Erebus Ransomware Utilizes a UAC Bypass and Request a $90 Ransom Payment

bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment

By
Lawrence Abrams

- February 7, 2017
- 03:08 PM
- 2

A sample of a potentially new ransomware called Erebus has been discovered by MalwareHunterTeam on VirusTotal. I say that this is a potentially new ransomware because TrendMicro had reported another ransomware using the same name was previously released back in September 2016. Though I do not have a sample of the original Erebus, from its outward characteristics, the one discovered today looks like either a complete rewrite or a new ransomware using the same name..

While at this time, it is not currently known how Erebus is being distributed, analysis of the ransomware shows some interesting features. The first, and most noticeable features, is the low ransom amount of ~$90 USD being requested by the ransomware. Another interesting features is its use of a UAC bypass that allows the ransomware to run at elevated privileges without displaying a UAC prompt.

Erebus performs a UAC Bypass by Hijacking the MSC File Association

When the installer for Erebus is executed, it will also utilize a User Account Control (UAC) bypass method so that victim's will not be prompted to allow the program to run at higher privileges. It does this by copying itself to a random named file in the same folder. It will then modify the Windows registry in order to hijack the association for the **.msc** file extension so that it will launch the random named Erebus executed instead.

The hijacked keys are shown below.

```
HKEY_CLASSES_ROOT\.msc
HKCU\Software\Classes\mscfile
HKCU\Software\Classes\mscfile\shell
HKCU\Software\Classes\mscfile\shell\open
HKCU\Software\Classes\mscfile\shell\open\command
HKCU\Software\Classes\mscfile\shell\open\command\       %UserProfile%\[random].exe
```

Erebus will then execute eventvwr.exe (Event Viewer), which in turn will automatically open the eventvwr.msc file. As the .msc file is no longer associated with mmc.exe, but now with the random named Erebus executable, Event Viewer will launch Erebus instead. As Event Viewer runs in a elevated mode, the launched Erebus executable will also launch with the same privileges. This allows it to bypass User Account Control.

A big thanks to MalwareHunterTeam for pointing out the article that describes this bypass.

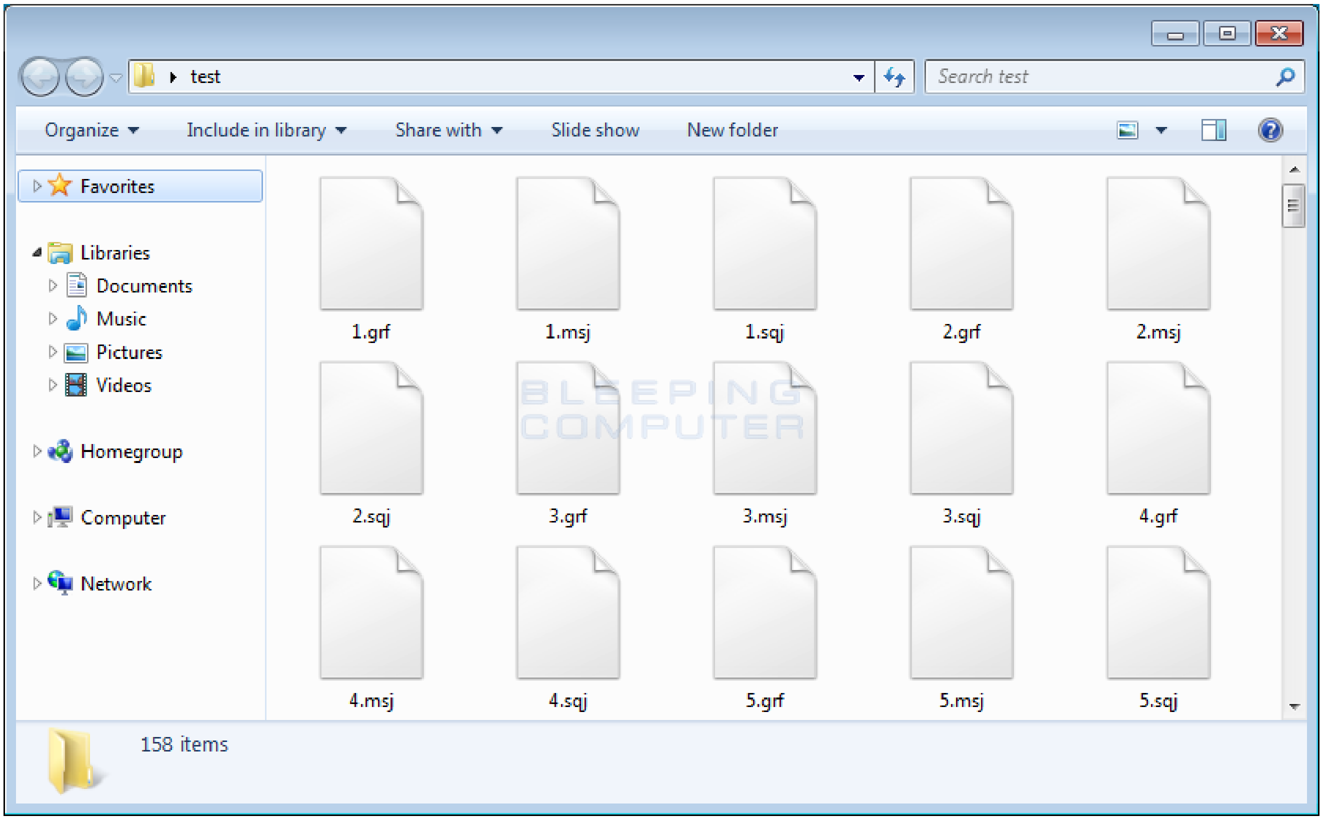
How Erebus Encrypts a Computer

When Erebus is executed it will connect to http://ipecho.net/plain and http://ipinfo.io/country in order to determine the victim's IP address and country that they are located in. It will then download a TOR client and use it to connect to the site's Command & Control server.

Erebus will then begin to scan the victim's computer and search for certain file types. When it detects a targeted file type, it will encrypt the file using AES encryption. The current list of targeted files are:

```
.accdb, .arw, .bay, .cdr, .cer, .crt, .crw, .dbf, .dcr, .der, .dng, .doc, .docm,
.docx, .dwg, .dxf, .dxg, .eps, .erf, .indd, .jpe, .jpg, .kdc, .mdb, .mdf, .mef, .mrw,
.nef, .nrw, .odb, .odm, .odp, .ods, .odt, .orf, .pdd, .pef, .pem, .pfx, .png, .ppt,
.pptm, .pptx, .psd, .pst, .ptx, .raf, .raw, .rtf, .rwl, .srf, .srw, .txt, .wpd, .wps,
.xlk, .xls, .xlsb, .xlsm, .xlsx
```

When Erebus encrypts a file, it will encrypt the extension using ROT-23. For example, a file called **test.jpg** would be encrypted and renamed as **test.msj**.

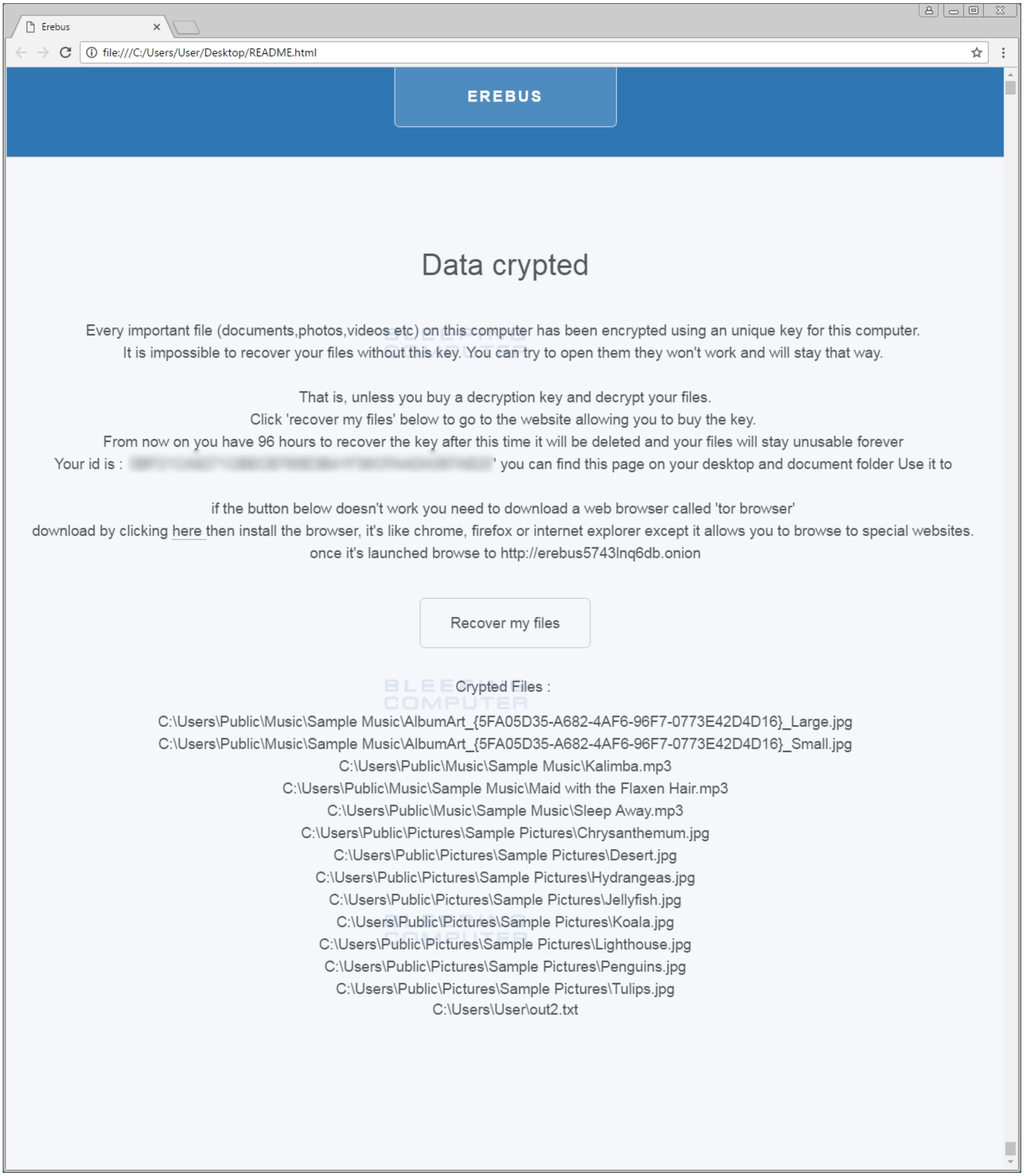


Encrypted Files

During this process, Erebus will also clear the Windows Volume Shadow Copies so that they cannot be used to recover files. The command executed to clear the shadow copies is:

```
cmd.exe /C vssadmin delete shadows /all /quiet && exit
```

When it has finished encrypting the computer, it will display the ransom note located on the Desktop called **README.HTML**. This ransom note will contain a unique ID that can be used to login to the payment site, a list of encrypted files, and a button that takes you to the TOR payment site.



EREBUS

Data crypted

Every important file (documents,photos,videos etc) on this computer has been encrypted using an unique key for this computer.
It is impossible to recover your files without this key. You can try to open them they won't work and will stay that way.

That is, unless you buy a decryption key and decrypt your files.
Click 'recover my files' below to go to the website allowing you to buy the key.
From now on you have 96 hours to recover the key after this time it will be deleted and your files will stay unusable forever
Your id is : [redacted]' you can find this page on your desktop and document folder Use it to

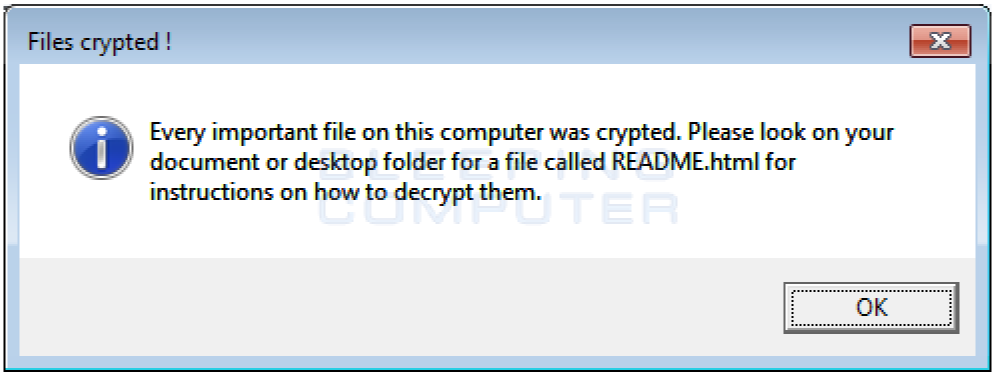
if the button below doesn't work you need to download a web browser called 'tor browser'
download by clicking here then install the browser, it's like chrome, firefox or internet explorer except it allows you to browse to special websites.
once it's launched browse to http://erebus5743lnq6db.onion

Recover my files

Crypted Files :
C:\Users\Public\Music\Sample Music\AlbumArt_{5FA05D35-A682-4AF6-96F7-0773E42D4D16}_Large.jpg
C:\Users\Public\Music\Sample Music\AlbumArt_{5FA05D35-A682-4AF6-96F7-0773E42D4D16}_Small.jpg
C:\Users\Public\Music\Sample Music\Kalimba.mp3
C:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3
C:\Users\Public\Music\Sample Music\Sleep Away.mp3
C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
C:\Users\Public\Pictures\Sample Pictures\Desert.jpg
C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
C:\Users\Public\Pictures\Sample Pictures\Koala.jpg
C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg
C:\Users\User\out2.txt

Erebus Ransomware Ransom Note

Erebus will also display a message box on the Windows desktop alerting the victim that their files are encrypted.

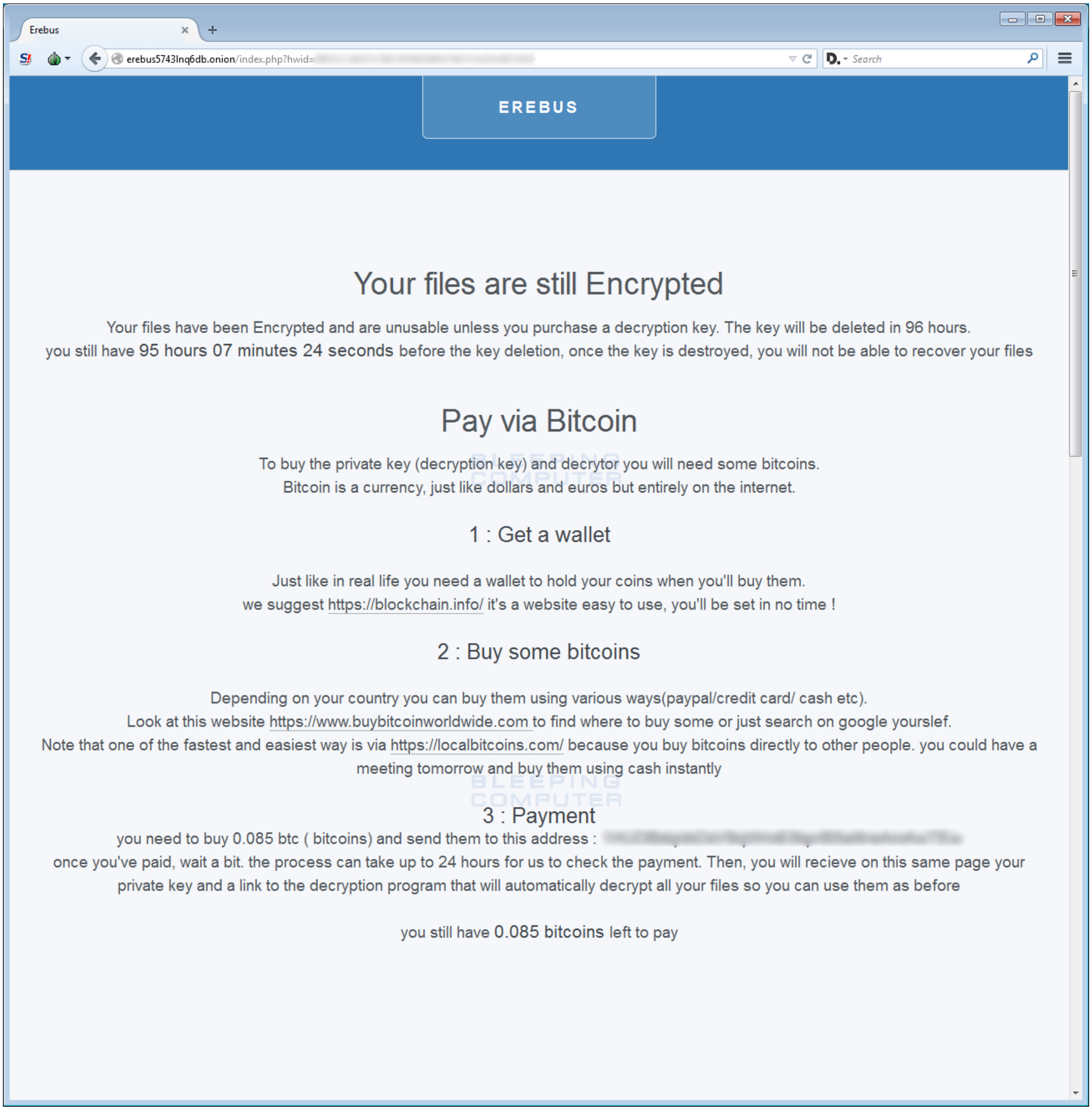


Files crypted !

Every important file on this computer was crypted. Please look on your document or desktop folder for a file called README.html for instructions on how to decrypt them.

Message Box Alert

When a victim clicks on the Recover my files button, they will be brought to Erebus' TOR payment site where they can get payment instructions. At this time the ransom amount is set to .085 bitcoins, which is approximately $90 USD.



Your files are still Encrypted

Your files have been Encrypted and are unusable unless you purchase a decryption key. The key will be deleted in 96 hours.
you still have 95 hours 07 minutes 24 seconds before the key deletion, once the key is destroyed, you will not be able to recover your files

Pay via Bitcoin

To buy the private key (decryption key) and decrytor you will need some bitcoins.
Bitcoin is a currency, just like dollars and euros but entirely on the internet.

1 : Get a wallet

Just like in real life you need a wallet to hold your coins when you'll buy them.
we suggest https://blockchain.info/ it's a website easy to use, you'll be set in no time !

2 : Buy some bitcoins

Depending on your country you can buy them using various ways(paypal/credit card/ cash etc).
Look at this website https://www.buybitcoinworldwide.com to find where to buy some or just search on google yourslef.
Note that one of the fastest and easiest way is via https://localbitcoins.com/ because you buy bitcoins directly to other people. you could have a meeting tomorrow and buy them using cash instantly

3 : Payment

you need to buy 0.085 btc (bitcoins) and send them to this address : [redacted]
once you've paid, wait a bit. the process can take up to 24 hours for us to check the payment. Then, you will recieve on this same page your private key and a link to the decryption program that will automatically decrypt all your files so you can use them as before

you still have 0.085 bitcoins left to pay

Eerebus Ransomware Payment Site

Unfortunately, at this time there is no way to decrypt files encrypted by Erebus for free. For those who wish to discuss this ransomware or receive support, you can use our dedicated help topic: Erebus Ransomware Support & Help Topic.

Associated Erebus Ransomware Files:

```
%UserProfile%\AppData\Local\Temp\tor\
%UserProfile%\AppData\Local\Temp\tor\Data\
%UserProfile%\AppData\Local\Temp\tor\Data\Tor\
%UserProfile%\AppData\Local\Temp\tor\Data\Tor\geoip
%UserProfile%\AppData\Local\Temp\tor\Data\Tor\geoip6
%UserProfile%\AppData\Local\Temp\tor\Tor\
%UserProfile%\AppData\Local\Temp\tor\Tor\libeay32.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\libevent-2-0-5.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\libevent_core-2-0-5.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\libevent_extra-2-0-5.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\libgcc_s_sjlj-1.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\libssp-0.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\ssleay32.dll
%UserProfile%\AppData\Local\Temp\tor\Tor\tor-gencert.exe
%UserProfile%\AppData\Local\Temp\tor\Tor\tor.exe
%UserProfile%\AppData\Local\Temp\tor\Tor\zlib1.dll
%UserProfile%\AppData\Local\Temp\tor.zip
%UserProfile%\AppData\Roaming\tor\
%UserProfile%\AppData\Roaming\tor\cached-certs
%UserProfile%\AppData\Roaming\tor\cached-microdesc-consensus
%UserProfile%\AppData\Roaming\tor\cached-microdescs.new
%UserProfile%\AppData\Roaming\tor\lock
%UserProfile%\AppData\Roaming\tor\state
%UserProfile%\Desktop\test\xor-test.pdf
%UserProfile%\Desktop\README.html
%UserProfile%\Documents\README.html
%UserProfile%\[random].exe
```

Registry entries associated with the Erebus Ransomware

```
HKEY_CLASSES_ROOT\.msc
HKCU\Software\Classes\mscfile
HKCU\Software\Classes\mscfile\shell
HKCU\Software\Classes\mscfile\shell\open
HKCU\Software\Classes\mscfile\shell\open\command
HKCU\Software\Classes\mscfile\shell\open\command\       %UserProfile%\[random].exe
```

Network Communication:

```
http://erebus5743lnq6db.onion/
```

Hashes:

```
SHA256: ed3a685ca65de70b79faf95bbd94c343e73a150e83184f67e0bdb35b11d05791
```

Message Box Alert Text:

```
Files crypted!
Every important file on this computer was crypted. Please look on your documents or
desktop folder for a file called README.html for instructions on how to decrypt them.
```

Ransom Note Text:

```
Data crypted

Every important file (documents,photos,videos etc) on this computer has been
encrypted using an unique key for this computer.
It is impossible to recover your files without this key. You can try to open them
they won't work and will stay that way.

That is, unless you buy a decryption key and decrypt your files.
Click 'recover my files' below to go to the website allowing you to buy the key.
From now on you have 96 hours to recover the key after this time it will be deleted
and your files will stay unusable forever
Your id is : '[id]' you can find this page on your desktop and document folder Use it
to

if the button below doesn't work you need to download a web browser called 'tor
browser'
download by clicking here then install the browser, it's like chrome, firefox or
internet explorer except it allows you to browse to special websites.
once it's launched browse to http://erebus5743lnq6db.onion
```

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

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

- Erebus
- 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

Comments

-

  Kreppelklaus - 5 years ago

  The registry change shouldn't work if registry is PW protected?!
  Like in a domain where users are only users?

-

  Amigo-A - 5 years ago

  Lawrence, thanks for the detailed analysis and increased review!

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: