Free decryptor released for HermeticRansom victims in Ukraine

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

March 3, 2022 11:30 AM 2

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 (https://www.bleepingcomputer.com/news/security/new-worm-and-data-wiper-malware-seen-hitting-ukrainian-networks/) 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 (http://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/) 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).

> **BleepingComputer** @BleepinCompu... · Feb 25, 2022
> Replying to @BleepinComputer
> The ransom note starts with this proverb:
>
> "The only thing that we learn from new elections is we learned nothing from the old!"

BleepingComputer
@BleepinComputer

The malware itself has functions/project names that appear to reference the 403ForBiden meme:

_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
_/C_/projects/403forBiden/wHiteHousE.GoodOffice
1
C:/projects/403forBiden/main.go
main.voteFor403

2:31 AM · Feb 25, 2022

14 Reply Share

Read 1 reply

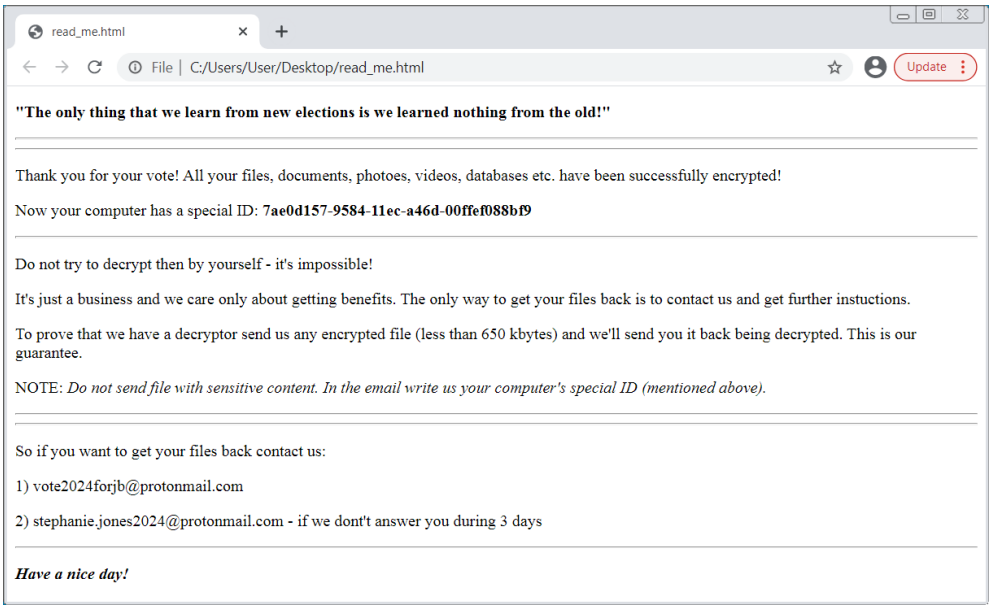
HermeticRansom was never meant to serve as a modern ransomware strain that would lay the ground for double extortion, inflicting financial and reputational damage.

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 (http://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/) 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 (https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/#howto).

Related Articles:

Microsoft: Ukraine hit with FoxBlade malware hours before invasion (https://www.bleepingcomputer.com/news/security/microsoft-ukraine-hit-with-foxblade-malware-hours-before-invasion/)

Ransomware used as decoy in data-wiping attacks on Ukraine (https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/)

CISA and FBI warn of potential data wiping attacks spillover (https://www.bleepingcomputer.com/news/security/cisa-and-fbi-warn-of-potential-data-wiping-attacks-spillover/)

Conti ransomware's internal chats leaked after siding with Russia (https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/)

Ransomware gangs, hackers pick sides over Russia invading Ukraine (https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/)