Conti Ransomware

Archived: 2026-04-05 20:44:02 UTC

Conti Ransomware Recovery, Payment & Decryption Statistics

The information below describes relevant statistics of Conti ransomware recovery, payment and decryption. The recovery process of Conti ransomware includes identifying the strain and the risk associated with pursuing a ransom payment for data decryption. Please review the information below, or contact our support team, to learn more about Conti ransomware recovery, payment and decryption statistics.

HOW MUCH ARE Conti RANSOMWARE RANSOM DEMANDS?

Conti targets mid to large size enterprises and ransom amounts are scaled based on the size of the organization and the perceived capacity to pay. This group is also known to exfiltrate data, which leads to increased demands.

Conti RANSOMWARE: RANSOM AMOUNTS

Average Conti Ransom Payment (June 2022)

$110,000

HOW LONG DOES IT TAKE TO RECOVER FROM A Conti RANSOMWARE ATTACK?

Conti incidents reflect slightly less than average recovery times. The decryptor is fairly straightforward to use and the decryption rate depends on the complexity of the network.

WHAT DATA RECOVERY RATE IS EXPECTED WHEN PAYING FOR A Conti RANSOMWARE DECRYPTOR?

The data recovery rate for Conti is high and the tool is fairly straightforward to use.

Immediate CONTI Ransomware Help

Contact us for help assessing your case. Assessments are free and all information shared is treated as confidential.

For immediate assistance contact us

Conti RANSOMWARE FREQUENTLY ASKED QUESTIONS

1. ARE THERE FREE CONTI DECRYPTION TOOLS?

The majority of active Conti ransomware variants can not be decrypted by any free tool or software. If you submit a file example to us, we will have a look for free and let you know. There are also good free websites that you can upload a sample file to and independently check. **You should NOT pay a data recovery firm or any other service provider to research your file encryption.** They will use the same free resources noted above… so don't waste your money or time!

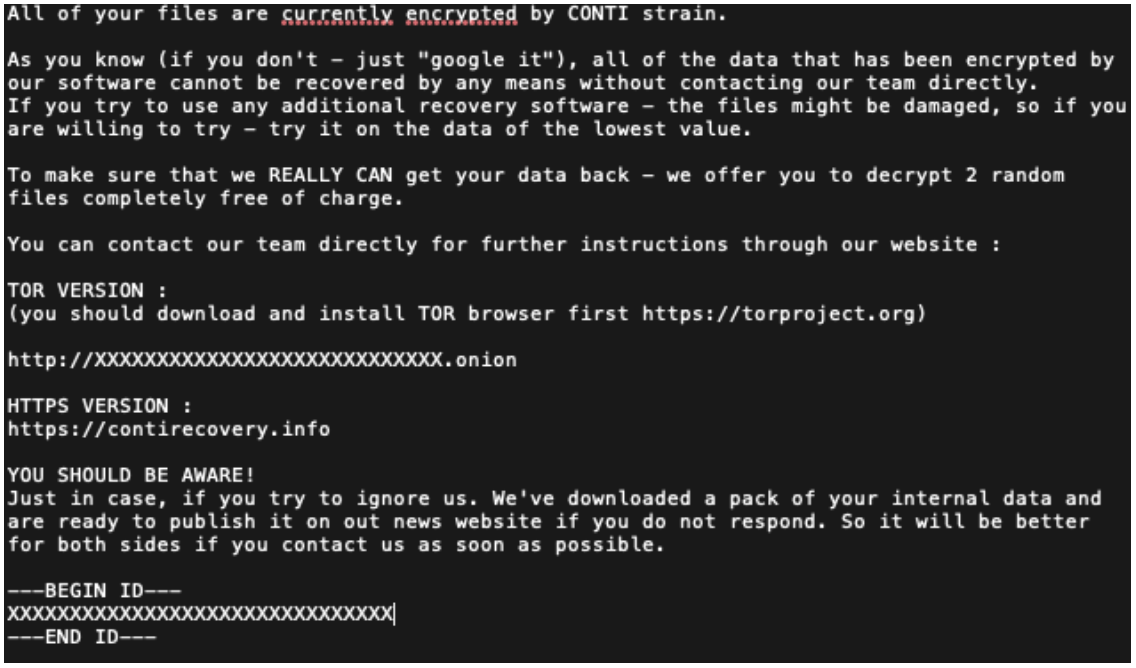
2. HOW DID I GET INFECTED WITH CONTI RANSOMWARE?

Most Conti ransomware is laid directly by a hacker that has accessed an unprotected RDP port, utilized email phishing to remote into a network via an employee's computer, or utilized malicious attachments, downloads, application patch exploits or vulnerabilities to gain access to a network.

3. WHAT ARE RECENT CONTI RANSOMWARE FILE EXTENSIONS?

Conti extensions are randomized. Encrypted files on a given network will have their own unique extension and a readme.txt ransom note will be stored on each host.

4. WHAT DOES A CONTI RANSOM NOTICE LOOK LIKE?



The ransom note is a fairly vague and is comparable to several other variants. The threat actor states that the only way to decrypt files is by purchasing a decryptor and they provide a TOR site for communications. Lastly, the group usually exfiltrates data from networks and the note emphasizes that the data will be leaked if a payment is not made.

RANSOMWARE FREQUENTLY ASKED QUESTIONS

WHAT INFORMATION DO I NEED TO PROVIDE?

You will need to provide information from both the ransom notice and a sample encrypted file. We will schedule a call to discuss the severity of the attack, the operability of your company and the likely timeline / cost of recovering from the attack. You will also need to provide identifying information on your company, and an authorized representative of your company.

HOW MUCH WILL THIS COST?

You are already being extorted; we don’t think you deserve to pay another large fee. Coveware charges flat per incident fees. Whether the case lasts one week or three weeks, our fees are flat. We do not charge spreads of fees tied to the size of the ransom amount. Our fees will never be even close to the amount of the ransom demanded by the cyber criminal, and you should be skeptical of why any other service provider would charge a fee that high.

WHAT ABOUT FIRMS THAT HAVE TOLD ME THEY CAN DECRYPT MY FILES WITHOUT PAYING THE HACKER?

You should be extremely skeptical of any data recovery firm that claims they can decrypt ransomware. Typically they are just paying the cyber criminal without your knowledge and pocketing the difference between the ransom amount and what they will charge you. Know the facts before you engage. If the ransomware IS decryptable, the tool can be found for free. If not, purchasing a key from the cyber criminal is the only way to unlock your files.

While Coveware does not condone paying cyber criminals, we recognize it is often the only choice if backups are not available or have become compromised as well. If that is the case, you deserve an honest, transparent experience.

WILL THE RANSOMWARE PAYMENT BE SUCCESSFUL?

There is no guarantee that paying the ransom will result in a working decryption tool being delivered. However, Coveware believes that data aggregation can help customers make the most informed data-driven decisions. Since we handle lots of cases of the same ransomware types, we are able to share our experiences and help customers decide how to proceed.

HOW DO I UNLOCK MY FILES?

If the ransomware payment is successful, a decryption tool & key is provided by the hacker that can be used to manually decrypt your files.

HOW DO I PREVENT THIS FROM HAPPENING AGAIN?

There are some common security mis-configurations that lead to a ransomware attack. We can share some tips and resources for preventing future attacks, but encourage companies to perform a full forensic review or security assessment as soon as possible. Consistent investment in security IT is the best antidote to preventing future attacks.

WHY CHOOSE COVEWARE RANSOMWARE RECOVERY SERVICES?

FREE
RANSOMWARE ASSESSMENT

Provide a few details from the ransom notice, an example encrypted file and details of the operability of your company and budget/time. We will provide context into the severity of the attack and your options for decryption and recovery using our database of similar cases.

- Identify ransomware type
- Find free decryptor tools

- Identify threat actor group

24x7 SUPPORT
- RANSOMWARE INCIDENT RESPONSE

We have deep experience communicating and negotiating with hackers. It's what we do all day long! Take advantage of our experience and allow us to shoulder this burden.

- Secure & safe negotiations
- Proactive service
- Transparent communications
- Determine risks & outcomes

FILE DECRYPTION
& RECOVERY SUPPORT

Coveware has access to a ready supply of any crypto currency, and offers a 15 minute disbursement service level agreement. We also support the decryption/data recovery process.

- Professional IT support
- Insurance documentation
- Post-incident follow up

- Post-incident support

How does Coveware help our partners?
