New Ransom X Ransomware used in Texas TxDOT cyberattack

bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/

Lawrence Abrams

By
Lawrence Abrams

- June 26, 2020
- 10:17 AM
- 4

A new ransomware called Ransom X is being actively used in human-operated and targeted attacks against government agencies and enterprises.

May 2020 was not a good month for Texas as both the Texas Courts and the Texas Department of Transportation (TxDOT) were hit with ransomware attacks.

At the time of the attacks, it was not known what ransomware targeted the government agencies.

We still do not know for the Texas Courts, but due to a ransomware sample found by MalwareHunterTeam, we now know that TxDot suffered an attack by new targeted ransomware called Ransom X.

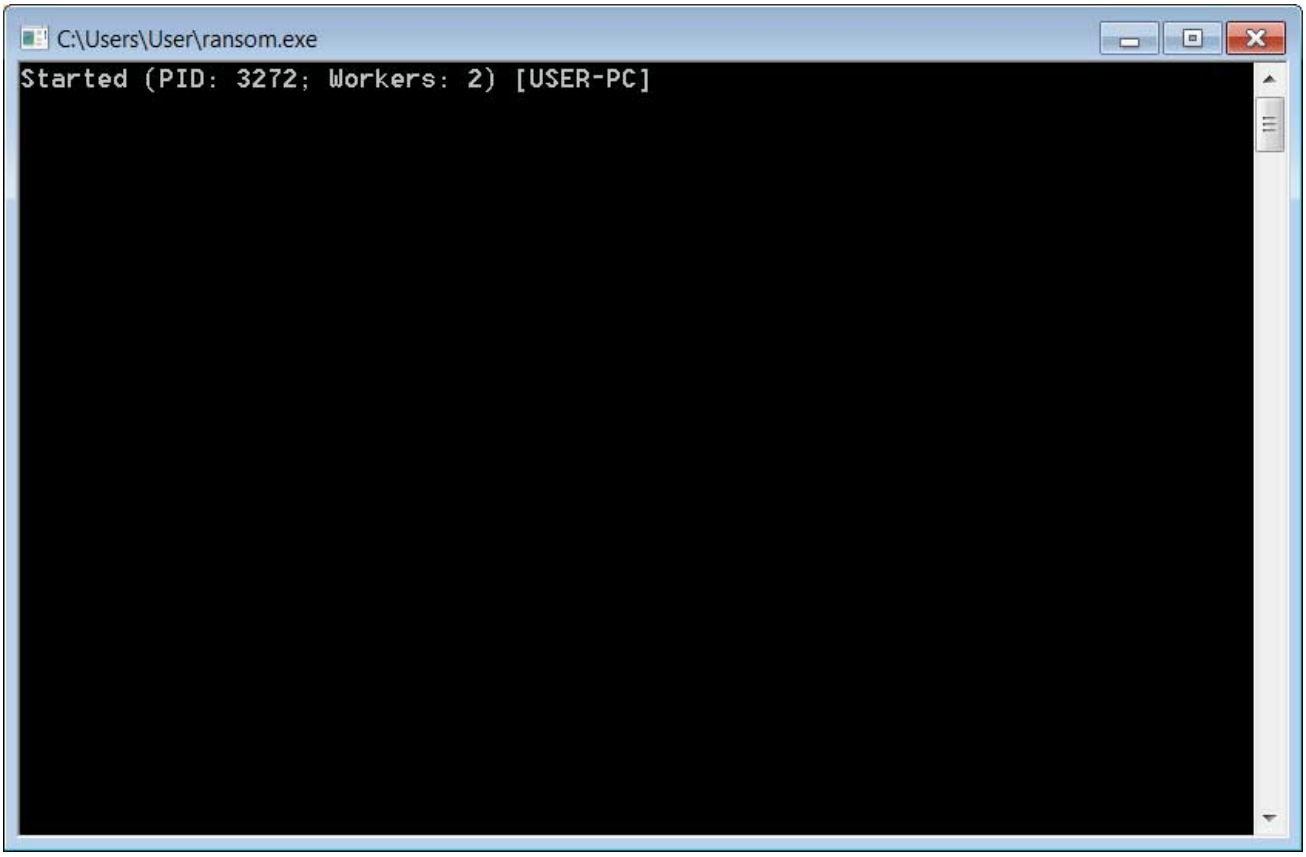
Taking a look at Ransom X

After MalwareHunterTeam shared a sample of Ransom X with Advanced Intel's Vitali Kremez and BleepingComputer, we took it for a spin to see what we could find.

Naming ransomware infections is not always easy, as many times, there is no indication as to what the developers call it.

In this case, Advanced Intel's Vitali Kremez found a 'ransom.exx' string in the executable, which we believe is the name of the ransomware.

As this is human-operated ransomware, rather than one distributed via phishing or malware, when executed the ransomware will open a console that displays information to the attacker while it is running.



Ransom X console
Source: BleepingComputer
According to Kremez, Ransom.exx will terminate 289 processes related to security software, database servers, MSP software, remote access tools, and mail servers.

The ransomware will also bypass various Windows system folders and any files that match the follow extensions:

```
.ani, .cab, .cpl, .cur, .diagcab, .diagpkg, .dll, .drv, .hlp, .icl, .icns, .ico,
.iso, .ics, .lnk, .idx, .mod, .mpa, .msc, .msp, .msstyles, .msu, .nomedia, .ocx,
.prf, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .exe, .bat, .cmd, .url, .mui
```

Of particular interest are three bypassed folders that Kremez and I theorize are being used to store the ransomware executable and other utilities used during an attack.

```
crypt_detect
cryptolocker
ransomware
```

By bypassing these folders, it allows the attackers to encrypt a computer while also attack other computers on the network without fear their tools will become encrypted.

The list of terminated processes and bypassed extensions and folders can be found on our GitHub page.

Ransom X will also perform a series of commands throughout the encryption process that:

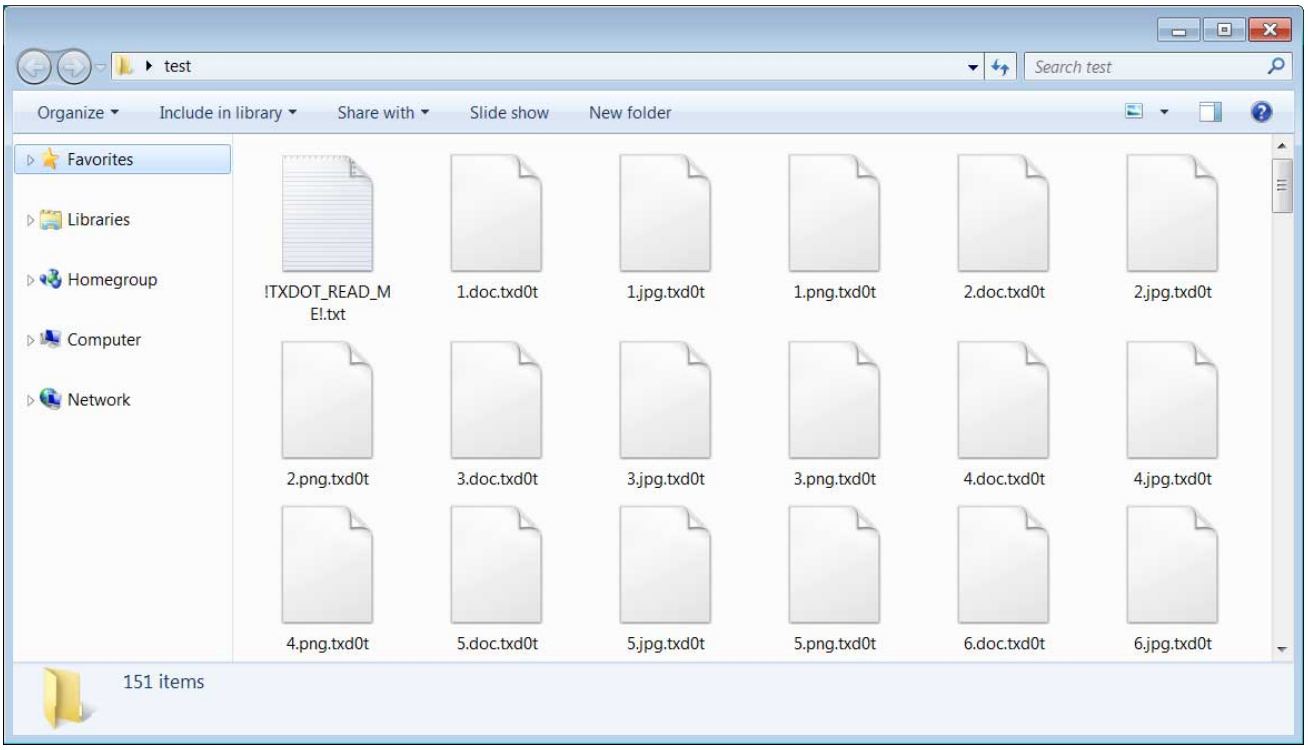
- Clear Windows event logs
- Delete NTFS journals
- Disable System Restore
- Disable the Windows Recovery Environment
- Delete Windows backup catalogs
- Wipe free space from local drives.

The commands executed are listed below.

```
cipher /w %s
wbadmin.exe delete catalog -quiet
bcdedit.exe /set {default} recoveryenabled no
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable
wevtutil.exe cl Application
wevtutil.exe cl System
wevtutil.exe cl Setup
wevtutil.exe cl Security
wevtutil.exe sl Security /e:false
fsutil.exe usn deletejournal /D C:
```

The ransomware will now begin to encrypt all of the data on the computer and append a custom extension associated with the victim to each encrypted file.

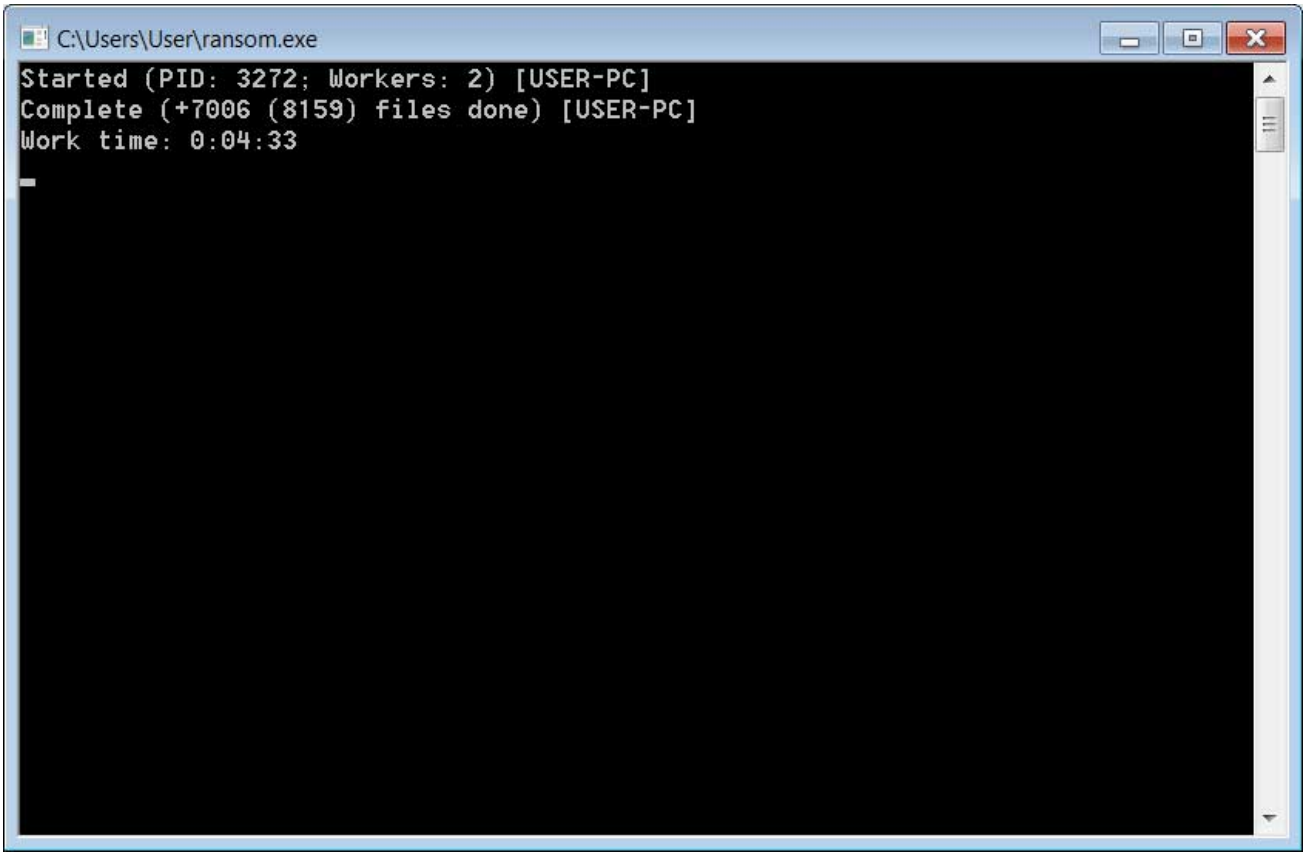
As you can see below, the custom extension for the Texas Department of Transportation attack was **.txd0t.**



Ransom X encrypted files

Source: BleepingComputer

When completed, the Ransom X console will display the number of encrypted files and how long it took to complete it.



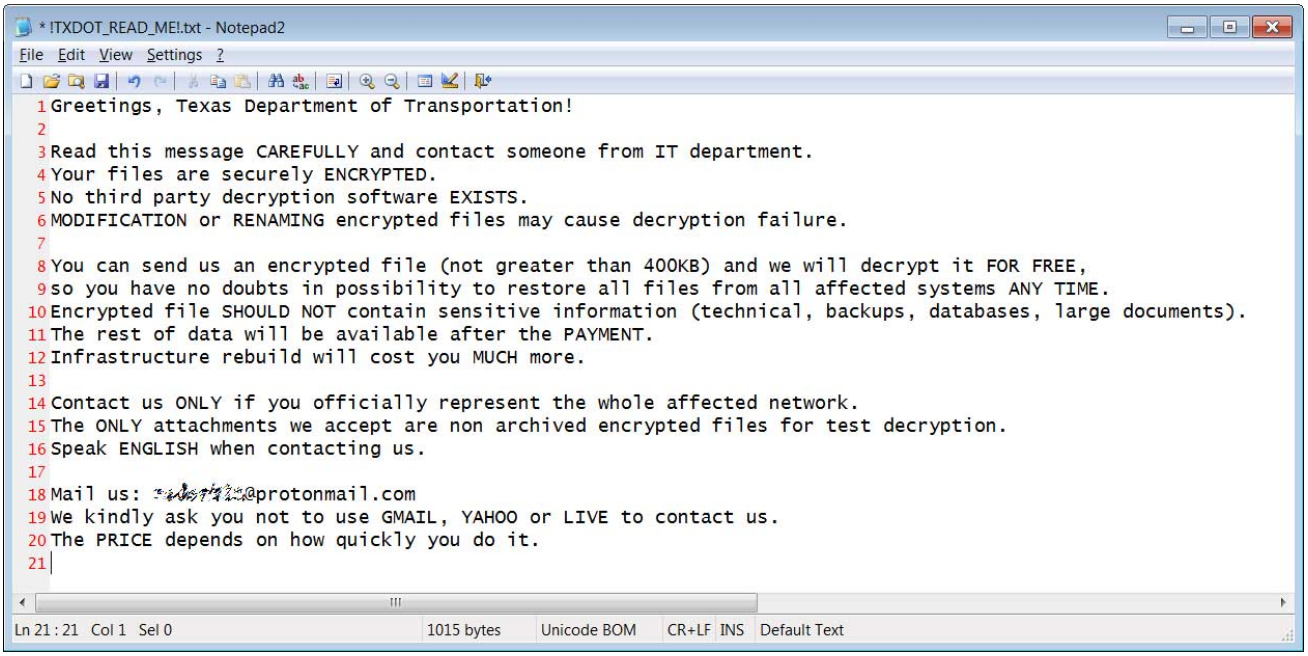
Encryption has finished

Source: BleepingComputer

In each folder that was scanned during the encryption process, a ransom note named ![extension]_READ_ME!.txt will be created.

This ransom note includes the company name, an email address to contact, and instructions on how to pay the ransom.

As you can see below, the ransom note is customized for the specific victim that is under attack, which in this case is the Texas Department of Transportation.



Ransom X ransom note
Source: BleepingComputer
Due to the limited visibility into this ransomware operation, there is no information regarding the ransom amounts or whether they steal data as part of the attacks.

This ransomware has been analyzed and appears secure, which means there is no way to decrypt the files for free.

Related Articles:

Luxury fashion house Zegna confirms August ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

IOCs

Ransom Note text:

```
Greetings, Texas Department of Transportation!

Read this message CAREFULLY and contact someone from IT department.
Your files are securely ENCRYPTED.
No third party decryption software EXISTS.
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it
FOR FREE,
so you have no doubts in possibility to restore all files from all affected systems
ANY TIME.
Encrypted file SHOULD NOT contain sensitive information (technical, backups,
databases, large documents).
The rest of data will be available after the PAYMENT.
Infrastructure rebuild will cost you MUCH more.

Contact us ONLY if you officially represent the whole affected network.
The ONLY attachments we accept are non archived encrypted files for test decryption.
Speak ENGLISH when contacting us.

Mail us: xxx@protonmail.com
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.
The PRICE depends on how quickly you do it.
```

- Ransom X
- RansomEXX
- Ransomware
- Texas

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

Comments

- 
  R-K - 1 year ago
  -
  -
  Cyber-terrorists
- 
  Amigo-A - 1 year ago
  -
  -
  This is RansomEXX Ransomware
  https://twitter.com/VK_Intel/status/1275133575927562241

- 

  Lawrence Abrams - 1 year ago

  -
  -

  Didn't I already state that?

  "In this case, Advanced Intel's Vitali Kremez found a 'ransom.exx' string in the executable, which we believe is the name of the ransomware."

- 

  Amigo-A - 1 year ago

  -
  -

  Above written several times as "Ransom X" :)
  To avoid confusion later.

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: