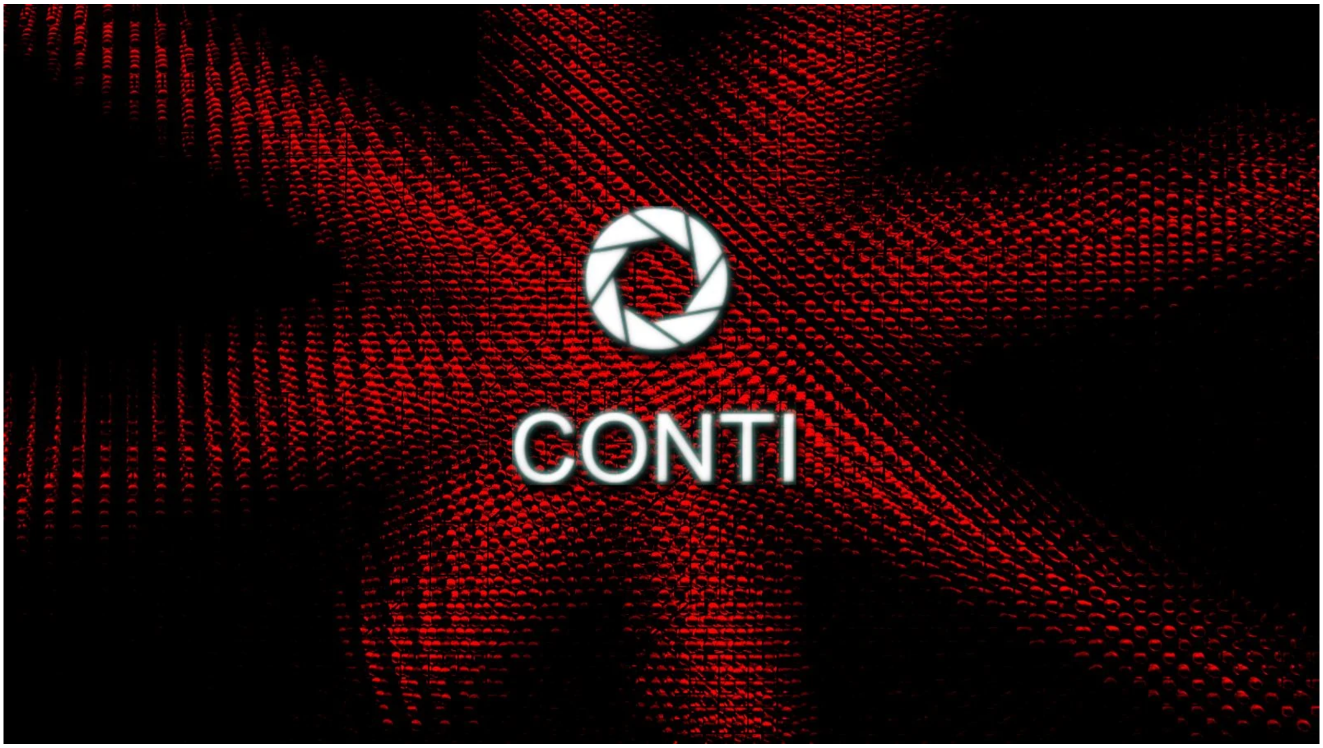
Conti Ransomware source code leaked by Ukrainian researcher

bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

Lawrence Abrams

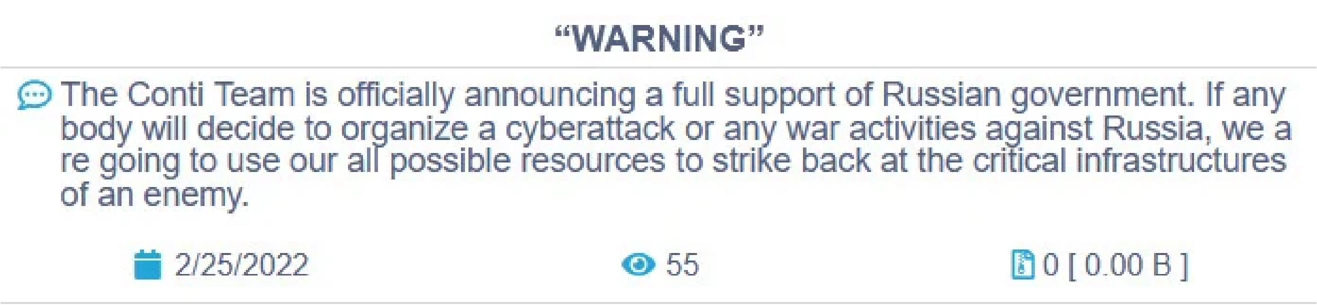
By
Lawrence Abrams

- March 1, 2022
- 05:24 PM
- 0



A Ukrainian researcher continues to deal devastating blows to the Conti ransomware operation, leaking further internal conversations, as well as the source for their ransomware, administrative panels, and more.

It has been quite a damaging week for Conti after they sided with Russia on the invasion of Ukraine and upset Ukrainian adverts (affiliates) and a researcher who has been secretly snooping on their operation.



"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

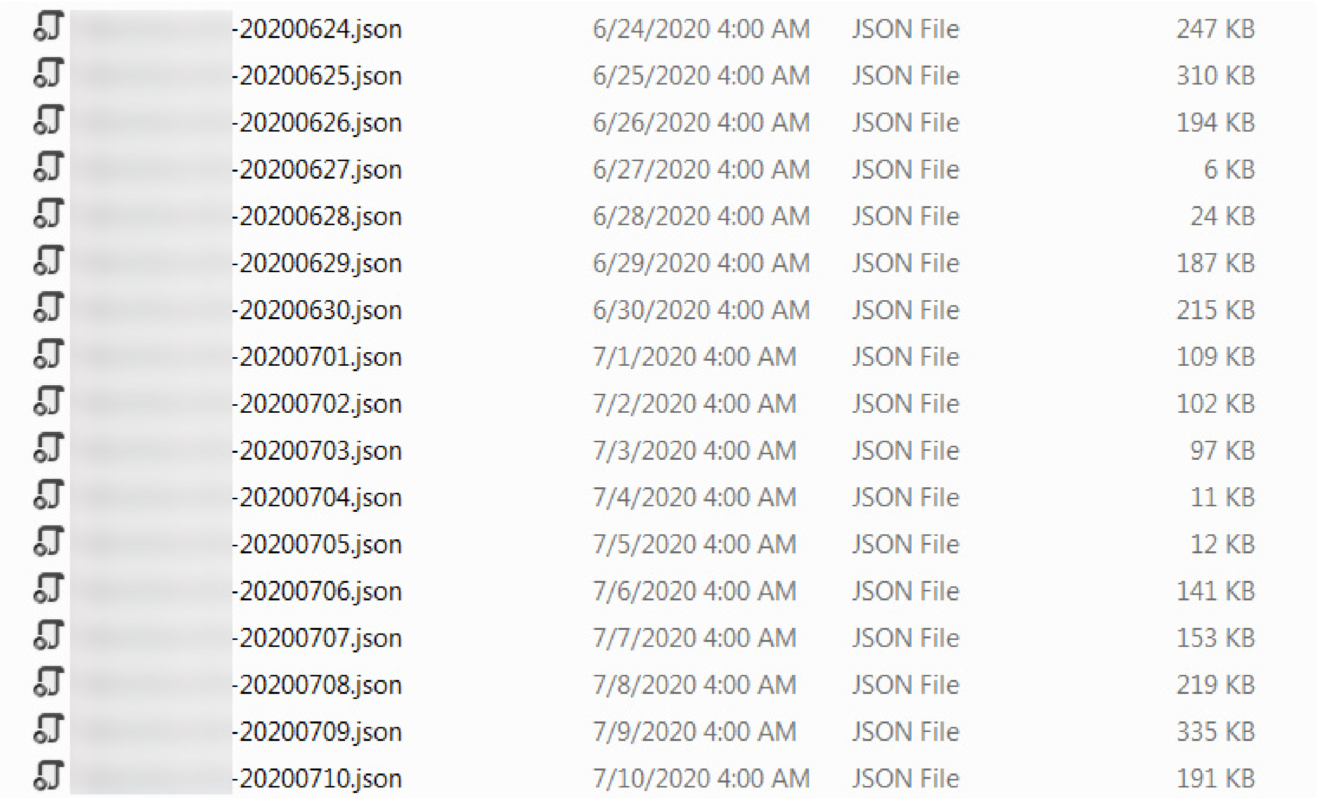
2/25/2022 55 0 [0.00 B]

Conti siding with Russia on the invasion of Ukraine

On Sunday, a Ukrainian researcher using the Twitter handle @ContiLeaks leaked 393 JSON files containing over 60,000 internal messages taken from the Conti and Ryuk ransomware gang's private XMPP chat server.

These conversations were from January 21st, 2021, through February 27th, 2022, providing a treasure trove of information on the cybercrime organization, such as bitcoin addresses, how the gang is organized as a business, evading law enforcement, how they conduct their attacks, and much more.

On Monday, the researcher kept leaking more damaging Conti data, including an additional 148 JSON files containing 107,000 internal messages since June 2020, which is around when the Conti ransomware operation was first launched.



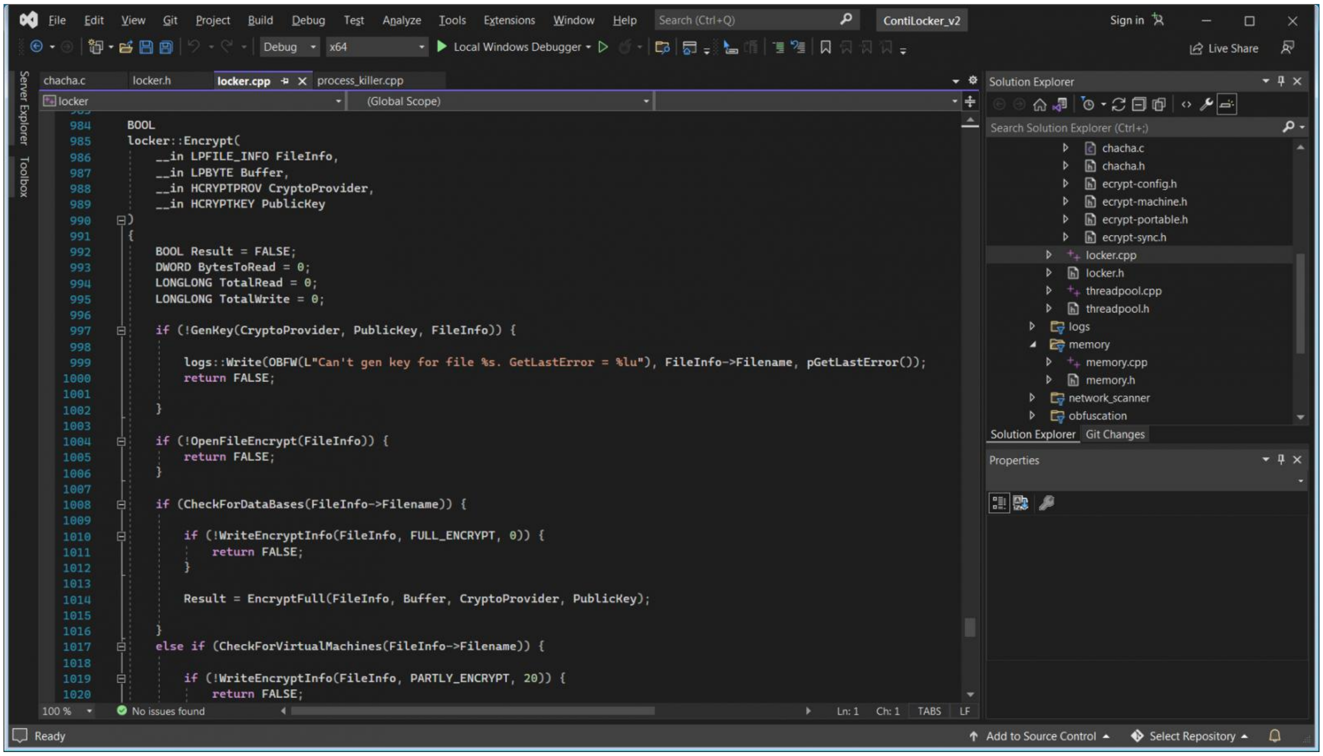
[redacted]-20200624.json	6/24/2020 4:00 AM	JSON File	247 KB
[redacted]-20200625.json	6/25/2020 4:00 AM	JSON File	310 KB
[redacted]-20200626.json	6/26/2020 4:00 AM	JSON File	194 KB
[redacted]-20200627.json	6/27/2020 4:00 AM	JSON File	6 KB
[redacted]-20200628.json	6/28/2020 4:00 AM	JSON File	24 KB
[redacted]-20200629.json	6/29/2020 4:00 AM	JSON File	187 KB
[redacted]-20200630.json	6/30/2020 4:00 AM	JSON File	215 KB
[redacted]-20200701.json	7/1/2020 4:00 AM	JSON File	109 KB
[redacted]-20200702.json	7/2/2020 4:00 AM	JSON File	102 KB
[redacted]-20200703.json	7/3/2020 4:00 AM	JSON File	97 KB
[redacted]-20200704.json	7/4/2020 4:00 AM	JSON File	11 KB
[redacted]-20200705.json	7/5/2020 4:00 AM	JSON File	12 KB
[redacted]-20200706.json	7/6/2020 4:00 AM	JSON File	141 KB
[redacted]-20200707.json	7/7/2020 4:00 AM	JSON File	153 KB
[redacted]-20200708.json	7/8/2020 4:00 AM	JSON File	219 KB
[redacted]-20200709.json	7/9/2020 4:00 AM	JSON File	335 KB
[redacted]-20200710.json	7/10/2020 4:00 AM	JSON File	191 KB

Further leaked internal conversations

ContiLeaks began releasing more data throughout the night, including the source code for the gang's administrative panel, the BazarBackdoor API, screenshots of storage servers, and more.

However, a part of the leak that got people excited was a password-protected archive containing the source code for the Conti ransomware encryptor, decryptor, and builder.

While the leaker did not share the password publicly, another researcher soon cracked it, allowing everyone access to the source code for the Conti ransomware malware files.



```
BOOL
locker::Encrypt(
    __in LPFILE_INFO FileInfo,
    __in LPBYTE Buffer,
    __in HCRYPTPROV CryptoProvider,
    __in HCRYPTKEY PublicKey
)
{

    BOOL Result = FALSE;
    DWORD BytesToRead = 0;
    LONGLONG TotalRead = 0;
    LONGLONG TotalWrite = 0;

    if (!GenKey(CryptoProvider, PublicKey, FileInfo)) {

        logs::Write(OBFW(L"Can't gen key for file %s. GetLastError = %lu"), FileInfo->Filename, pGetLastError());
        return FALSE;

    }

    if (!OpenFileEncrypt(FileInfo)) {
        return FALSE;
    }

    if (CheckForDataBases(FileInfo->Filename)) {

        if (!WriteEncryptInfo(FileInfo, FULL_ENCRYPT, 0)) {
            return FALSE;
        }

        Result = EncryptFull(FileInfo, Buffer, CryptoProvider, PublicKey);

    }
    else if (CheckForVirtualMachines(FileInfo->Filename)) {

        if (!WriteEncryptInfo(FileInfo, PARTLY_ENCRYPT, 20)) {
            return FALSE;
```

Conti source code for encrypting a file

If you are a reverse engineer, the source code may not provide additional information. However, the source code provides enormous insight into how the malware works for those who can program in C, but not necessarily reverse engineer.

While this is good for security research, the public availability of this code does have its drawbacks.

As we saw when the HiddenTear (*for "educational reasons"*) and Babuk ransomware source code was released, threat actors quickly coopt the code to launch their own operations.

With code as tight and clean as the Conti ransomware operation, we should expect other threat actors to attempt to launch their own criminal operations using the leaked source code.

What may be more helpful, though, is the BazarBackdoor APIs and TrickBot command and control server source code that was released, as there is no way to access that info without having access to the threat actor's infrastructure.

As for Conti, we will have to wait and see if this "data breach" has much of an impact on their operation.

This has been a significant reputational blow for the group that may cause affiliates to move to another ransomware operation.

But, just like all businesses, and there is no denying Conti is run like a business, data breaches happen all the time.

Related Articles:

Conti ransomware shuts down operation, rebrands into smaller units

Hackers use Conti's leaked ransomware to attack Russian companies

Snap-on discloses data breach claimed by Conti ransomware gang

Globant confirms hack after Lapsus$ leaks 70GB of stolen data

Shutterfly discloses data breach after Conti ransomware attack

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.