Ransomware as a distraction

kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/

Ransomware

HermeticRansom cryptor was used as a distraction to support HermeticWiper attacks.

- Editorial Team
- March 1, 2022

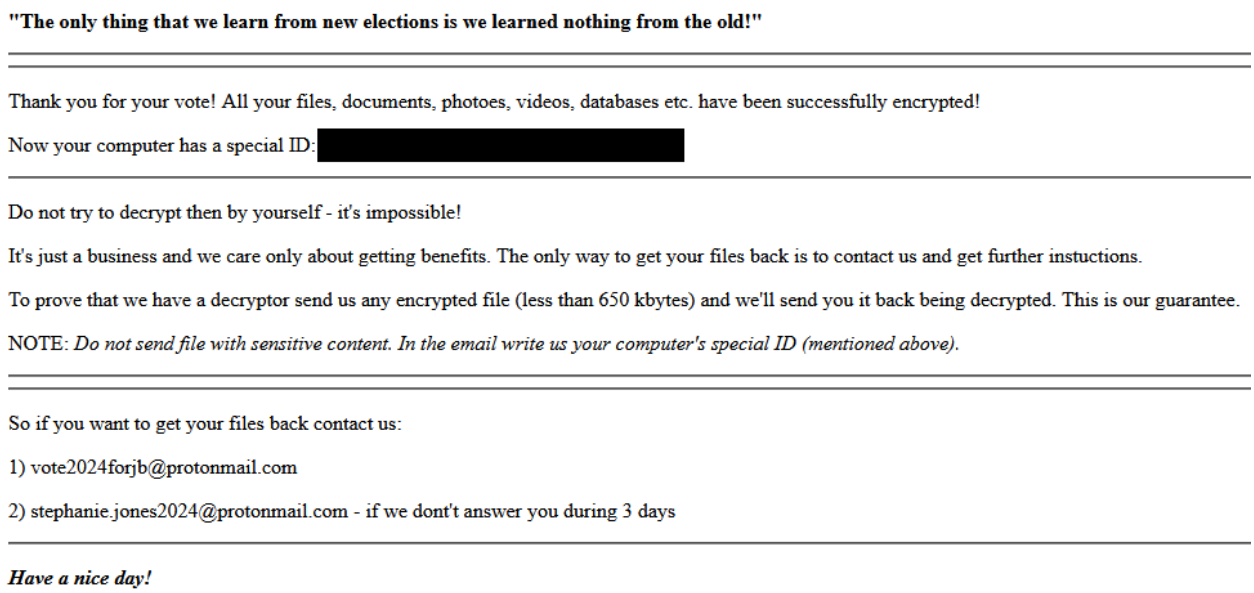
Our researchers analyzed the HermeticRansom malware also known as Elections GoRansom. By and large, this is a fairly simple cryptor. What is interesting in this case is the purpose for which attackers are using it.

HermeticRansom goals

HermeticRansom attacked computers at the same time as another malware known as HermeticWiper, and based on publicly available information from security community, it was used in recent cyberattacks in Ukraine. According to our experts, the relative simplicity and questionable malware workflow implementation suggests that HermeticRansom was used as a smokescreen for HermeticWiper attacks.

What HermeticRansom is capable of

Once infecting the victim's computer, the malware first identifies hard drives and collects a list of directories and files located everywhere except for the Windows and Program Files folders. It then encrypts certain categories of files and renames them adding a .encrypted tag and the email address of the ransomware operators. The malware also creates a read_me.html file in the Desktop folder containing a ransom note with the attackers' contacts. The note looks like this:



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

Ransom note left by HermeticRansom malware

HermeticRansom encrypts files with following extensions: .inf, .acl, .avi, .bat, .bmp, .cab, .cfg, .chm, .cmd, .com, .crt, .css, .dat, .dip, .dll, .doc, .dot, .exe, .gif, .htm, .ico, .iso, .jpg, .mp3, .msi and odt.

HermeticRansom peculiarities

HermeticRansom is written in Golang. It does not use any obfuscation mechanisms, and the encryption method itself is rather cumbersome and inefficient. Judging by these and some other signs, our experts think that this malware was created in a hurry.

You can find a more detailed technical analysis of the malware along with indicators of compromise on our Securelist blog.

How to stay safe

Kaspersky Lab security solutions successfully detect HermeticRansom malware and similar threats. We have a range of tools to protect both home computers and corporate infrastructure, including:

- Kaspersky Internet Security: our multi-platform security solution for home users;
- Kaspersky Endpoint Security Cloud: our solution for business protection;
- Kaspersky Anti-Ransomware Tool: our free corporate solution that can work as an additional layer of protection in parallel with products from other vendors.

- cryptors
- HermeticRansom
- HermeticWiper
- Ransomware
- wipers

Share article

Related