Kaspersky releases tool for decrypting Conti-based ransomware

By Kaspersky

Published: 2023-03-16 · Archived: 2026-04-05 20:04:52 UTC

Woburn, MA – March 16, 2023 – Kaspersky has published a new decryption tool that helps victims of a ransomware modification based on previously leaked Conti source code. Conti is a ransomware gang that has dominated the cybercrime scene since 2019, and whose data, including source code, was leaked in March 2022, following an internal conflict caused by geopolitical crisis in Europe. The discovered modification was distributed by an unknown ransomware group and has been used against companies and state institutions.

In late February 2023, Kaspersky experts uncovered a new portion of leaked data published on forums. After analyzing the data, which contained 258 private keys, source code and some pre-compiled decryptors, Kaspersky released a new version of the public decryptor to help victims of this modification of Conti ransomware.

Conti appeared in late 2019 and was very active throughout 2020, accounting for more than 13 percent of all ransomware victims during this period. However, a year ago, once the source code was leaked, multiple modifications of Conti ransomware were created by various criminal gangs and used in their attacks.

The malware variant whose keys were leaked had been discovered by Kaspersky specialists in December 2022. This strain was used in multiple attacks against companies and state institutions.

The leaked private keys are located in 257 folders (only one of these folders contains two keys). Some of them contain previously generated decryptors and several ordinary files: documents, photos, etc. Presumably the latter are test files – a couple of files that the victim sends to the attackers to make sure that the files can be decrypted.

Thirty-four of these folders have explicitly named companies and government agencies. Assuming that one folder corresponds to one victim, and that the decryptors were generated for the victims who paid the ransom, it can be suggested that14 victims out of the 257 paid the ransom to the attackers.

After analyzing the data, the experts released a new version of the public decryptor to help victims of this modification of the Conti ransomware. The decryption code and all 258 keys were added to the latest build of Kaspersky's utility RakhniDecryptor 1.40.0.00. Moreover, the decryption tool has been added to Kaspersky's "No Ransom" site (https://noransom.kaspersky.com).

"For many consecutive years, ransomware has remained a major tool used by cybercrooks," said Fedor Sinitsyn, lead malware analyst at Kaspersky. "However, because we have studied the TTPs of various ransomware gangs and found out that many of them operate in similar ways, preventing attacks becomes easier. The decryption tool against a new Conti-based modification is already available on our 'No Ransom' webpage. However, we would like to emphasize that the best strategy is to strengthen defenses and stop the attackers at early stages of their intrusion, preventing ransomware deployment and minimizing the consequences of the attack."

To protect yourself and your business from ransomware attacks, consider following the rules proposed by Kaspersky:

- Do not expose remote desktop services (such as RDP) to public networks unless absolutely necessary and always use strong passwords for them.
- Promptly install available patches for commercial VPN solutions providing access for remote employees and acting as gateways in your network.
- Focus your defense strategy on detecting lateral movements and data exfiltration to the Internet. Pay special attention to the outgoing traffic to detect cybercriminals' connections.
- Back up data regularly. Make sure you can quickly access it in an emergency when needed.
- Use solutions like Kaspersky Endpoint Detection and Response Expert and Kaspersky Managed Detection and Response service, which help to identify and stop the attack on early stages, before attackers reach their final goals.
- Use the latest Threat Intelligence information to stay aware of actual TTPs used by threat actors. The Kaspersky Threat Intelligence Portal is a single point of access for Kaspersky's TI, providing cyberattack data and insights gathered by our team for 25 years. To help businesses enable effective defenses in these turbulent times, Kaspersky has announced access to independent, continuously updated and globally sourced information on ongoing cyberattacks and threats, at no charge. Request access to this offer here.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments, and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies, and we help 240,000 corporate clients protect what matters most to them. Learn more at usa.kaspersky.com.

Media Contact

Sawyer Van Horn

sawyer.vanhorn@Kaspersky.com

(781) 503-1866
