Thanatos Ransomware Decryptor Released by the Cisco Talos Group

bleepingcomputer.com/news/security/thanatos-ransomware-decryptor-released-by-the-cisco-talos-group

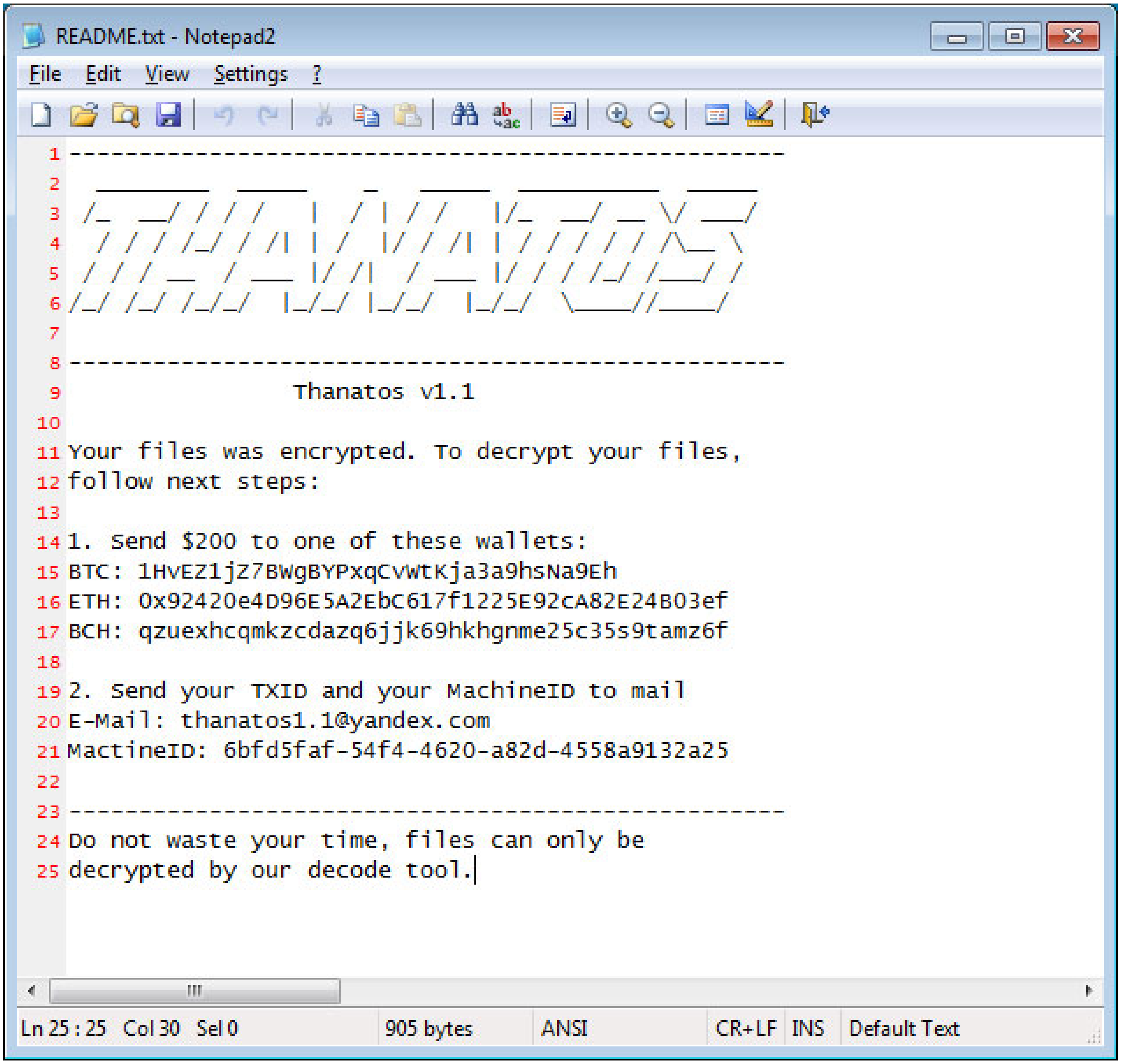
By
Lawrence Abrams

- June 26, 2018
- 04:32 PM
- 3

Back in February we wrote about a new ransomware called Thanatos that was encrypting victim's data, but contained flaws that would not allow the authors to decrypt a victims files even if they paid. Thankfully, the Cisco Talos Group was able to find a method to break the encryption routine in order to create a decryptor that allows victims to recover their files for free.

While Thanatos never had a wide distribution, there were some victims of this ransomware as indicated by submissions to ID Ransomware and from Cisco's analysis. According to Cisco there were multiple campaigns, with version 1.1 being distributed most widely.

This version used a more advanced ransom note and visibly showed the name and version of the ransomware as displayed below. Victim's of this ransomware would also have their files encrypted and the names of the file's would have the .THANATOS extension appended to them. For example, test.jpg would be encrypted and named as test.jpg.THANATOS.



```
--------------------------------------------------
  ________  _____    _   _____  __________  _____
 /_  __/ / / /   |  / | / /   |/_  __/ __ \/ ___/
  / / / /_/ / /| | /  |/ / /| | / / / / / /\__ \
 / / / __  / ___ |/ /|  / ___ |/ / / /_/ /___/ /
/_/ /_/ /_/_/  |_/_/ |_/_/  |_/_/  \____//____/

--------------------------------------------------
                Thanatos v1.1

Your files was encrypted. To decrypt your files,
follow next steps:

1. Send $200 to one of these wallets:
BTC: 1HvEZ1jZ7BWgBYPxqCvWtKja3a9hsNa9Eh
ETH: 0x92420e4D96E5A2EbC617f1225E92cA82E24B03ef
BCH: qzuexhcqmkzcdazq6jjk69hkhgnme25c35s9tamz6f

2. Send your TXID and your MachineID to mail
E-Mail: thanatos1.1@yandex.com
MactineID: 6bfd5faf-54f4-4620-a82d-4558a9132a25

--------------------------------------------------
Do not waste your time, files can only be
decrypted by our decode tool.
```

Thanatos Ransom Note

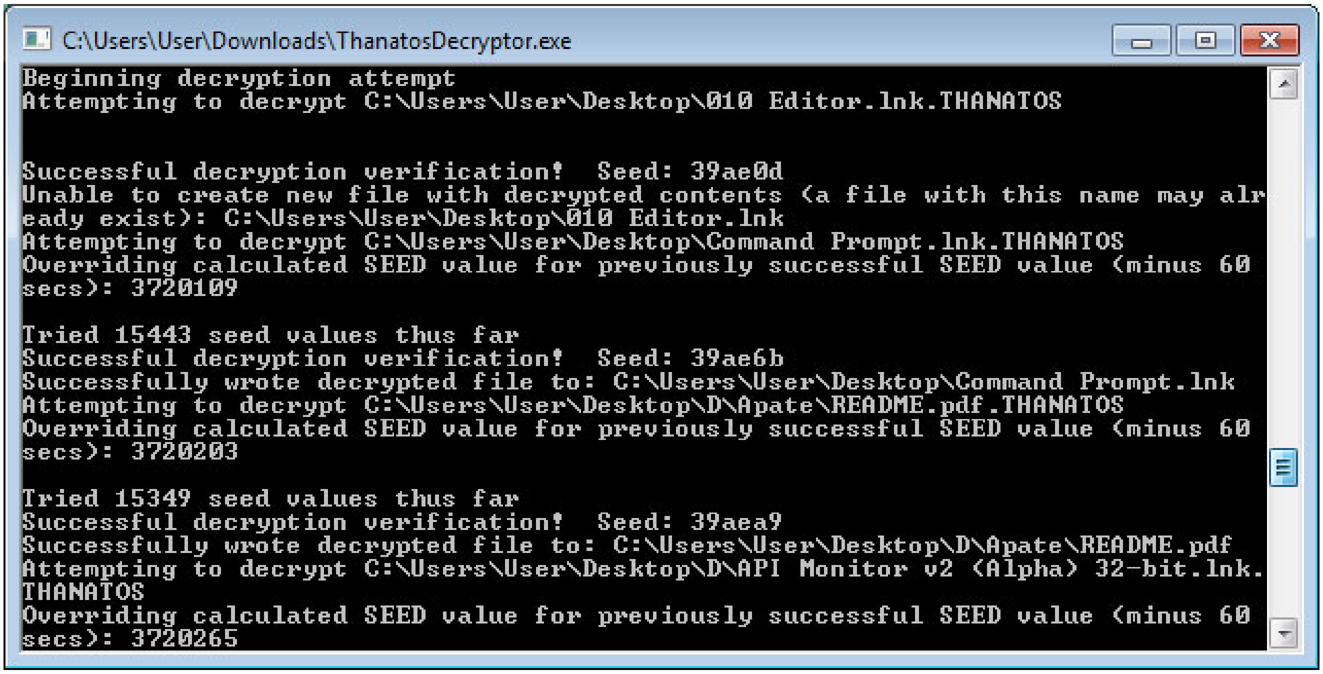
Cisco has also stated that other versions were released that did not contain any contact information and appeared to be designed to simply destroy the victim's data.

"In investigating the distribution mechanisms being used by the attacker to infect victims and remove their ability to access data on their system, we identified an interesting campaign that indicated that at least in this particular case, the attacker had no intention of providing any sort of data decryption to the victim," Cisco's report stated. "The malware appears to have been delivered to the victim as an attachment to a chat message sent to the victim using the Discord chat platform."

As Thanatos was released at one time as an open-source project, it is possible that other developers were creating their own versions using same ransomware code base.

Decrypting files encrypted by the Thanatos Ransomware

To decrypt files encrypted by the Thanatos Ransomware, you should download the Thanatos Decryptor and save it to your desktop. You also need to make sure you have the Microsoft Visual C++ Redistributable for Visual Studio 2017 installed or you will receive errors about missing DLLs when you try to run the decryptor.



```
Beginning decryption attempt
Attempting to decrypt C:\Users\User\Desktop\010 Editor.lnk.THANATOS


Successful decryption verification!  Seed: 39ae0d
Unable to create new file with decrypted contents (a file with this name may alr
eady exist): C:\Users\User\Desktop\010 Editor.lnk
Attempting to decrypt C:\Users\User\Desktop\Command Prompt.lnk.THANATOS
Overriding calculated SEED value for previously successful SEED value (minus 60
secs): 3720109

Tried 15443 seed values thus far
Successful decryption verification!  Seed: 39ae6b
Successfully wrote decrypted file to: C:\Users\User\Desktop\Command Prompt.lnk
Attempting to decrypt C:\Users\User\Desktop\D\Apate\README.pdf.THANATOS
Overriding calculated SEED value for previously successful SEED value (minus 60
secs): 3720203

Tried 15349 seed values thus far
Successful decryption verification!  Seed: 39aea9
Successfully wrote decrypted file to: C:\Users\User\Desktop\D\Apate\README.pdf
Attempting to decrypt C:\Users\User\Desktop\D\API Monitor v2 (Alpha) 32-bit.lnk.
THANATOS
Overriding calculated SEED value for previously successful SEED value (minus 60
secs): 3720265
```

Thanatos Decryptor

Once you have everything you need, simply double-click on the executable and the decryptor will begin to search for files to decrypt. At this time, the decryptor will only decrypt the following file types:

- Image: .gif, .tif, .tiff, .jpg, .jpeg, .png
- Video: .mpg, .mpeg, .mp4, .avi
- Audio: .wav
- Document: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .odt, .ods, .odp, .rtf
- Other: .zip, .7z, .vmdk, .psd, .lnk

Cisco also recommends that the decryptor be run on the same machine that the files were encrypted. The decryption process can take quite a while, so please be patient while it decrypts your files.

For those who are interested in learning how decryptors work, Cisco has open sourced their tool, which be found at the project's Github page.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

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

New RansomHouse group sets up extortion market, adds first victims

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.