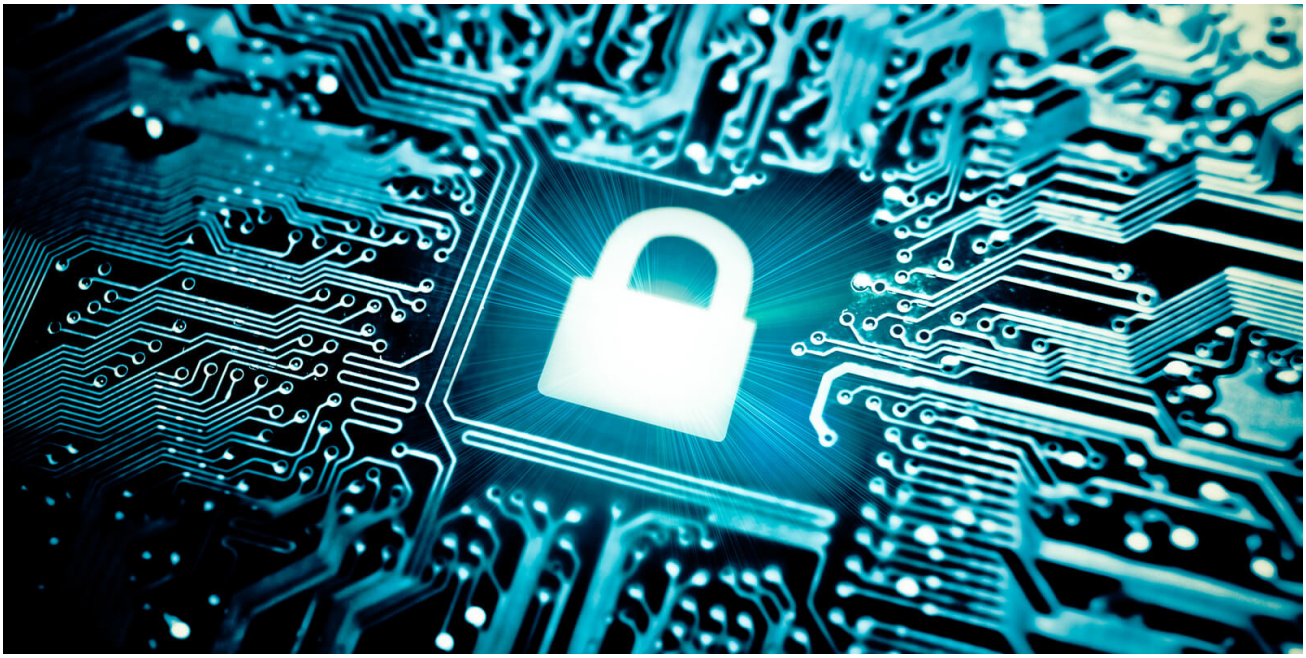
Ryuk successor Conti Ransomware releases data leak site

bleepingcomputer.com/news/security/ryuk-successor-conti-ransomware-releases-data-leak-site/

Lawrence Abrams

By
Lawrence Abrams

- August 25, 2020
- 01:49 PM
- 0



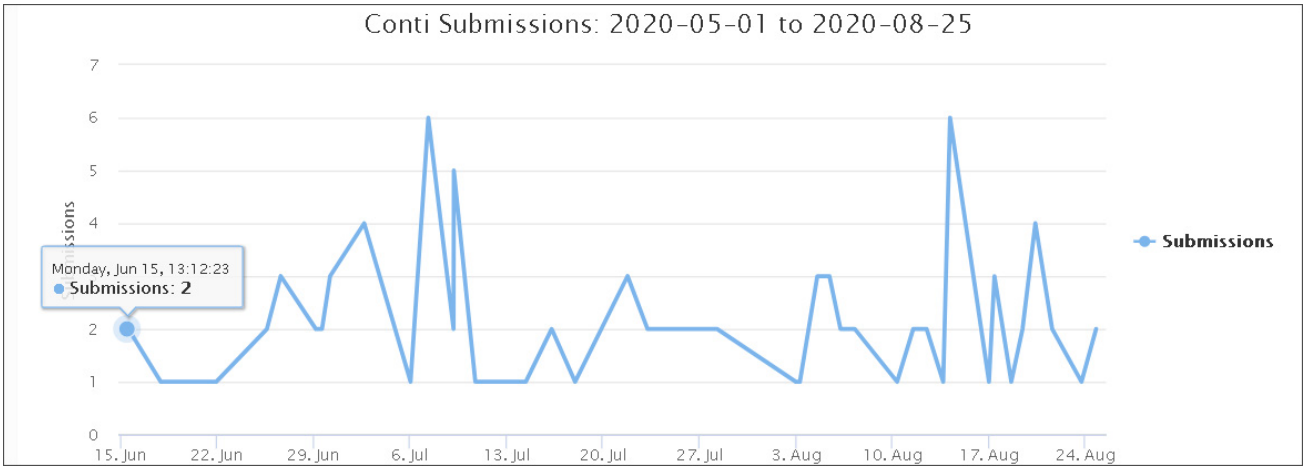
Conti ransomware, the successor of the notorious Ryuk, has released a data leak site as part of their extortion strategy to force victims into paying a ransom.

In the past, when the TrickBot trojan infected a network, it would eventually lead to the deployment of the Ryuk ransomware as a final attack.

According to Advanced Intel's Vitali Kremez, since July 2020, Ryuk is no longer being deployed, and in its place, the TrickBot-linked operators, are now deploying the Conti ransomware.

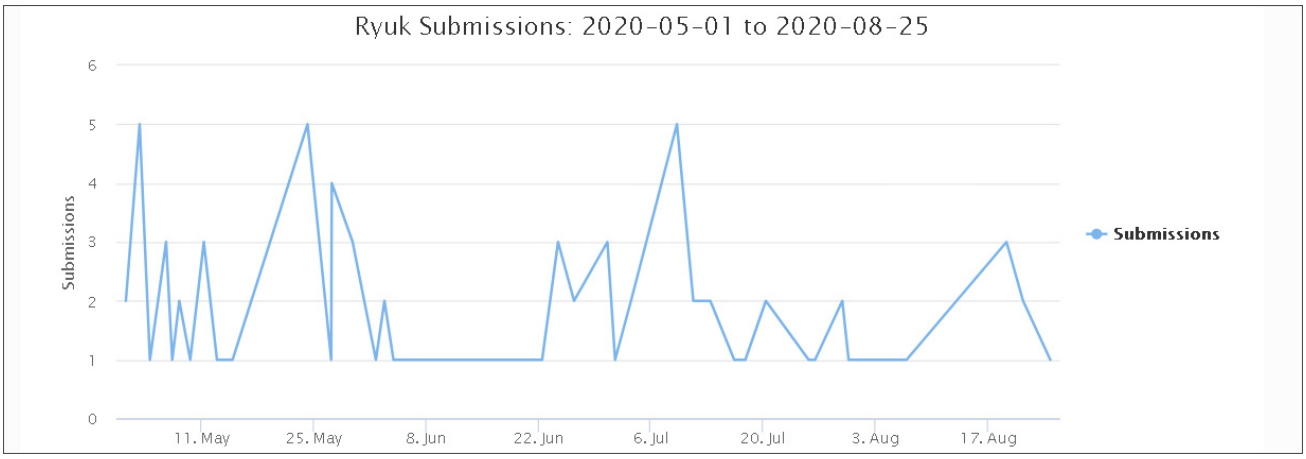
Conti is a relatively new private Ransomware-as-a-Service (RaaS) that has recruited experienced hackers to distribute the ransomware in exchange for a large share of the ransom payment.

Submissions to ransomware identification site ID Ransomware also show the increased activity of Conti ransomware since June 15th.



Conti submissions to ID-R

Ryuk on the other hand, has seen a steady decline since July.



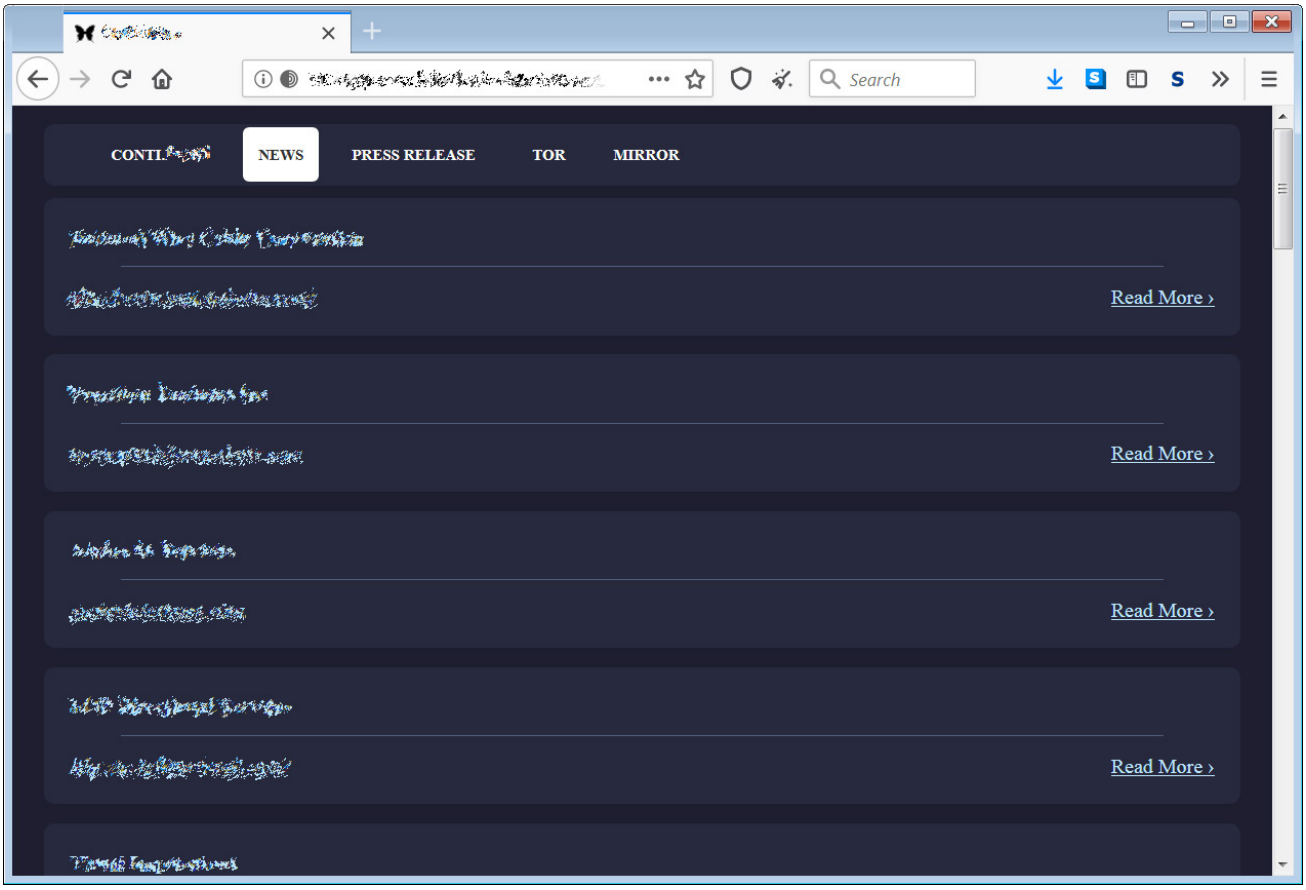
Ryuk subnmissions

Conti releases a data leak site

When human-operated ransomware operations attack a corporate network, they commonly steal unencrypted data before encrypting the files.

This stolen data is then used as leverage to get a victim to pay the ransom under threat that the files will be released on ransomware data leak sites.

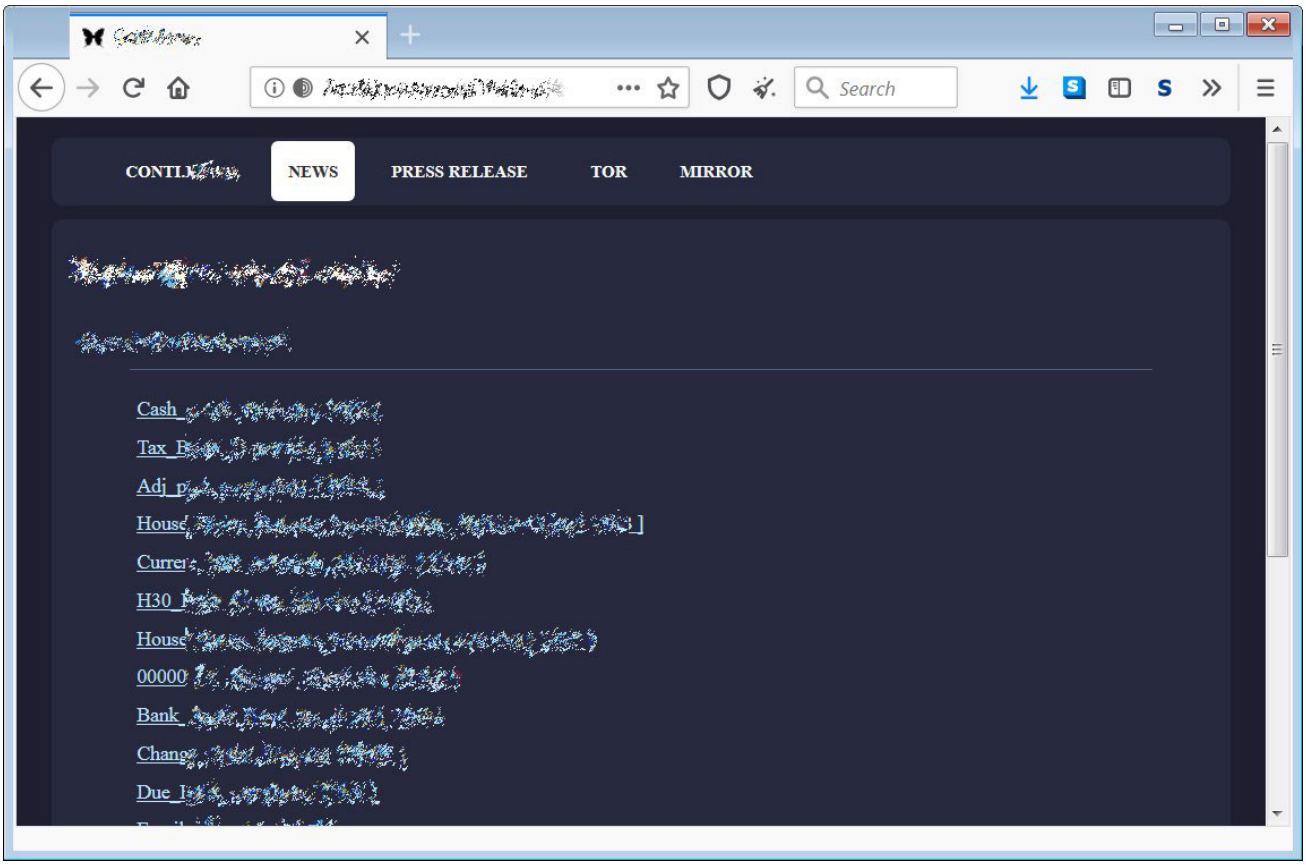
Conti ransomware has been active since this summer, but it wasn't until recently that it released its own 'Conti.News' data leak site.



Conti data leak site

This data leak site currently lists twenty-six victims, with some of the names being large and well-known companies.

For each victim listed, a dedicated page is created that contains samples of the stolen data.

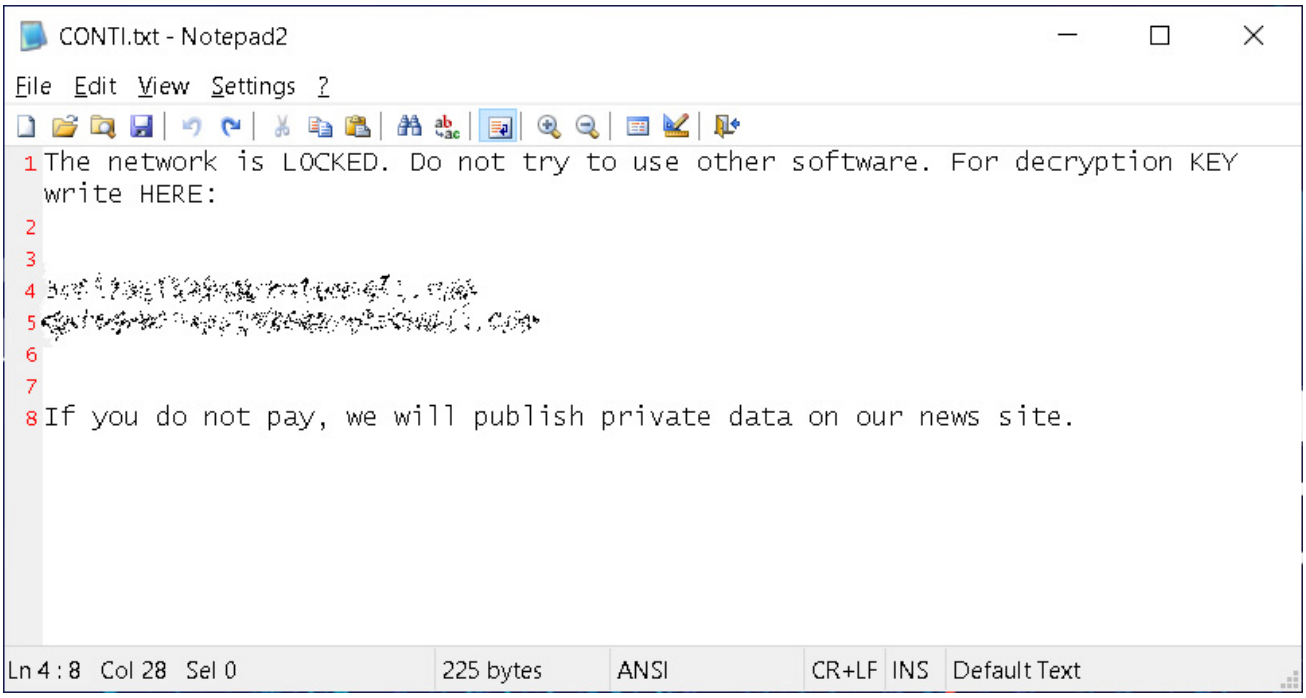


Leaked data

The ransomware's adoption stealing data to be used in extortion is also reflected in the latest ransom notes from Conti.

In the past, the ransomware operators would just include a message that the victim was encrypted, and include two email addresses to contact them.

Conti ransom notes now include specific language stating that they will publish a victim's data if a ransom is not paid, as shown below.



Conti ransom note

Other ransomware operations that steal or have stolen unencrypted files to extort their victims include Ako, Avaddon, Clop, CryLock, DoppelPaymer, Maze, MountLocker, Nemty, Nephilim, Netwalker, Pysa/Mespinoza, Ragnar Locker, REvil, Sekhmet, Snatch, and Snake.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

Industrial Spy data extortion market gets into the ransomware game

The Week in Ransomware - May 20th 2022 - Another one bites the dust

- Conti
- Data Exfiltration
- Ransomware
- Ryuk
- TrickBot

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article

- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: