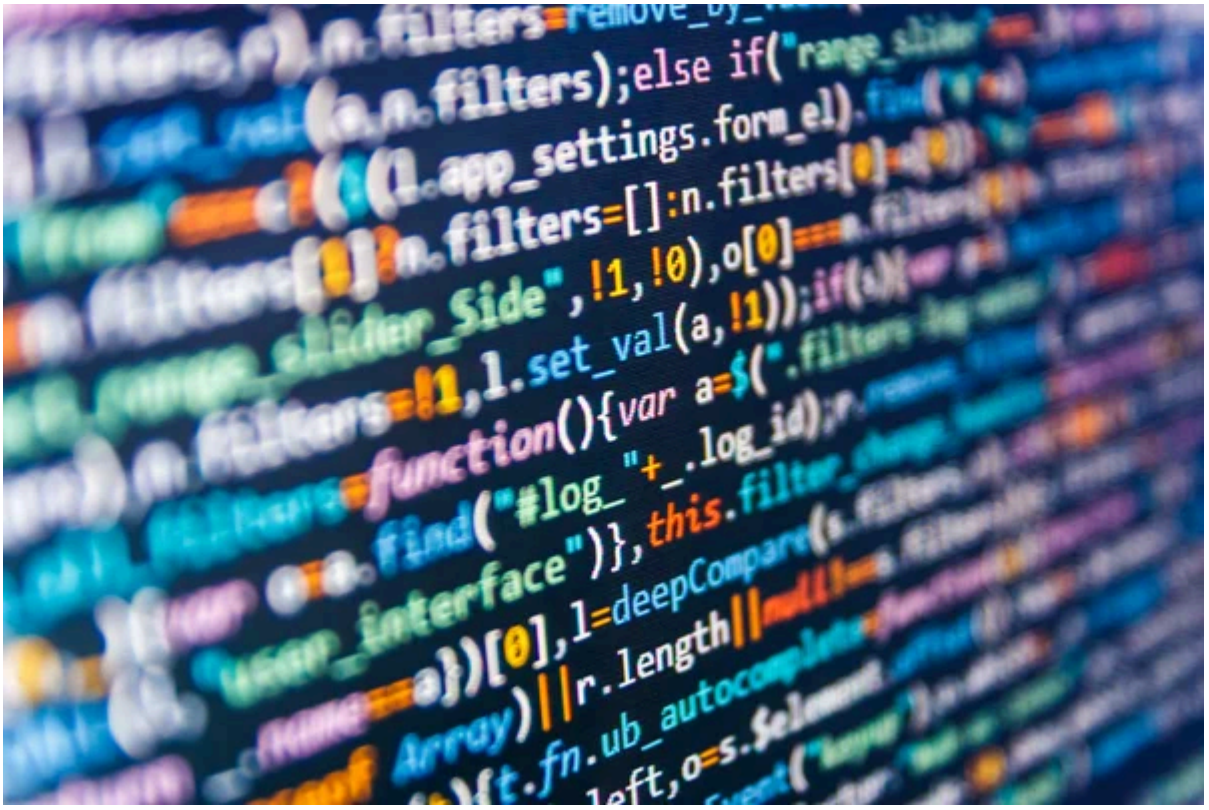
The Conti ransomware leaks demonstrate what happens when hackers support Russia

By Ofir Ashman

Published: 2022-03-22 · Archived: 2026-04-06 01:35:22 UTC

March 22, 2022 • Ofir Ashman



The Conti ransomware group rose to fame in 2020, and while it has only been active for about 3 years, it quickly became on of the most prevalent - and dangerous - ransomware operations out there. Between 2020-2021 the Conti gang raked in over $1.2 Billion in ransom payments, with the largest payment amounting to 180 million dollars. Just last year, these cyber attackers successfully deployed a ransomware attack on the Irish Healthcare system, creating dramatic human impact - and a whopping response and recovery cost of about $50,000,000.

While in the past, some Russian and Ukranian hackers have worked side by side, the current war on Ukraine (and its unprecedented use of the internet as another field of battle), even the hackers are taking sides. After Putin ordered Russian troops to invade Ukraine, the Conti gang announced its support for the Russian government in an aggressive post on their website, enraging one of the group's members or associates (probably of Ukranian origin) and costing them tons of their operation's data.

Image: vx-underground

The anonymous individual, who had internal access to the Conti ransomware group, angrily leaked a goldmine of the ransomware group's information. The first leak consisted of 60,000 internal chat messages belonging to the Conti ransomware operation that were taken from a log server for the Jabber communication system used by the gang. Over the course of a month, 170,000 conversations were leaked, providing detailed insight into the operation's activities and its member's involvement.

While the security industry was analyzing these rare messages (and while the Conti may have been losing their s#!$), a second wave of leaks hit in the form of a data dump including the ransomware's source code and decryptor, as well as TrickBot malware group chats and code components. According to a Twitter update by Emisoft's Fabian Wosar, the leaked decryptor is for a previous version of the ransomware and therefore will not work with current versions.

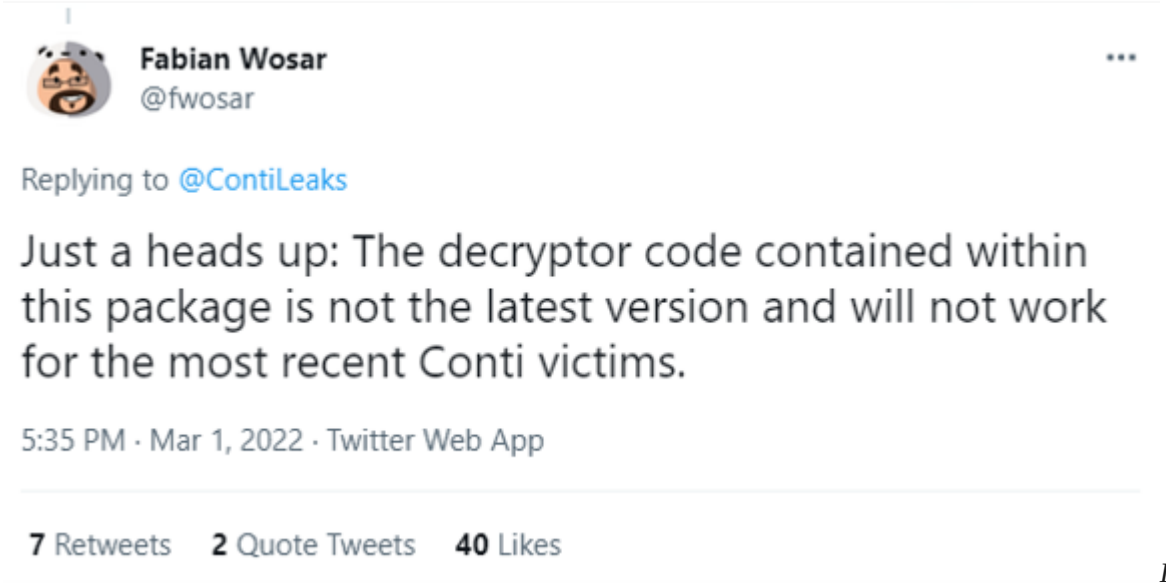


Image: Twitter

But that's not all - yesterday, the Conti Leaks twitter account posted a link to the source code for Conti V3 which had been uploaded to VirusTotal. The third Conti version is much newer, with the last update dated January 25th, 2021, with a fully functional and operational source code. Researchers at Bleeping Computer easily compiled the code and created their own ransomware based on it.

Many threat actors and ransomware gangs have been picking sides since Russia's invasion of Ukraine, while others, like LockBit, are trying to stay neutral. As the Russia-Ukraine war advances, more pressure is being set in every industry and space to help (like Ukraine asking volunteer researchers and hackers to join their "IT Army").

ThreatSTOP customers are protected from Conti and other ransomware variants using our Ransomware IP and Domain target bundles in policies that are enforced by firewalls, DNS servers, and more. We also offer a Russian-Controlled Entities Target which protects our customers from network communications with all IP addresses owned or taken over by Russia.

Not a ThreatSTOP customer yet? Want to see ThreatSTOP instantly eliminate attacks like Conti ransomware on your network?

Get a Demo

For live updates on the attack on Conti group, check out the Twitter handle @ContiLeaks.
