Conti Ransomware Decryptor, TrickBot Source Code Leaked

By Lisa Vaas

Published: 2022-03-02 · Archived: 2026-04-06 01:24:54 UTC

The decryptor spilled by ContiLeaks won't work with recent victims. Conti couldn't care less: It's still operating just fine. Still, the dump is a bouquet's worth of intel.

The pro-Ukraine member of the Conti ransomware gang who promised to eviscerate the extortionists after they pledged support for the Russian government has spilled yet more Conti guts: The latest dump includes source code for Conti ransomware, TrickBot malware, a decryptor and the gang's administrative panels, among other core secrets.

On Monday, vx-underground – an internet collection of malware source code, samples and papers that's generally considered to be a benign entity – shared on Twitter a message from a Conti member saying that "This is a friendly heads-up that the Conti gang has just lost all their sh•t."

The first of what ContiLeaks promised would be a series of "very interesting" leaks included 60,000 of the Conti gang's internal chat messages.

The Conti Intel Treasure Trove

Then, on Tuesday, ContiLeaks leaked even more of Conti's common tactics, techniques and procedures (TTPs), which were shared by vx-underground.

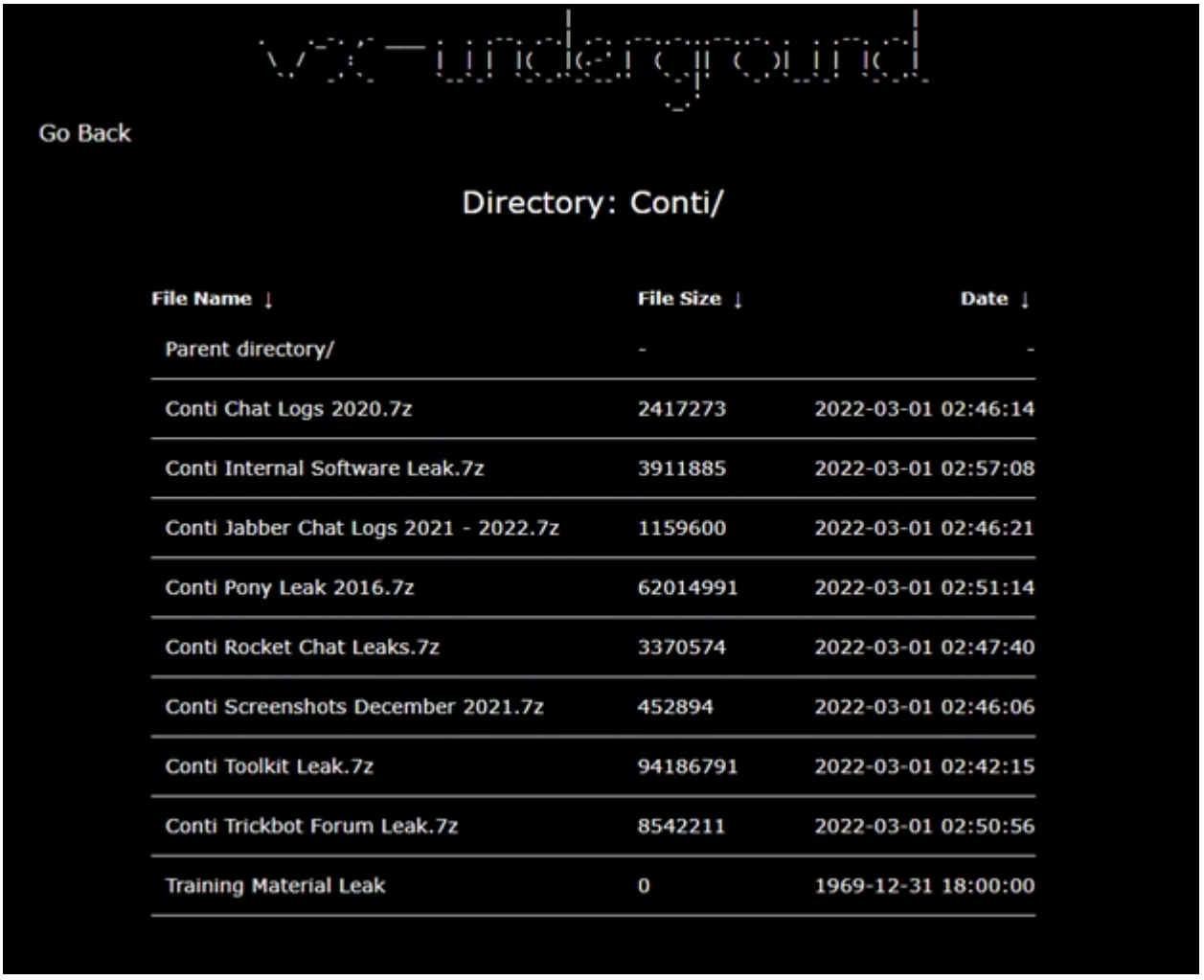
In a Wednesday analysis, CyberArk researchers enumerated the leaked content and why it's important. This intel is vital as Russian tanks roll through Ukraine and cyberattacks fly in support of either aiding the besieged country or tripping up the aggressor, CyberArk researchers asserted.

Its analysis pointed to a cybersecurity bulletin issued jointly over the weekend by the Cybersecurity and Infrastructure Agency (CISA) and the FBI: an advisory that warned that Russia's attack on Ukraine – which has included cyberattacks on Ukrainian government and critical infrastructure organizations – may spill over Ukraine's borders, particularly in the wake of sanctions imposed by the United States and its allies.

"As cybersecurity researchers, we believe insight gained from these leaks is incredibly important to the cybersecurity community at large. Ongoing awareness and visibility into the leaked tools while supporting the need for continued vigilance is critical during this time, and reinforced by [the CISA/FBI alert]."

What's in the Second Dump

The files shared by ContiLeaks have a slew of fresh meat, with some dated as recently as yesterday, March 1.



Go Back

Directory: Conti/

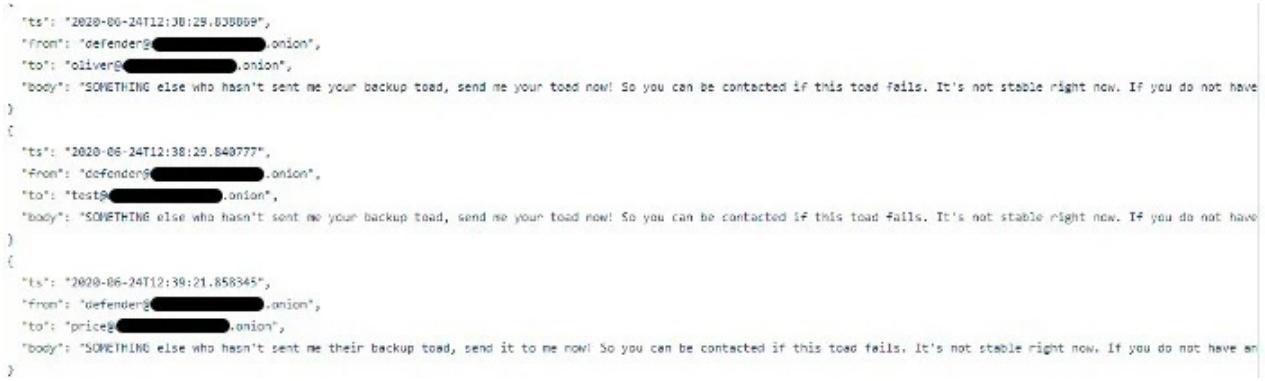
File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1159600	2022-03-01 02:46:21
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Training Material Leak	0	1969-12-31 18:00:00

ContiLeaks' data dump content as of March 1. Source: vx-underground.

Here's a selection of the repositories and what researchers can do with them:

Chats

As far as the leaked chats go, they span internal communications of the Conti gang between June and November 2020. CyberArk noted that one user in particular "frequently spams all the other users."




```
{
  "ts": "2020-06-24T12:38:28.838888",
  "from": "defender@[redacted].onion",
  "to": "oliver@[redacted].onion",
  "body": "SOMETHING else who hasn't sent me your backup toad, send me your toad now! So you can be contacted if this toad fails. It's not stable right now. If you do not have
}
{
  "ts": "2020-06-24T12:38:28.840777",
  "from": "defender@[redacted].onion",
  "to": "test@[redacted].onion",
  "body": "SOMETHING else who hasn't sent me your backup toad, send me your toad now! So you can be contacted if this toad fails. It's not stable right now. If you do not have
}
{
  "ts": "2020-06-24T12:39:21.858345",
  "from": "defender@[redacted].onion",
  "to": "price@[redacted].onion",
  "body": "SOMETHING else who hasn't sent me their backup toad, send it to me now! So you can be contacted if this toad fails. It's not stable right now. If you do not have an
}
```

This can also be a useful tool for us to investigate since we can see maybe even all the usernames in one place, allowing us to enumerate all the people in the Conti group.

The chats will enable researchers to see a good chunk of Conti gang usernames in one place, researchers said, "allowing us to enumerate all the people in the Conti group."

Admin Panel Code

A quick look at the cache's repositories led the researchers to surmise that most of the code Conti uses appears to be open-source software. They pointed to two examples: the two PHP frameworks yii2 and Kohana, which are "used as part of (what seems to be) the admin panel," they said.

"The code is mostly written in PHP and is managed by Composer, with the exception of one repository of a tool written in Go," they said. The repositories also contain some config files that list local database usernames and passwords, as well as a few public IP addresses.

Credentials Ripped Off by Pony Malware

The Conti Pony Leak 2016 repository contains a collection of email accounts and passwords – including from mail services such as gmail.com, mail.ru and yahoo.com – that were apparently stolen from various sources by the Pony credential-stealing malware: a credential stealer that, at least as of 2018, was crooks' favorite stealer.

It also contains credentials from FTP/ RDP and SSH services, plus credentials from different websites.

TTPs

The Conti Rocket Chat Leaks contains a chat history of Conti members swapping tips about targets and carrying out attacks via crooks' favorite: Cobalt Strike, the legitimate, commercially available tool used by network penetration testers and by crooks to sniff out vulnerabilities.

The Conti gang chatters talked about these techniques:

- Active Directory Enumeration
- SQL Databases Enumeration via sqlcmd.
- How to gain access to Shadow Protect SPX (StorageCraft) backups.
- How to create NTDS dumps vs vssadmin
- How to open New RDP Port 1350

And these tools:

- Cobalt Strike
- Metasploit
- PowerView
- ShareFinder
- AnyDesk
- Mimikatz

Conti Locker v2 & the Decryptor That Probably De-Won't

The dump also contains the source code for Conti Locker v2, which was first leaked as a password-protected zip file but then again without any password.

Besides the source code for v2 of the ransomware encryption source code, the leak also contained source code for the decryptor – a decryptor that reportedly won't work, as pointed out on Twitter.

"I had heard it's not the latest version and does not work," Marcus confirmed.

The released decryptor might be a version that Conti sends to victims who've paid the ransom, he suggested.

Decryptors act kind of like unzipping a password-protected file, he suggested, except that they're more complex, given that they vary by the ransomware family.

"Some are built into a standalone binary, others can be remote-enabled. Usually they have keys built into them," Marcus described.

Conti Training Materials

The leaked documents also contain training materials, including videos of online courses in Russian, as well as how-tos about this list of TTPs:

- Cracking
- Metasploit
- Network Pentesting
- Cobalt Strike
- PowerShell for Pentesters
- Windows Red Teaming
- WMI Attacks (and Defenses)
- SQL Server
- Active Directory
- Reverse Engineering

Conti training in Russia. Course: CyberArk.

TrickBot Leaks

One of the leaked files is a dump of chats from the forums used by the operators of the TricKBot trojan/malware, spanning forum messages from 2019 until 2021.

Most of the chats are about how to move laterally across networks and how to use certain tools, but CyberArk also found out quite a bit about the TrickBot and Conti gang's TTPs.

"For instance in one of the correspondences a member shares his web shell of choice, 'he lightest and most durable webshell I use,'" researchers said.

Also included are evidence from early July 2021 that the group used exploits such as Zerologon: Not surprising, given that starting in September 2020, at least four public proof-of-concept (PoC) exploits for the flaw were released on Github, along with technical details of the vulnerability.

Other TrickBot leaks include server-side components written in Erlang, a trickbot-command-dispatcher-backend and trickbot-data-collector-backend, dubbed lero and dero.

Thank heavens for the readable code, said one Twitter commenter: "That's finally something worth reviewing (Conti Trickbot Leaks.7z file) – clean, reusable implementation in Erlang, better than several open source Erlang server examples."

TrickBot Code Could Lead to … Better TrickBot

Will the leak slow down TrickBot operators? Well, it didn't actually have to, since the operators already seem to have taken a few hits of Zanax.

Last week, researchers at Intel 471 published a report about how the group behind the TrickBot malware is back after an unusually long lull between campaigns. If not a full stop, they've been operating pretty languidly: from Dec. 28, 2021 until Feb. 17, Intel 471 researchers hadn't seen any new TrickBot campaigns.

Researchers said at the time that the pause could be due to the TrickBot gang making an operational shift to focus on partner malware, such as Emotet.

The ContiLeaks source code leak could, however, change the scene, and not for the better. David Marcus, senior director of threat intelligence at threat-intel security company LookingGlass, told Threatpost on Wednesday that the leaks will have "a huge impact" long term as security researchers continue to research the fresh data. "The amount we will learn about their tactics, code development, monetization efforts, potential members and such cannot be overstated," he said via email.

But as far as the source code leak is concerned, that will be a double-edged sword, he cautioned. "It will benefit researchers from a defensive point-of-view, as a better understanding of how TrickBot works will allow for better defensive measures," he said. "The flip side of that is that it will also allow for more TrickBot development by more malware writers."

Conti Couldn't Care Less

As far as the leak of Conti code goes, it would be nice to think that the gang's operators were howling in pain at the disclosures, but that's not exactly what's happening.

Yelisey Boguslavskiy, head of research at the threat intel firm Advanced Intelligence (AdvInt), told Threatpost on Wednesday that none of the firm's primary source intel demonstrates that this will affect Conti.

"The leak was related to only one group out of six, and even though this group was likely the most important one, the rest of the teams were not impacted at all," he explained. "Conti relaunched all of its infrastructural capacities and keep operating."

Source: https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/