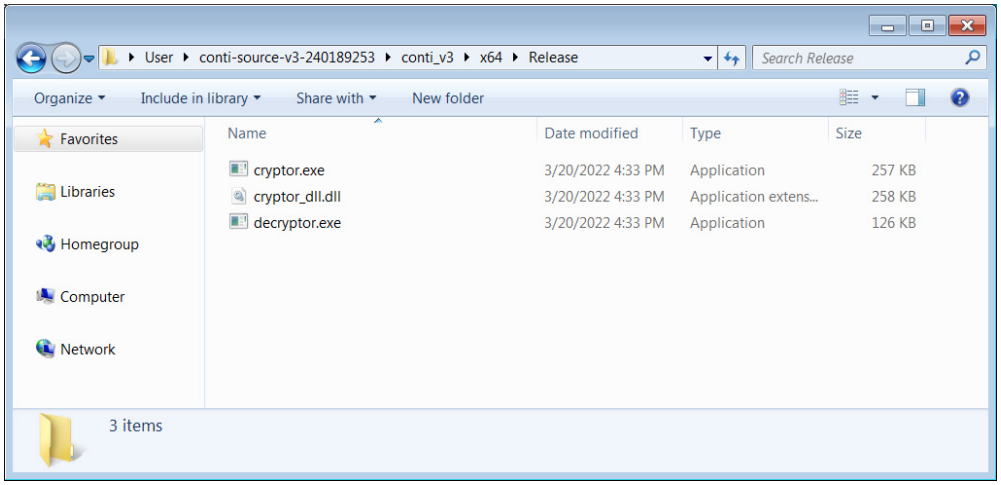



**Compiling the Conti source in Visual Studio**

*Source: BleepingComputer*

The source code compiles without error and can be easily modified by other threat actors to use their own public keys or add new functionality.

As you can see below, BleepingComputer compiled the source code without any issues, creating the cryptor.exe, cryptor_dll.dll, and decryptor.exe executables.




**Compiled Conti executables**

*Source: BleepingComputer*

The release of ransomware source code, especially for advanced operations like Conti, can have disastrous effects on corporate networks and consumers. This is because it is very common for other threat actors to use the released source code to create their own ransomware operations.

In the past, a researcher published the source code for a ransomware named 'Hidden Tear' that many threat actors quickly adopted to launch different operations.

While Hidden Tear can be decrypted, it led to a scourge of new ransomware infections that terrorized consumers and companies for years.

More recently, a threat actor leaked the source code for Babuk ransomware on a Russian-speaking hacking forum.

Within days, other threat actors used the source code for their use, and new ransomware operations were launched, such as Rook and Pandora.

With the continued leaks of the Conti ransomware gang's source code, it is only a matter of time until other threat actors use it to launch their own operations.



---