Conti Ransomware V. 3, Including Decryptor, Leaked

By Lisa Vaas

Published: 2022-03-21 · Archived: 2026-04-05 22:45:04 UTC

The latest is a fresher version of the ransomware pro-Ukraine researcher ContiLeaks already released, but it's reportedly clunkier code.

Pro-Ukraine security researcher @ContiLeaks yesterday uploaded a fresher version of Conti ransomware than they had previously released – specifically, the source code for Conti Ransomware V3.0 – to VirusTotal.

ContiLeaks posted a link to the code on Twitter. The code includes a compiled locker and decryptor, according to vx-underground, which has been archiving the leaks.

The archive is password-protected, but the password is easy to figure out, according to replies to ContiLeaks' release.

ContiLeaks followed up in a few hours by thumbing their nose at the pro-Russia law enforcement that the researcher said is looking for them in the UA – in other words, in Ukraine.

"i can tell you good luck mf!" ContiLeaks tweeted, using another acronym that probably doesn't need explaining.

Crap Code?

The code is apparently legitimate.

BleepingComputer compiled the newly released source code for Version 3 of Conti ransomware without any issues, successfully creating the gang's executables for encrypting and decrypting files.

But just because it works doesn't mean it's an improvement, some said.

After analyzing the source code, Payload – a Polish magazine about offensive IT security – dismissed Version 3 as being a "giant step back" from Version 2 in terms of code quality.

Maybe the changes between versions were done by a flunky dev, Payload suggested in its response to vx-underground. "We analyzed it. There is […] very little improvement, and giant step back in terms of source code quality. Most probably these changes were made by someone else than original developer."

For those who are combing through Conti code, you're better off sticking with the "cleaner" 2.0, Payload suggested. "But definitely: if anyone wants to learn anything from this code, please move to Conti 2.0, it's a lot cleaner and overall better to start with," Payload said.

Ross Williams, director of digital forensics and incident response (DFIR) at managed detection and response (MDR) services provider CRITICALSTART, told Threatpost on Monday that from a DFIR perspective, these leaks give security professionals and responders "insight into the gang's tactics, techniques and procedures as well as indicators of compromise." The information enables them "to identify a breach or infection more quickly and to thereby slow the spread of ransomware," Williams said via email.

It also gives anyone with the motivation and skillset to penetrate a network the tools they need to create their own ransomware gang: The criminally inclined can just use the Conti software along with its training manuals, which were also leaked, noted BreachQuest Head of Product Marco Figueroa.

With all this access to Conti code, tools and tactics, a hit from "Conti" could be close to a hit from "your guess is as good as mine."

"I believe the only way to verify that a victim was hit with 'Sterns Conti gang' is by tracking the payment to bitcoin addresses," Figueroa said. "Stern" is a reference to the name used by one of the Conti group's top managers.

The Conti Gutting Continues

This is just the latest in a series of leaks following ContiLeaks' promise to eviscerate the Conti group – a promise of revenge that followed Conti's having pledged support for the Russian government over its invasion of Ukraine.

ContiLeaks' earlier spills included an older version of Conti ransomware source code – one that dated to Jan. 25, 2021. Version 3.0 – the one released on Sunday – is over a year newer.

In their earlier leaks, ContiLeaks has also divulged source code for TrickBot malware, a decryptor and the gang's administrative panels, among other core secrets.

The leaks – an act of revenge wrought upon the cybercrooks who've sided with Russia in the war (one among the thousand cuts that have been bleeding Russia as cybercrooks take sides) – have also included nearly 170,000 chat conversations between the Conti ransomware gang members, covering more than a year from January 2021 through February 2022.

It's a treasure trove that researchers have spent weeks poring over, discovering the inner workings of the extortionists' dark business, its top brass and far more.

For example, a clear picture of Conti company culture has arisen from the leaks. For one thing, it's run like a legit high-tech company, offering bonuses, employee-of-the-month and other such benefits, researchers say. Chat logs also have shown that bored top management have mulled working on something new: say, Conti's own altcoin alternative to Bitcoin.

New Conti Affiliate Discovered

In related news, on Monday, eSentire's Threat Research Unit (TRU) published a report about a new Conti affiliate group. The report details new accounts, specific IP addresses, domain names and Protonmail email accounts linked to the affiliate, Indicators of Compromise that organizations should address immediately, an overview of

attack vectors, and how the affiliate is – like so many criminals – abusing the Cobalt Strike intrusion framework for attack purposes.

eSentire's report details one such Cobalt Strike incident, nicknamed ShadowBeacon, during which the Cobalt beacons were being deployed from the domain controllers via PsExec: a legitimate admin tool used for remotely executing binaries.

Together with BreakPoint Labs (BPL), TRU observed threat actors leveraging the Cobalt Strike infrastructure to attack seven different U.S. companies between 2021 and 2022. According to eSentire, victims included companies in the financial, environmental, legal and charitable sectors.

"The Windows logs revealed that the threat actor had been able to register their own virtual machine on the victim organization's network," the report noted, "using it as a pivot to their actual, exterior [command-and-control, aka C2, server]."

Data in Motion Most at Risk in Ransomware Attacks

To protect from ransomware attacks, Rajiv Pimplaskar, CEO of the VPN company Dispersive Holdings, told Threatpost on Monday that organizations should look beyond protecting data at rest: the data that's at risk of getting paralyzed in a ransomware attack. "Information is most vulnerable for a data breach or malware infection" when it's in motion, the CEO cautioned.

"Network resources are prime targets for Ransomware as a Service (RaaS) actors as they can be ideal vectors for insider threats, code and injection attacks, Man In The Middle (MITM), privilege escalation as well as lateral movement," Pimplaskar said via email.

Pimplaskar suggested that, beyond establishing proper access control and device posture checking to prevent unauthorized access, "network security must also be bolstered with advanced capabilities such as managed attribution and active data multi-pathing. These capabilities obfuscate network soft targets as well as keep data secure from hostile detection and interception."

032122 14:90 UPDATE: Added input from Ross Williams.

032122 16:43 UPDATE: Added input from Marco Figueroa.

032122 18:05 Corrected explanation of UA: It is, in fact, the two-letter acronym for Ukraine.
