Free decryptor released for HermeticRansom victims in Ukraine

bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/

Bill Toulas

By
Bill Toulas

- March 3, 2022
- 11:30 AM
- 3

Avast has released a decryptor for the HermeticRansom ransomware strain used in targeted attacks against Ukrainian systems over the past ten days.

The decryptor is offered as a free-to-download tool from Avast's website and can help Ukrainians restore their data quickly and reliably.

The first signs of HermeticRansom's distribution were observed by ESET researchers on February 23, mere hours before the invasion of Russian troops unfolded in Ukraine.

A weak decoy

The ransomware strain was delivered along with a computer worm named HermeticWizard and served more as a decoy in wiper attacks rather than a tool to support financial extortion. Still, its infections have disrupted vital Ukrainian systems.

Crowdstrike was quick to spot a weakness in the cryptographic schema of the GO-written strain and offered a script to decrypt the files encrypted by HermeticRansom (aka PartyTicket).

"The ransomware contains implementation errors, making its encryption breakable and slow. This flaw suggests that the malware author was either inexperienced writing in Go or invested limited efforts in testing the malware, possibly because the available development time was limited," explains Crowdstrike in a new blog post released on Tuesday.

As BleepingComputer explained on Twitter, the HermeticRansom contains numerous politically oriented string names in the ransomware binary, ransom note, and contact emails (vote2024forjb@protonmail.com and stephanie.jones2024@protonmail.com).

> The malware itself has functions/project names that appear to reference the 403ForBiden meme:
>
> _/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
> _/C_/projects/403forBiden/wHiteHousE.GoodOffice1
> C:/projects/403forBiden/main.go
> main.voteFor403 pic.twitter.com/gcLmHscZbl
>
> — BleepingComputer (@BleepinComputer) February 24, 2022

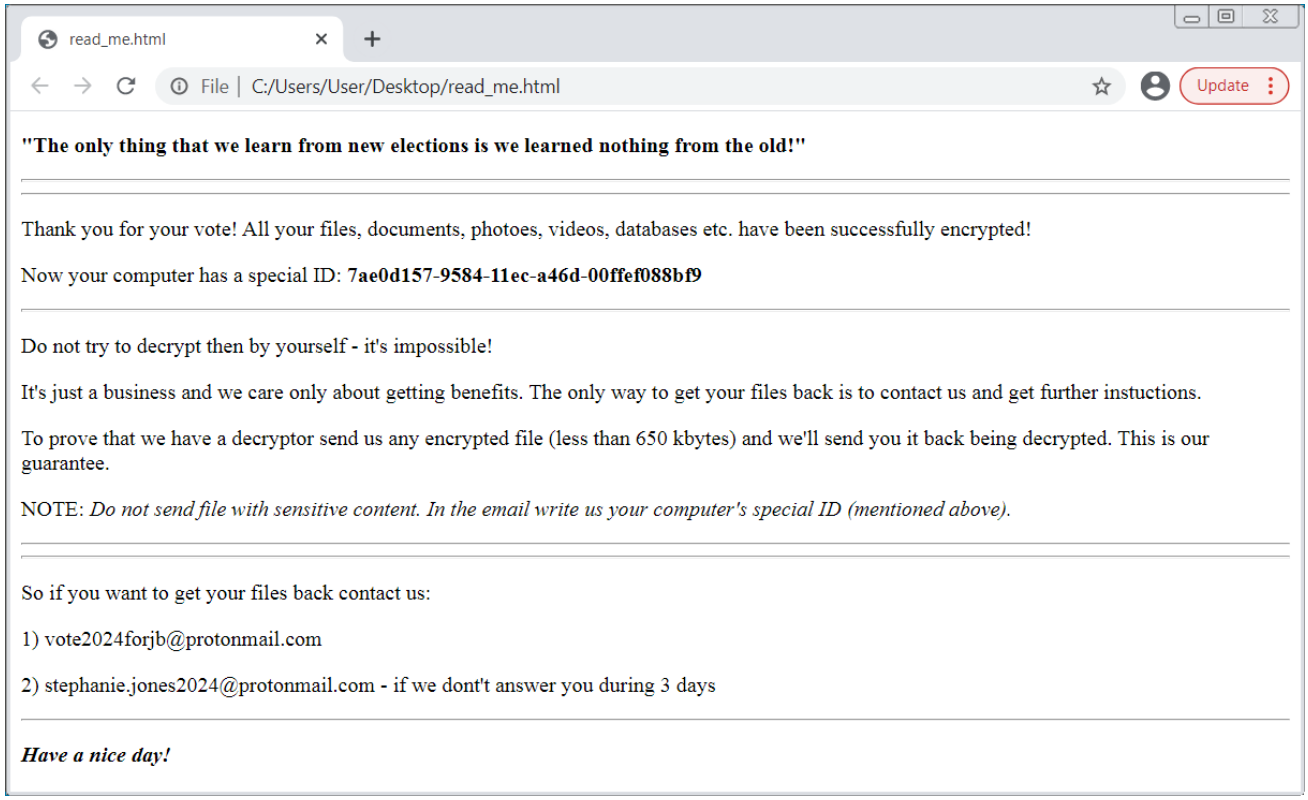
HermeticRansom was never meant to serve as a modern ransomware strain that would lay the ground for double extortion, inflicting financial and reputational damage.

Still a danger

The above doesn't mean that HermeticRansom infections don't impact the targeted machines.

On the contrary, this strain can still encrypt valuable files outside the Program Files and Windows folders, using an RSA-2048 key.

The ransom note seen by the victims has a typical form and content, asking them to contact a ProtonMail address to acquire a decryptor.



HermeticRansom/PartyTicket ransom note

New decryptor recovers files

Although Crowdstrike's script is reliable, it's not easy for everyone to use it in this situation. To make it easier, Avast has released a GUI decryptor that makes it easier to decrypt files encrypted by HermeticRansom.

Also, the tool offers the option to backup the encrypted files to avoid ending up with irreversibly corrupted files if something goes wrong with the encryption process.

Avast's graphical decryptor

For a step-by-step guide on how to use the decryptor, you can start from here.

Related Articles:

Free decryptor released for Yanluowang ransomware victims

Hackers use Conti's leaked ransomware to attack Russian companies

Clop ransomware gang is back, hits 21 victims in a single month

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Decryptor
- HermeticRansom
- HermeticWiper
- PartyTicket
- Ransomware
- Ukraine

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

- 

Mac_Jones - 2 months ago
    -
    -

    WOW!!!! It is nice to see a another company that effortly made a decryptor for the victims of the said ransomware. I just hope that they will make an another one for other ransomwares like Conti, or even STOP.

- 

  horsedoggs - 2 months ago

  -
  -

  They can’t just make them, weakness have to be found or the keys for the big boys eg revil have to be leaked in order for this to happen.

- 

  Mac_Jones - 2 months ago

  -
  -

  "They can’t just make them, weakness have to be found or the keys for the big boys eg revil have to be leaked in order for this to happen. "

  Expect an outcome so time will tell mate ;-)

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: