Conti ransomware gang chats leaked by pro-Ukraine member

By Catalin Cimpanu

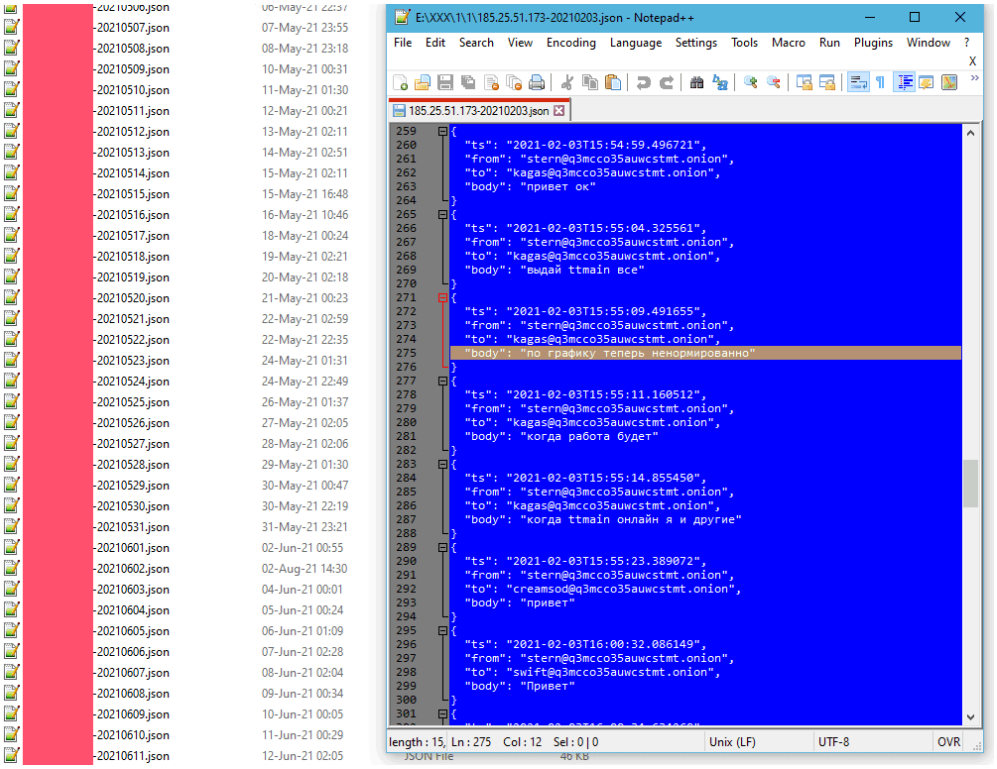
Published: 2023-01-17 · Archived: 2026-04-05 20:23:04 UTC

A member of the Conti ransomware group, believed to be Ukrainian of origin, has leaked the gang's internal chats after the group's leaders posted an aggressive pro-Russian message on their official site, on Friday, in the aftermath of Russia's invasion of Ukraine.

The message appears to have rubbed Conti's Ukrainian members the wrong way, and one of them has hacked the gang's internal Jabber/XMPP server. Internal logs were leaked earlier today via an email sent to multiple journalists and security researchers.

Dmitry Smilyanets, a threat intelligence analyst for Recorded Future, who has interacted with the Conti gang in the past, has confirmed the authenticity of the leaked conversations.

The leaked data contains 339 JSON files, with each file consisting of a full day's log. Conversations from **January 29, 2021**, to today, **February 27, 2022**, have been leaked and can be read online here, courtesy of security firm IntelligenceX.



"We promise it is very interesting," the leaker wrote in the email sent earlier today.

John Fokker, Head of Investigations at Trellix, said the chats are still being analyzed but added that "having access to internal conversations has proven to be very helpful in analyzing the crime groups TTPs" in the past.

Among the content of the leaked messages that has been identified so far, there are:

- Messages showing Conti's relationship with the TrickBot and Emotet malware gangs, from where they often rented access to infected computers to deploy their malware.
- Messages confirming that the TrickBot botnet had shut down earlier this month.
- Messages containing ransom negotiations and payments from companies that had not disclosed a breach or ransomware incident.
- Bitcoin addresses where the Conti gang received payments, which would be useful to law enforcement to track down the gang's profits.
- Messages showing that the Conti gang attempted to set up demos with security companies like CarbonBlack and Sophos in an attempt to test their tools and find evasion methods to avoid detection.

The leaker also added that the Jabber/XMPP logs are only the first part of a larger set of Conti-related files they plan to release in the future.

Conti admins misstepped; LockBit did not

But the leak is also the result of days of turmoil in the cybercriminal underground, where the Russo-Ukrainian conflict has also divided the community.

While in the past Russian and Ukrainian hackers previously worked side by side, since Tuesday, this fraternity has been under strain, with several groups choosing sides in the armed conflict between the two countries.

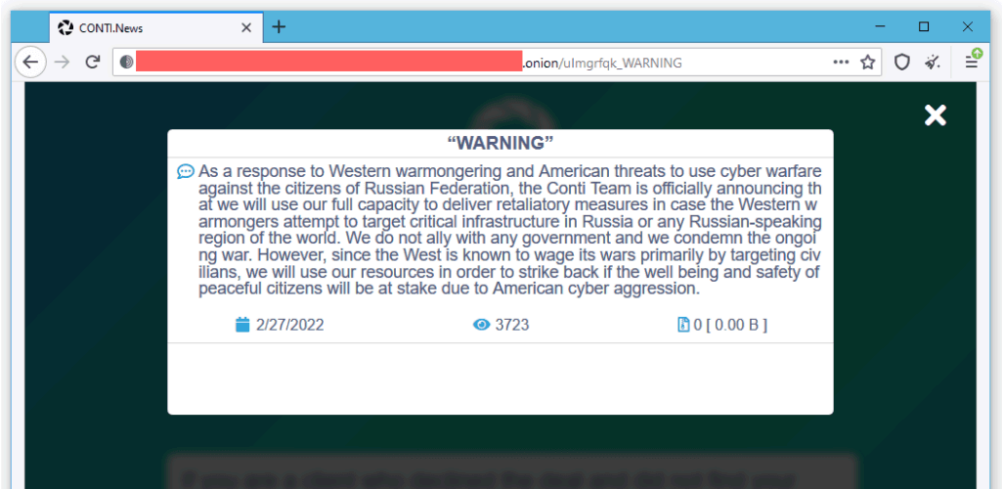
Several gangs have come forward to announce plans to launch cyberattacks in support of one of the two sides, with Conti being one of the many gangs that chose to side with Russia.

"The Conti Team is official announcing a full support of Russian government," the group said in a very aggressive message posted on Friday.

"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. [sic]"

According to FellowSecurity, this aggressive pro-Russian message is what led to one of the gang's members rebelling and leaking internal chats.

The Conti administrators realized their blunder hours later and tried to fix things by editing their blog post to have a more neutral tone, but by that point, the damage had been done.



The internal Conti drama and the leak appear to have shown other gangs not to make the same mistake. For example, in a very neutrally-worded message posted earlier today, the LockBit gang said they were not going to choose any sides.

"For us it is just business and we are all apolitical. [...] We are only interested in money for our harmless and useful work," they said.

Article updated with details about the contents of some messages, as security researchers analyze them.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
