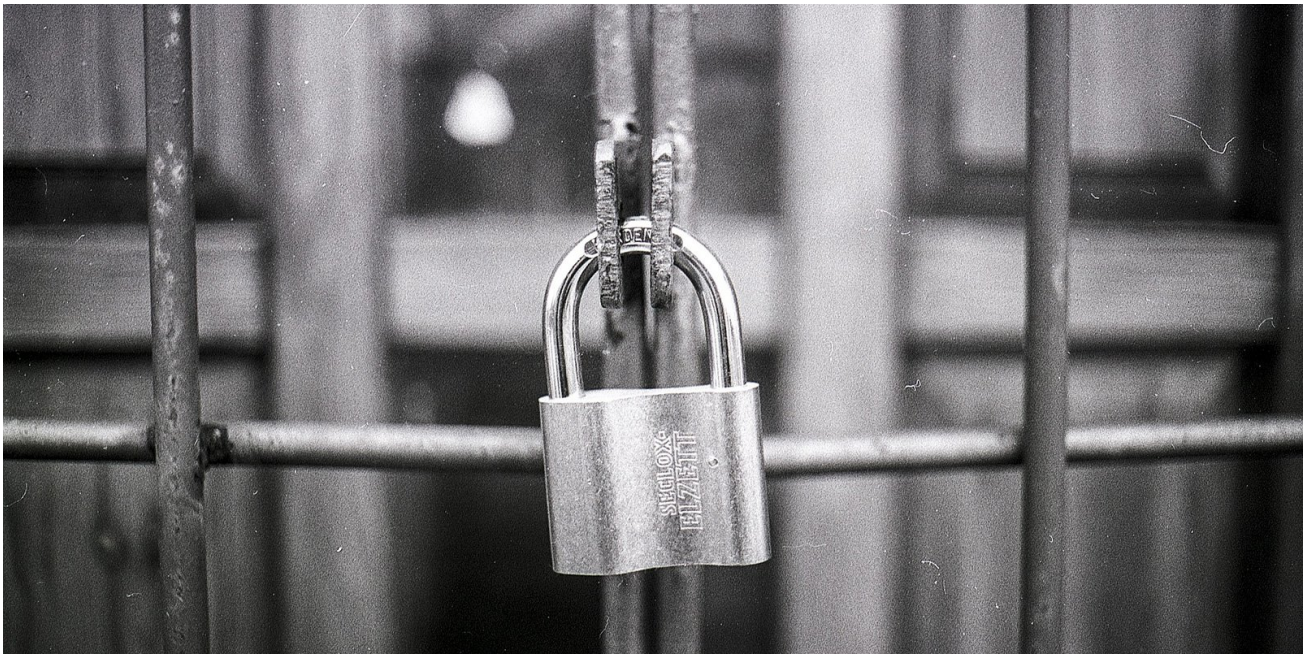
# Mount Locker ransomware joins the multi-million dollar ransom game

bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game/

Lawrence Abrams

By
Lawrence Abrams

- September 24, 2020
- 05:42 PM
- 0



A new ransomware operation named Mount Locker is underway stealing victims' files before encrypting and then demanding multi-million dollar ransoms.

Starting around the end of July 2020, Mount Locker began breaching corporate networks and deploying their ransomware.

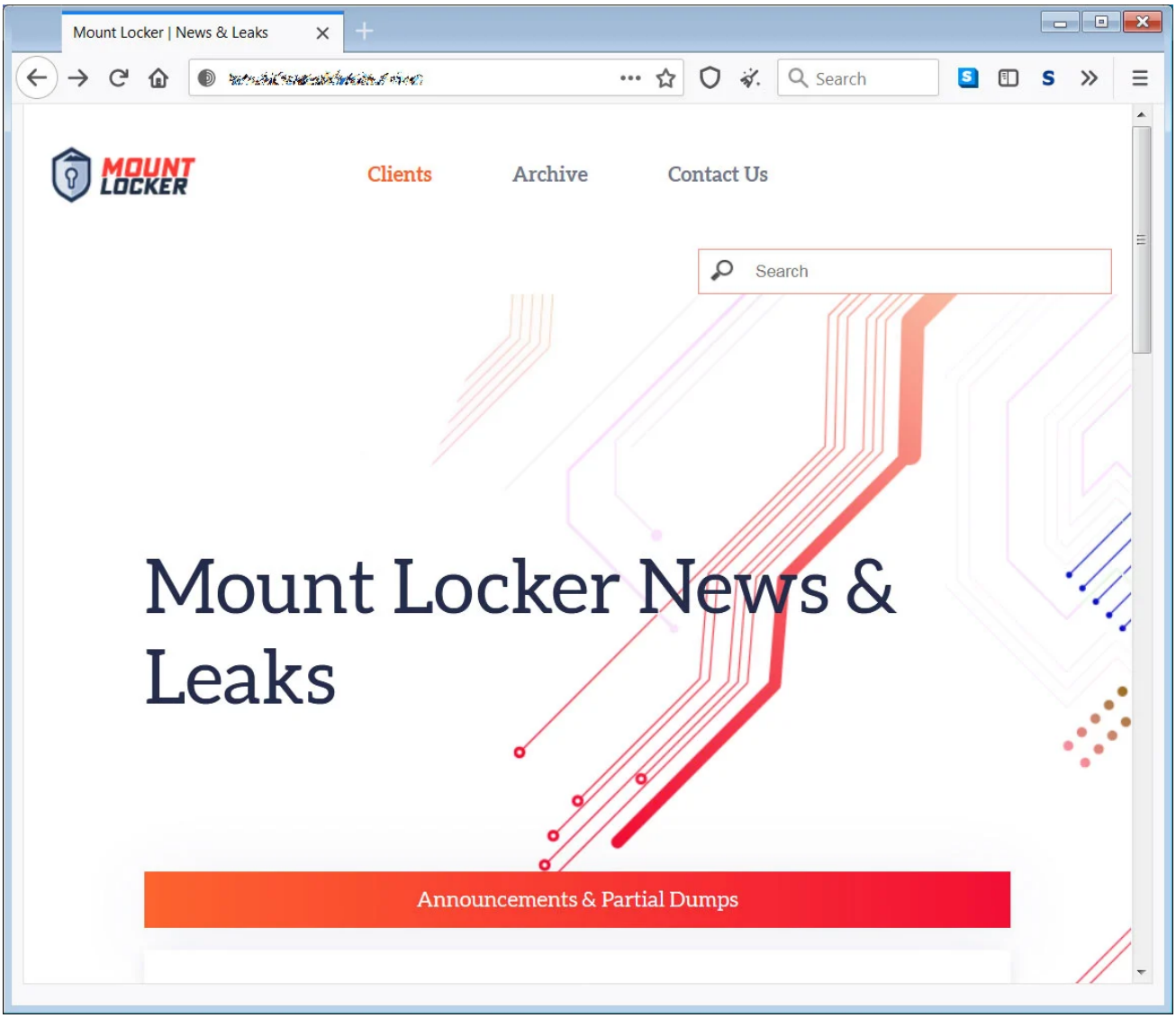
From ransom notes shared with BleepingComputer by victims, the Mount Locker gang is demanding multi-million dollar ransom payments in some cases.


**$2 million ransom demand from Mount Locker**

Before encrypting files, Mount Locker will also steal unencrypted files and threaten victims that the data will be published if a ransom is not paid.

For example, Mount Locker told one victim that they stole 400 GB of their data, and if they are not paid, they will contact the victim's competitors, the media, TV channels, and newspapers.

Ultimately, the victim did not pay, and their data was published to a ransomware data leak site.




**Mount Locker data leak site**

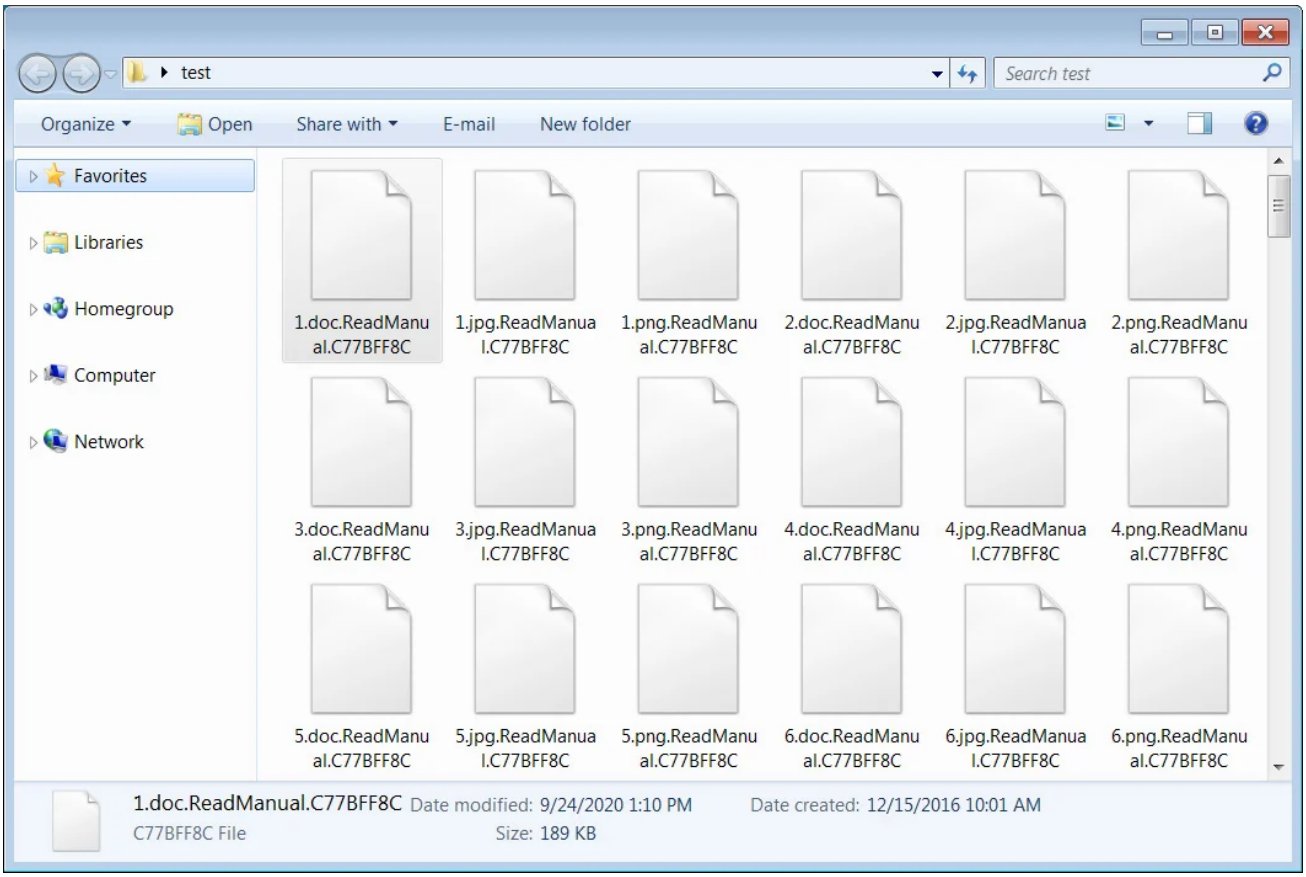
This data leak site currently lists four victims, with only one having files leaked.

## The MountLocker ransomware

It was only until recently that MalwareHunterTeam discovered a sample of Mount Locker, which allow allowed us to get a bit more insight into how the ransomware operates.

Michael Gillespie, who analyzed the ransomware, told BleepingComputer that Mount Locker uses ChaCha20 to encrypt the files and an embedded RSA-2048 public key to encrypt the encryption key.

From our analysis, when encrypting files, the ransomware will add an extension in the format **.ReadManual.ID**. For example, 1.doc would be encrypted and renamed to 1.doc.ReadManual.C77BFF8C, as shown in the encrypted folder below.

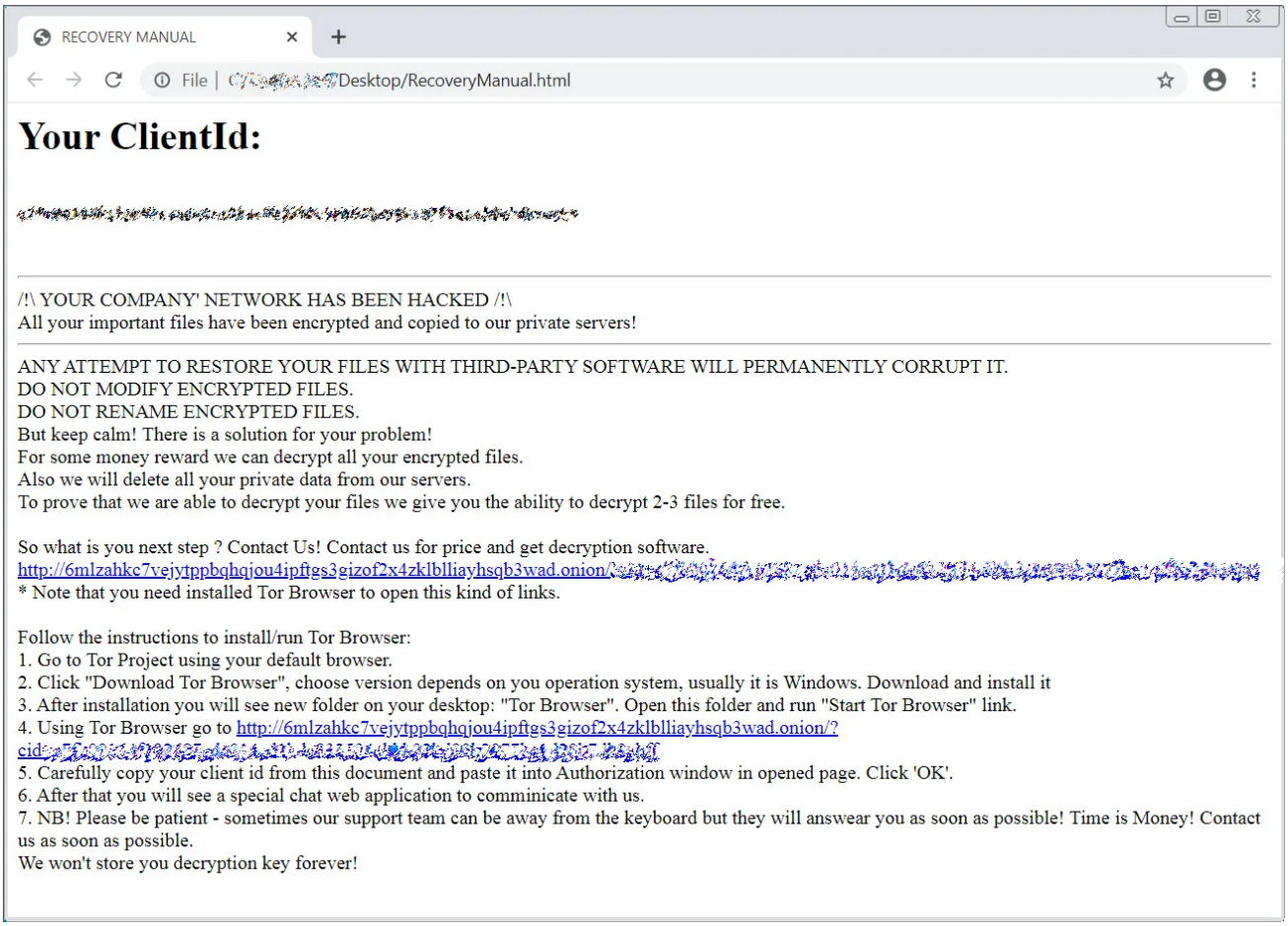



**Mount Locker encrypted files**

The ransomware will then register the extension in the Registry so that when you click on an encrypted file, it will automatically load the ransom note.

```
HKCU\Software\Classes\.C77BFF8C\shell\Open\command\ @="explorer.exe
RecoveryManual.html"
```

The ransom note is named RecoveryManual.html and contains instructions on how to access the Tor site to communicate with the ransomware operators.




**Mount Locker ransom note**

The Tor site is simply a chat service, where victims can negotiate the ransom or ask questions.

Unfortunately, the ransomware is secure, and there is no way to recover your files for free.

For those who wish to receive support related to this ransomware, you can use our dedicated Mount Locker support topic.

## Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Data Exfiltration
- Data Leak
- Mount Locker

- Ransomware

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



## You may also like: