

Conti ransomware's internal chats leaked after siding with Russia

bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/

Lawrence Abrams

By

[Lawrence Abrams](#)

- February 27, 2022
- 11:23 PM
- 0



































A Ukrainian security researcher has leaked over 60,000 internal messages belonging to the Conti ransomware operation after the gang sided with Russia over the invasion of Ukraine.

BleepingComputer has independently confirmed the validity of these messages from internal conversations previously shared with BleepingComputer regarding Conti's attack on Shutterfly.

AdvIntel CEO [Vitali Kremez](#), who has been tracking the Conti/TrickBot operation over the last couple of years, also confirmed to BleepingComputer that the leaked messages are valid and were taken from a log server for the Jabber communication system used by the ransomware gang.

Kremez told BleepingComputer that the data was leaked by a researcher who had access to the "ejabberd database" backend for Conti's XMPP chat server. This was also confirmed by cybersecurity firm Hold Security.

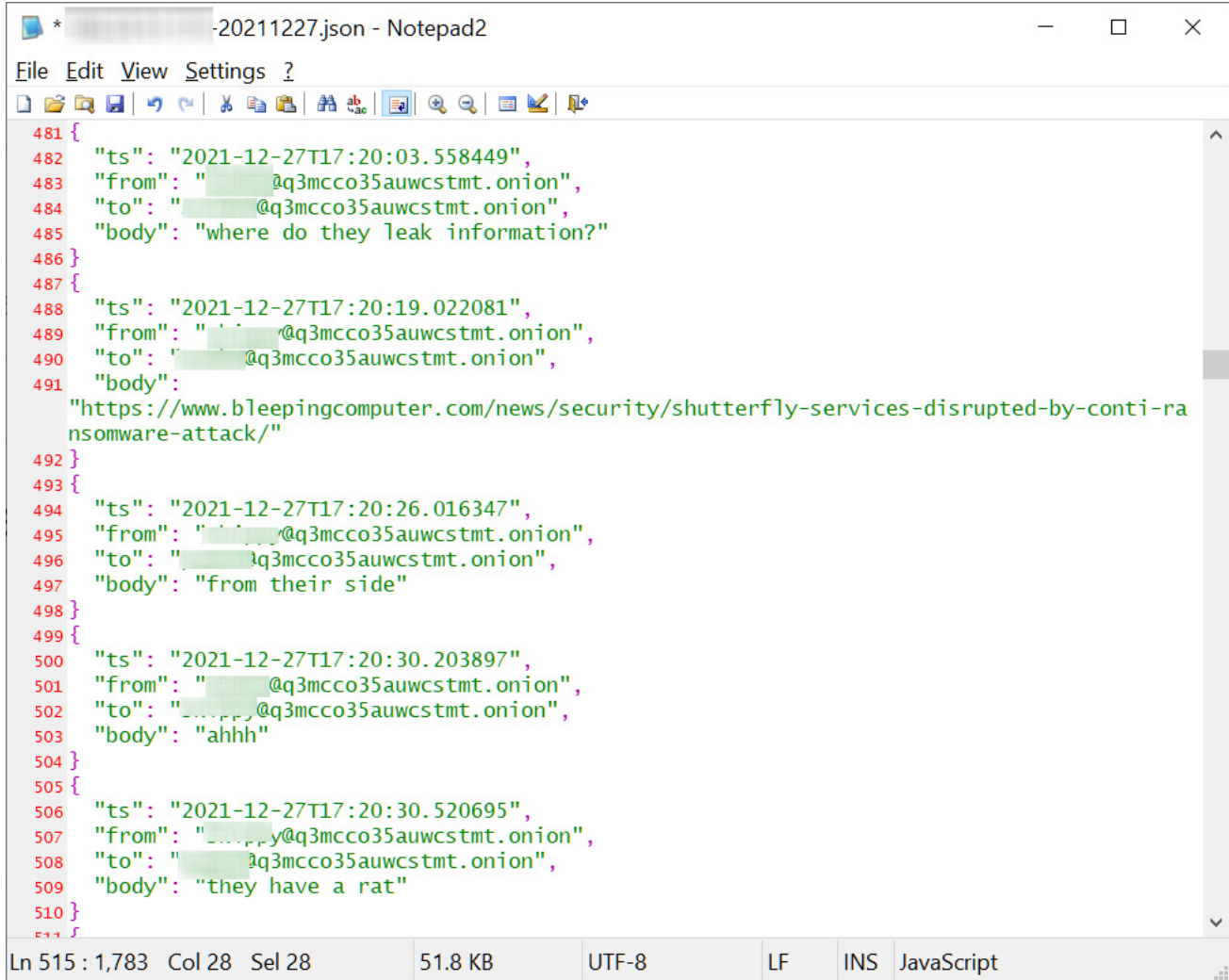
In total, there are 393 leaked JSON files containing a total of 60,694 messages since January 21, 2021, through today. Conti launched their operation in July 2020, so while it contains a big chunk of their internal conversations, it is not all of them.

	██████████-20220227.json	2/27/2022 2:21 PM	JSON File	5 KB
	██████████-20220226.json	2/26/2022 2:27 PM	JSON File	2 KB
	██████████-20220225.json	2/25/2022 5:26 PM	JSON File	7 KB
	██████████-20220224.json	2/24/2022 5:28 PM	JSON File	5 KB
	██████████-20220223.json	2/23/2022 5:29 PM	JSON File	13 KB
	██████████-20220222.json	2/22/2022 3:46 PM	JSON File	17 KB
	██████████-20220221.json	2/21/2022 5:30 PM	JSON File	39 KB
	██████████-20220220.json	2/20/2022 1:56 AM	JSON File	2 KB
	██████████-20220219.json	2/19/2022 2:29 PM	JSON File	12 KB
	██████████-20220218.json	2/18/2022 4:19 PM	JSON File	9 KB
	██████████-20220217.json	2/17/2022 3:56 PM	JSON File	23 KB
	██████████-20220216.json	2/16/2022 4:27 PM	JSON File	17 KB
	██████████-20220215.json	2/15/2022 3:05 PM	JSON File	26 KB
	██████████-20220214.json	2/14/2022 3:38 PM	JSON File	15 KB
	██████████-20220213.json	2/13/2022 7:10 AM	JSON File	2 KB
	██████████-20220212.json	2/12/2022 9:51 AM	JSON File	2 KB
	██████████-20220211.json	2/11/2022 1:55 PM	JSON File	5 KB
	██████████-20220210.json	2/10/2022 5:14 PM	JSON File	27 KB
	██████████-20220209.json	2/9/2022 12:48 PM	JSON File	12 KB
	██████████-20220208.json	2/8/2022 4:29 PM	JSON File	31 KB
	██████████-20220207.json	2/7/2022 6:01 PM	JSON File	13 KB
	██████████-20220203.json	2/7/2022 9:49 AM	JSON File	23 KB
	██████████-20220206.json	2/6/2022 4:45 PM	JSON File	14 KB
	██████████-20220205.json	2/5/2022 10:49 AM	JSON File	7 KB
	██████████-20220204.json	2/4/2022 3:42 PM	JSON File	17 KB
	██████████-20220202.json	2/2/2022 5:13 PM	JSON File	27 KB
	██████████-20220201.json	2/1/2022 3:43 PM	JSON File	16 KB
	██████████-20220131.json	1/31/2022 3:49 PM	JSON File	41 KB
	██████████-20220130.json	1/30/2022 3:21 PM	JSON File	2 KB
	██████████-20220129.json	1/29/2022 6:32 PM	JSON File	8 KB
	██████████-20220128.json	1/28/2022 4:06 PM	JSON File	26 KB
	██████████-20220127.json	1/27/2022 3:40 PM	JSON File	34 KB

Leaked Conti conversations

These conversations contain various information about the gang's activities, including previously unreported victims, private data leak URLs, bitcoin addresses, and discussions about their operations.

For example, the conversation below is the Conti members wondering how BleepingComputer learned of their attack on Shutterfly in December.



```
481 {
482   "ts": "2021-12-27T17:20:03.558449",
483   "from": "[REDACTED]@q3mcco35auwcstmt.onion",
484   "to": "[REDACTED]@q3mcco35auwcstmt.onion",
485   "body": "where do they leak information?"
486 }
487 {
488   "ts": "2021-12-27T17:20:19.022081",
489   "from": "[REDACTED]@q3mcco35auwcstmt.onion",
490   "to": "[REDACTED]@q3mcco35auwcstmt.onion",
491   "body": "https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomware-attack/"
492 }
493 {
494   "ts": "2021-12-27T17:20:26.016347",
495   "from": "[REDACTED]@q3mcco35auwcstmt.onion",
496   "to": "[REDACTED]@q3mcco35auwcstmt.onion",
497   "body": "from their side"
498 }
499 {
500   "ts": "2021-12-27T17:20:30.203897",
501   "from": "[REDACTED]@q3mcco35auwcstmt.onion",
502   "to": "[REDACTED]@q3mcco35auwcstmt.onion",
503   "body": "ahhh"
504 }
505 {
506   "ts": "2021-12-27T17:20:30.520695",
507   "from": "[REDACTED]@q3mcco35auwcstmt.onion",
508   "to": "[REDACTED]@q3mcco35auwcstmt.onion",
509   "body": "they have a rat"
510 }
511 }
```

Conversations shared with BleepingComputer about Shutterfly

Translated by Google Translate

Kremez also shared a snippet of conversation that he found discussing how the TrickBot operation was shut down, as we reported last week.

```
* [redacted]-20220214.json - Notepad2
File Edit View Settings ?
[Icons]
426 }
427 {
428   "ts": "2022-02-14T19:16:39.154766",
429   "from": "[redacted]@q3mcco35auwcstmt.onion",
430   "to": "[redacted]@q3mcco35auwcstmt.onion",
431   "body": "but I wrote the same trick - it no longer works, the project was closed"
432 }
433 {
434   "ts": "2022-02-14T19:17:57.550075",
435   "from": "[redacted]@q3mcco35auwcstmt.onion",
436   "to": "[redacted]@q3mcco35auwcstmt.onion",
437   "body": "hai!"
438 }
439 {
Ln 443 : 475 Col 74 Sel 109 14.5 KB UTF-8 LF INS JavaScript
```

Discussion about TrickBot closing down

Translated by Google Translate

There are also conversations about Conti/TrickBot's Diavol ransomware operation and 239 bitcoin addresses containing \$13 million in payments, which were added to the Ransomwhere site.

239 Bitcoin addresses representing ~\$13.1 million in payments from the Conti leak have been added to <https://t.co/IBxHWCQm7S>. The full dataset is available to download from the site. [#ransomware](#) [#Conti](#)

— Ransomwhere (@ransomwhere_) [February 27, 2022](#)

The leak of these messages is a severe blow to the ransomware operation, providing sensitive intelligence to researchers and law enforcement about their internal processes.

While the above snippets are only a tiny piece of the leaked conversations, we can expect to see far more information learned from the data in the coming weeks.

Messages leaked over Conti's siding with Russia


Earlier this week, the Conti ransomware operation published a blog post announcing their full support for the Russian government's attack on Ukraine. They also warned that if anyone organized a cyberattack against Russia, the Conti gang would strike back at critical infrastructure.

“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]

After Ukrainian Conti affiliates grew upset over the siding with Russia, the Conti gang replaced their message with another one, stating that they "do not ally with any government" and that they "condemn the ongoing war."

“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

📅 2/25/2022

👁 410

📄 0 [0.00 B]

However, their change of heart came too late, and a Ukrainian security researcher who reportedly had access to Conti's backend XMPP server emailed BleepingComputer and other journalists tonight with a link to the leaked data.

The reason shared as to why they leaked the private conversations can be read below:

Here is a friendly heads-up that the Conti gang has just lost all their sh*t. Please know this is true.

The link will take you to download an 1.tgz file that can be unpacked running `tar -xzf 1.tgz` command in your terminal .

The contents of the first dump contain the chat communications (current, as of today and going to the past) of the Conti Ransomware gang. We promise it is very interesting.

There are more dumps coming , stay tuned.

You can help the world by writing this as your top story.

It is not malware or a joke.

This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!

Russia's invasion of Ukraine has led to hackers, ransomware gangs, and security researchers picking sides in the conflict.

While some ransomware gangs have sided with Russia, others, like LockBit, are staying neutral.

On the other hand, Ukraine has [asked volunteer researchers and hackers to join their "IT Army"](#) to conduct cyberattacks on Russian targets, with many rallying to the call.

As for Conti, while this leak is embarrassing and provides immense insight into their operation, we are not likely to see them going away any time soon. With their recent [take over of the stealthy BazarBackdoor malware](#) and becoming an actual crime syndicate, they will, unfortunately, continue to be a threat.

Correction 2/28/22: This story initially stated an angry Conti affiliate who leaked the data. BleepingComputer later learned it was leaked by a Ukrainian security researcher. The article has been updated to clarify this information.

Related Articles:

[Hackers use Conti's leaked ransomware to attack Russian companies](#)

[The Week in Ransomware - April 15th 2022 - Encrypting Russia](#)

[The Week in Ransomware - May 20th 2022 - Another one bites the dust](#)

[Conti ransomware shuts down operation, rebrands into smaller units](#)

[The Week in Ransomware - May 13th 2022 - A National Emergency](#)

- [Conti](#)
- [Jabber](#)
- [Leak](#)
- [Ransomware](#)
- [Russia](#)
- [Ukraine](#)

[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.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
