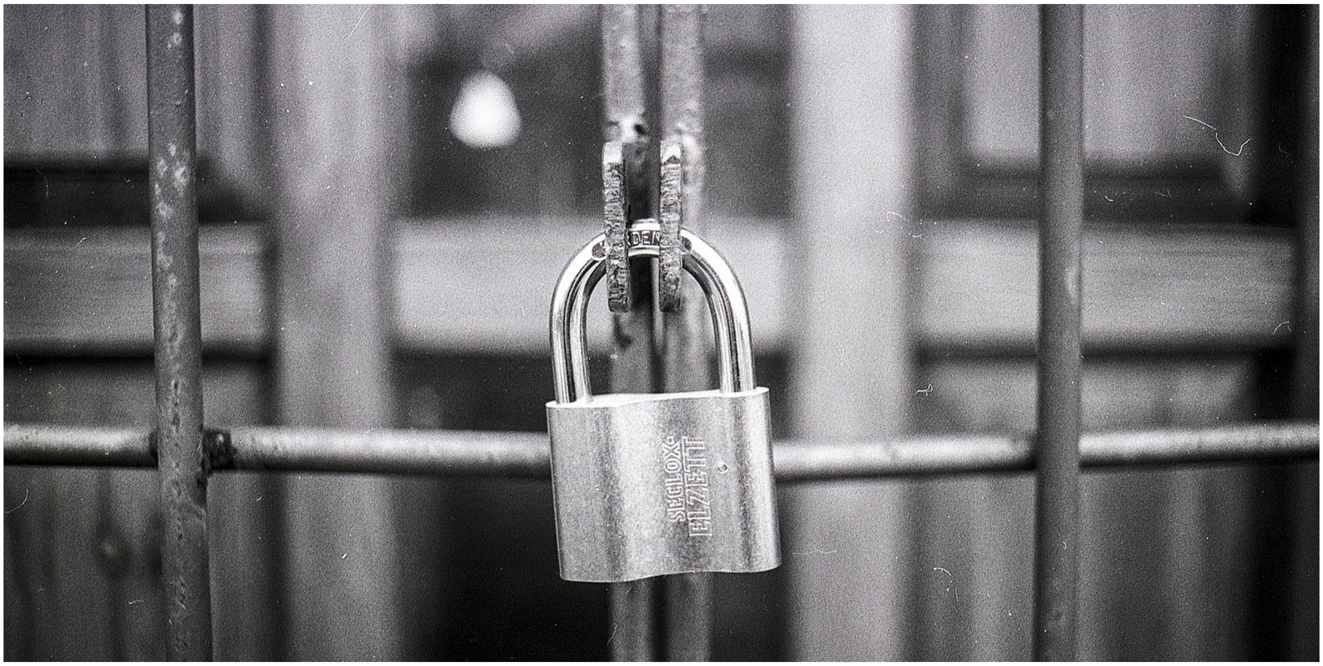
ThunderX Ransomware rebrands as Ranzy Locker, adds data leak site

Lawrence Abrams

By
Lawrence Abrams

- October 16, 2020
- 04:07 PM
- 0



ThunderX has changed its name to Ranzy Locker and launched a data leak site where they shame victims who do not pay the ransom.

ThunderX is a ransomware operation that was launched at the end of August 2020. Soon after launching, weaknesses were found in the ransomware that allowed a free decryptor to be released by Tesorion.

The ransomware operators quickly fixed their bugs and released a new version of the ransomware under Ranzy Locker name.

While the name has changed, strings associated with a PDB debug file in the ransomware executables still show it is the same as ThunderX.

```
C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb
```

BleepingComputer's theory is that they rebranded to start with a clean slate and avoid the stigma of being associated with the previously released decryptor.

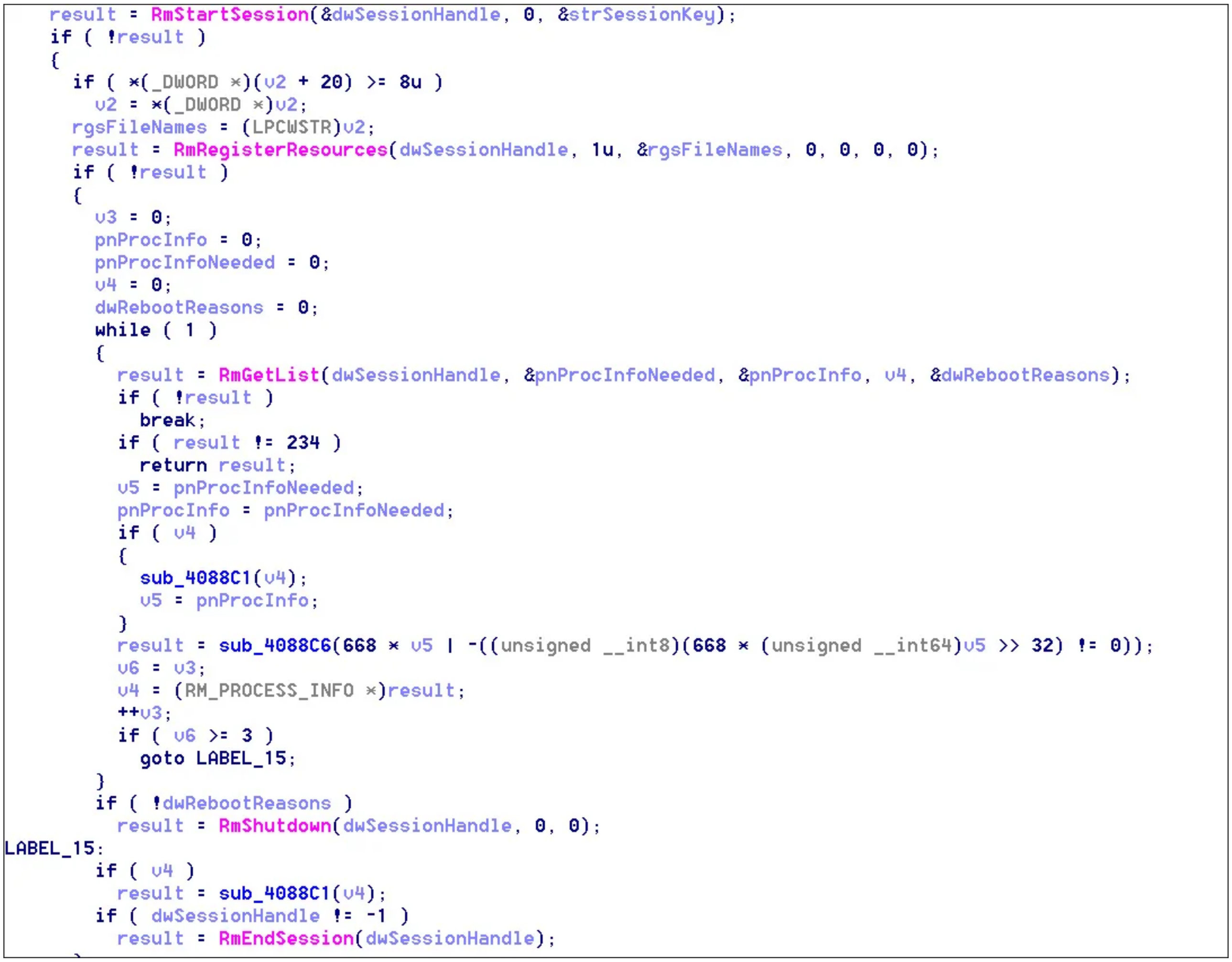
Meet the Ranzy Locker ransomware

Using a sample of the ransomware found by MalwareHunterteam and shared with BleepingComputer, we can get a deeper dive into how the ransomware operates.

When launched, Ranzy Locker will first clear Shadow Volume Copies so that victims can't use it to recover encrypted files.

```
vssadmin.exe Delete Shadows /All /Quiet;
```

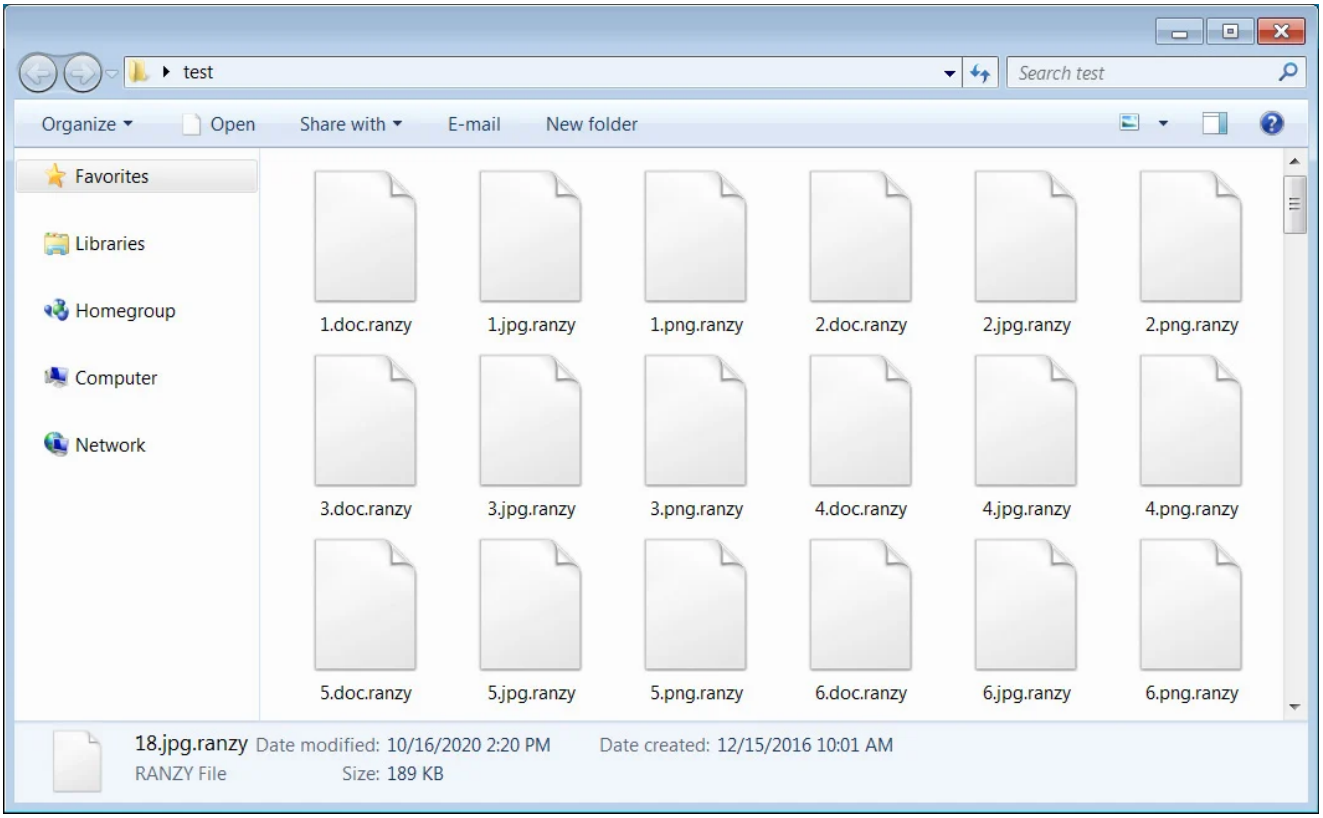
When encrypting files, the ransomware will use a Windows API called the 'Windows Restart Manager' that will terminate processes or Windows services that keep a file open and prevent it from being encrypted.



```
  result = RmStartSession(&dwSessionHandle, 0, &strSessionKey);
  if ( !result )
  {
    if ( *(_DWORD *)(v2 + 20) >= 8u )
      v2 = *(_DWORD *)v2;
    rgsFileNames = (LPCWSTR)v2;
    result = RmRegisterResources(dwSessionHandle, 1u, &rgsFileNames, 0, 0, 0, 0);
    if ( !result )
    {
      v3 = 0;
      pnProcInfo = 0;
      pnProcInfoNeeded = 0;
      v4 = 0;
      dwRebootReasons = 0;
      while ( 1 )
      {
        result = RmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, v4, &dwRebootReasons);
        if ( !result )
          break;
        if ( result != 234 )
          return result;
        v5 = pnProcInfoNeeded;
        pnProcInfo = pnProcInfoNeeded;
        if ( v4 )
        {
          sub_4088C1(v4);
          v5 = pnProcInfo;
        }
        result = sub_4088C6(668 * v5 | -((unsigned __int8)(668 * (unsigned __int64)v5 >> 32) != 0));
        v6 = v3;
        v4 = (RM_PROCESS_INFO *)result;
        ++v3;
        if ( v6 >= 3 )
          goto LABEL_15;
      }
      if ( !dwRebootReasons )
        result = RmShutdown(dwSessionHandle, 0, 0);
LABEL_15:
      if ( v4 )
        result = sub_4088C1(v4);
      if ( dwSessionHandle != -1 )
        result = RmEndSession(dwSessionHandle);
```

Windows Restart Manager

For each encrypted file, the ransomware appends the new **.ranzy** extension to the file's name. For example, a file named 1.doc would be encrypted and renamed to 1.doc.ranzy.

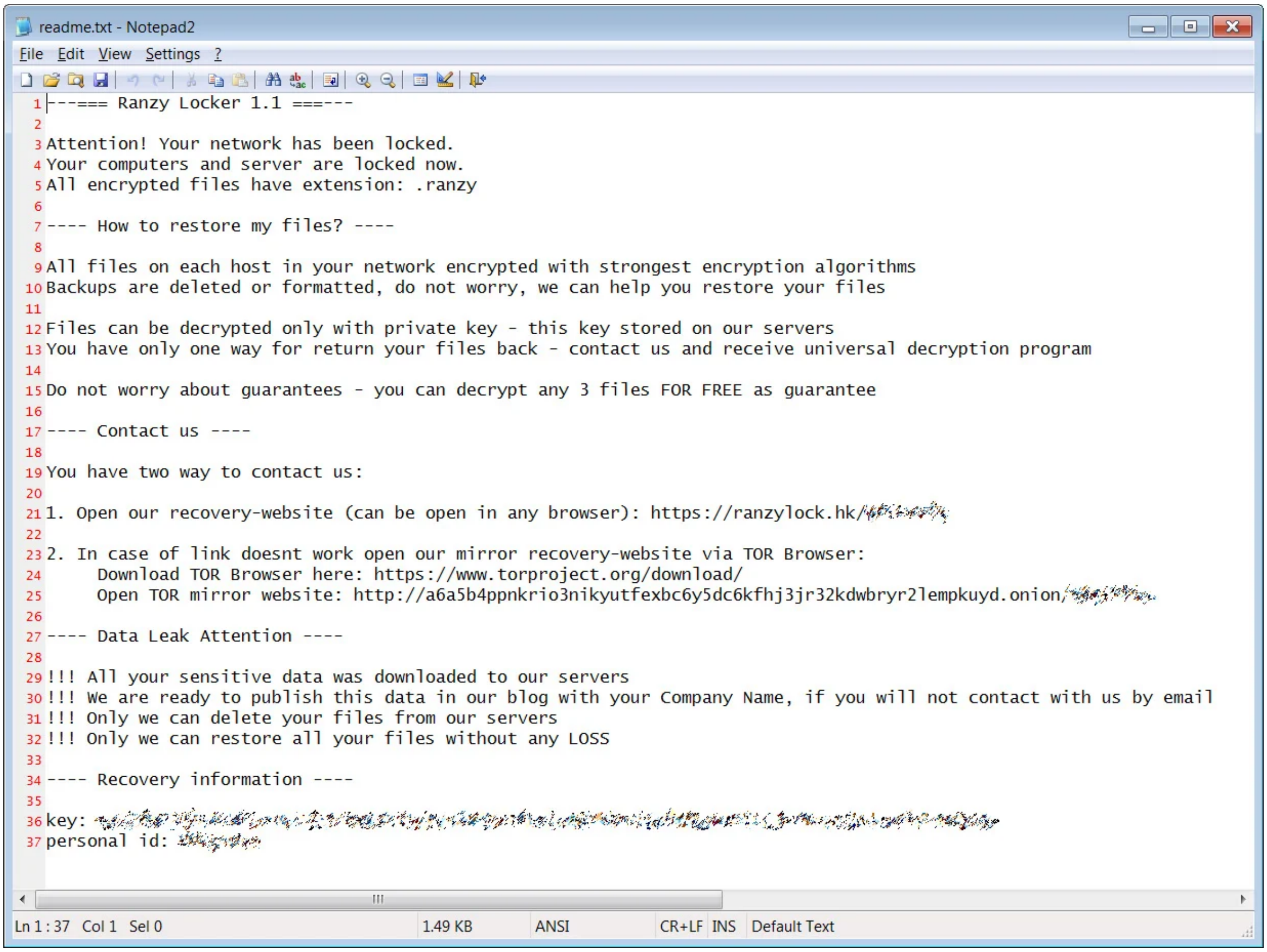


18.jpg.ranzy Date modified: 10/16/2020 2:20 PM Date created: 12/15/2016 10:01 AM
RANZY File Size: 189 KB

Ranzy Locker encrypted files

In each traversed folder, the ransomware will create a ransom note named '**readme.txt**' that includes information about what happened to a victim's data, a warning that their data was stolen, and a link to a Tor site where the victim can negotiate with the threat actors.

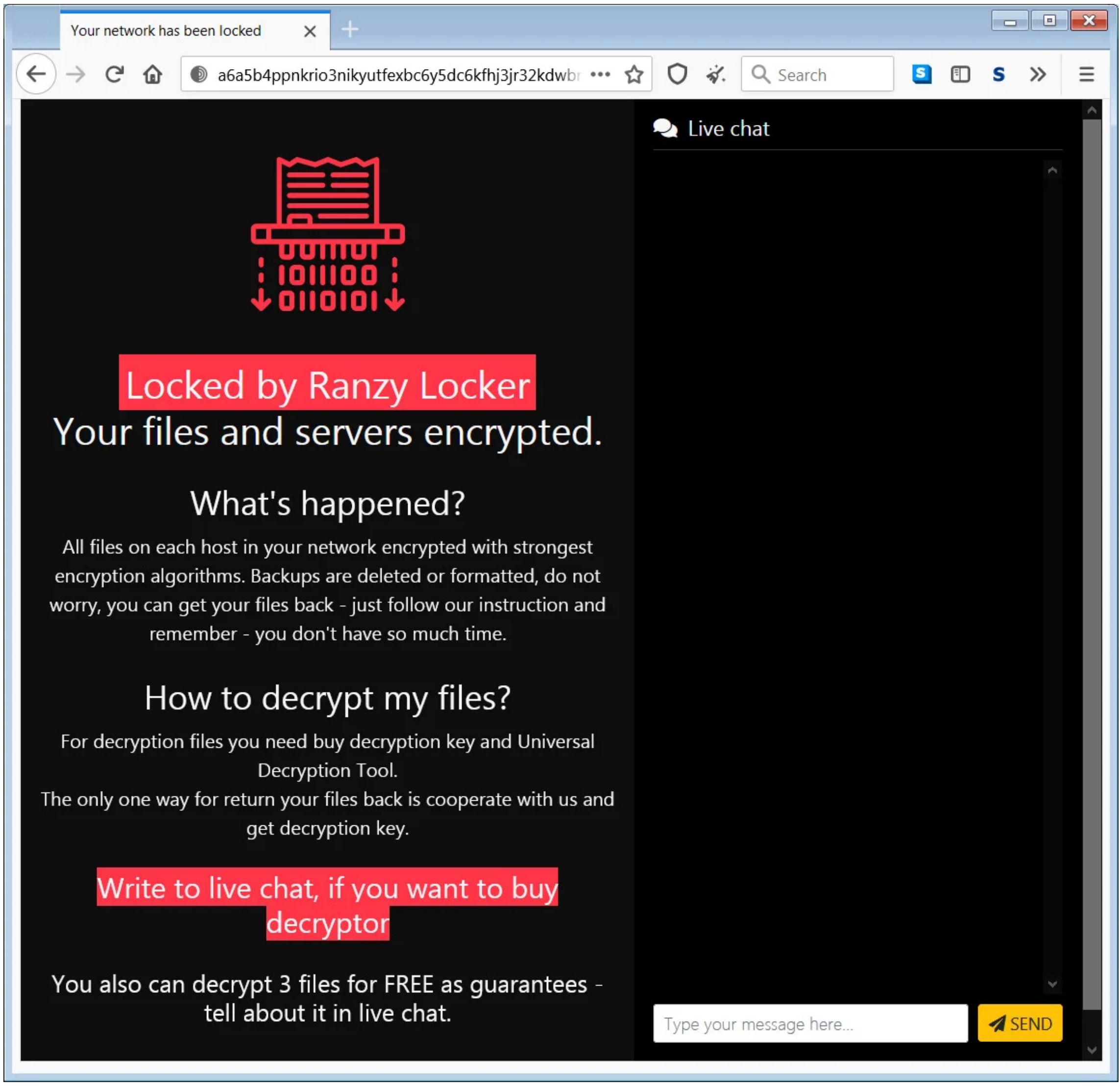
It should be noted that in previous versions of ThunderX, the ransomware operators communicated with victims via email rather than using a dedicated Tor site.



```
-----=== Ranzy Locker 1.1 ===---

Attention! Your network has been locked.
Your computers and server are locked now.
All encrypted files have extension: .ranzy

---- How to restore my files? ----

All files on each host in your network encrypted with strongest encryption algorithms
Backups are deleted or formatted, do not worry, we can help you restore your files

Files can be decrypted only with private key - this key stored on our servers
You have only one way for return your files back - contact us and receive universal decryption program

Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee

---- Contact us ----

You have two way to contact us:

1. Open our recovery-website (can be open in any browser): https://ranzylock.hk/[redacted]

2. In case of link doesnt work open our mirror recovery-website via TOR Browser:
     Download TOR Browser here: https://www.torproject.org/download/
     Open TOR mirror website: http://a6a5b4ppnkrio3nikyutfexbc6y5dc6kfhj3jr32kdwbryr2lempkuyd.onion/[redacted]

---- Data Leak Attention ----

!!! All your sensitive data was downloaded to our servers
!!! We are ready to publish this data in our blog with your Company Name, if you will not contact with us by email
!!! Only we can delete your files from our servers
!!! Only we can restore all your files without any LOSS

---- Recovery information ----

key: [redacted]
personal id: [redacted]
```

Ranzy Locker ransom note

When a victim visits the Tor payment site, they will be greeted with a 'Locked by Ranzy Locker' message and be shown a live chat screen to negotiate with the threat actors. As part of this 'service,' the ransomware operators allow victims to decrypt three files for free to prove that they can do so.



Your network has been locked
a6a5b4ppnkrio3nikyutfexbc6y5dc6kfhj3jr32kdwb
Search
Live chat
Type your message here...
SEND

Locked by Ranzy Locker
Your files and servers encrypted.

What's happened?

All files on each host in your network encrypted with strongest encryption algorithms. Backups are deleted or formatted, do not worry, you can get your files back - just follow our instruction and remember - you don't have so much time.

How to decrypt my files?

For decryption files you need buy decryption key and Universal Decryption Tool.
The only one way for return your files back is cooperate with us and get decryption key.

Write to live chat, if you want to buy decryptor

You also can decrypt 3 files for FREE as guarantees - tell about it in live chat.

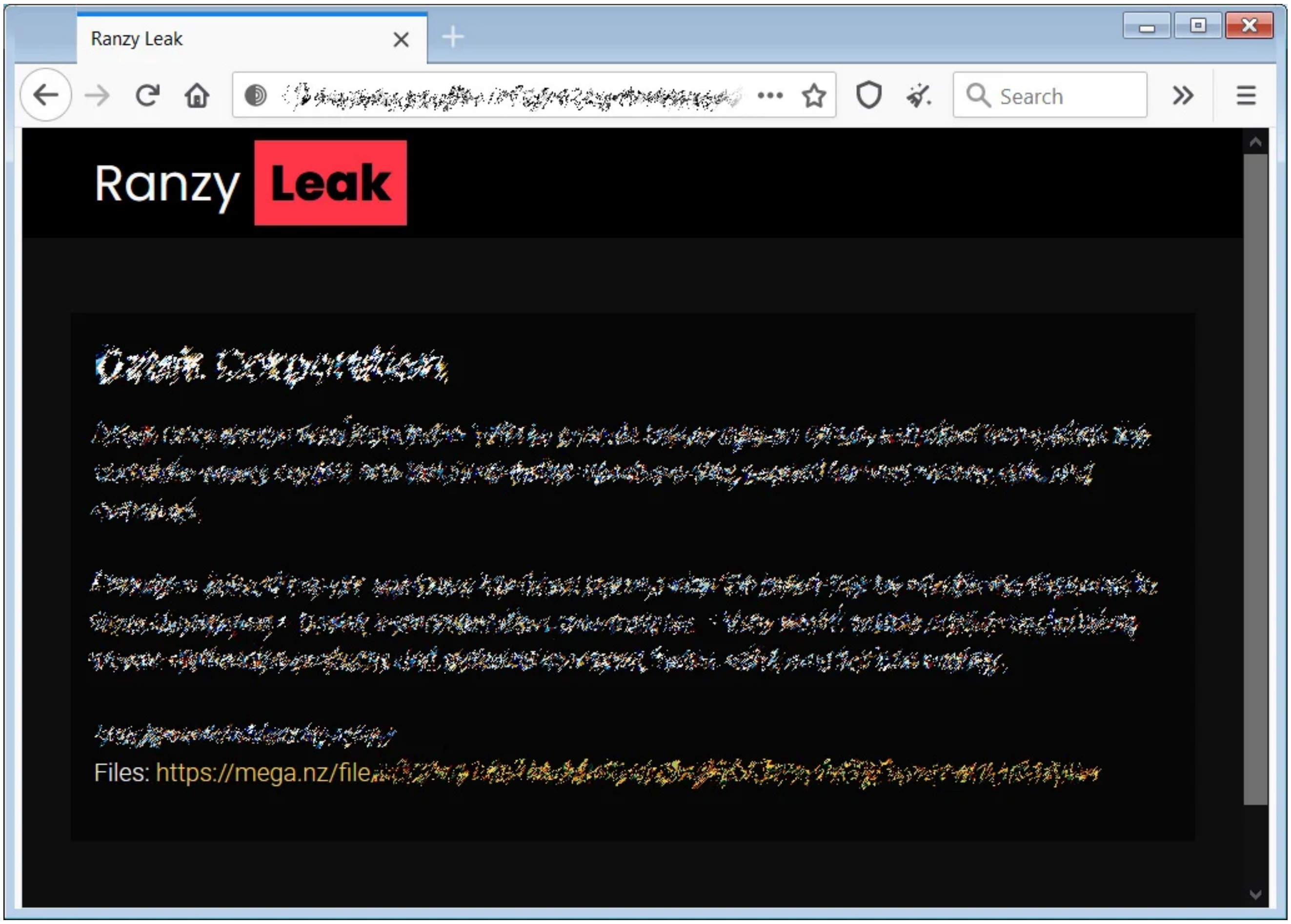
Ranzy Locker Tor payment site

Ranzy Locker launches a data leak site

Many ransomware gangs utilize a double-extortion attack method, which is to steal unencrypted files from a victim before they encrypt the devices on the corporate network.

This attack method provides the threat actors two ways to leverage the victim into paying a ransomware -- pay to get their files back and not have their data publicly leaked.

This week, the Ranzy Locker gang released a data leak site called 'Ranzy Leak' to leak the data of victims who do not pay.



Ranzy Leak

[redacted]

[redacted]

Files: https://mega.nz/file[redacted]

This web site currently includes one victim who develops power control solutions.

An item of interest is that the Tor onion URL used by the Ranzy Leak site is the same as the one previously used by Ako Ransomware.

The use of Ako's URL could indicate that both groups merged to form Ranzy Locker, or they are cooperating similarly as the Maze cartel.

Update 10/16/20: The Ako ransomware operators contacted us and stated ThunderX is part of their operation and that they have rebranded to Ranzy Locker.

"Because we update our original ransomware and its little rebranding.

ThunderX is test version our update, but some US kids share this build on virustotal — oops."

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

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.