

Elections GoRansom – a smoke screen for the HermeticWiper attack

By GReAT

Published: 2022-03-01 · Archived: 2026-04-05 23:20:41 UTC

Executive summary

On February 24, 2022, Avast Threat Research [published a tweet](#) announcing the discovery of new Golang ransomware, which they called HermeticRansom. This malware was found around the same time the [HermeticWiper](#) was found, and based on publicly available information from security community it was used in recent cyberattacks in Ukraine. The new ransomware was likely used as a smokescreen for the HermeticWiper attack due to its non-sophisticated style and poor implementation.

In this report, we present our analysis of HermeticRansom, which we also call Elections GoRansom.

Our findings in a nutshell:

- Elections GoRansom (aka HermeticRansom) was used to target assets on the same day as HermeticWiper;
- The developers used a sarcastic function-naming scheme related to US presidential elections;
- The malware does not use any kind of obfuscation and has pretty straightforward functionality, suggesting it was created in a short amount of time.

HermeticRansom' technical analysis

The malware is created in Golang and uses no anti-analysis components as string encryption, function names stripping, etc. After execution, it creates an ID which is later used as the key from the array of Latin alphabet characters and numbers using a standard Golang rand function:

```
v5 = runtime_makeslice((runtime__type_0 *)&RTYPE_uint8_0, 32LL, 32LL);
len_1 = v5.len;
cap = v5.cap;
array = (uint8 *)v5.array;
for ( i = 0LL; i < len_1; ++i )
{
    len = math_rand_Intn(36LL);
    if ( len >= 36 )
        runtime_panicindex();
    array = (uint8 *)v5.array;
    *((_BYTE *)v5.array + i) = byte_550986[len];
    len_1 = v5.len;
    cap = v5.cap;
}
_r0.array = array;
_r0.len = len_1;
_r0.cap = cap;
return _r0;
```

ID key generation routine

Then the malware identifies hard drives present on the infected system and collects a list of directories and files, excluding the Windows and Program Files folders.

```
f_data = v2[1];
f_n_len = *((_QWORD *)substr);
f_n_ptr = (uint8 *)((*((__int64 (__golang **)(uint8 *)f_itab + 6))(f_data));
dirname.str = f_n_ptr;
dirname.len = *((_QWORD *)substr);
substra.str = (uint8 *)"Windows";
substra.len = 7LL;
if ( !strings_Contains(dirname, substra) )
{
    dirnamea.str = f_n_ptr;
    dirnamea.len = f_n_len;
    substrb.str = (uint8 *)"Program Files";
    substrb.len = 13LL;
    if ( !strings_Contains(dirname, substrb) )
    {
        if ( ((*((__unsigned __int8 (__golang **)(uint8 *)f_itab + 3))(f_data) )
```

Folder profiling

After that, the ransomware note is created as a “read_me .html” file and dropped to the user’s Desktop folder. The note contains the victim ID and the actor’s contact emails on the ProtonMail domain; emails are hard-coded as seen below:

"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, photos, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: XXXXXXXXXX

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 instructions.

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 don't answer you during 3 days

Have a nice day!

Ransomware note in HTML format

The malware utilizes a strange ineffective encryption workflow – it creates a copies of the initial sample and runs them as separate processes for each file encrypted; copy names are generated using Golang GUID library functions.

5ddf6c27-9593-11ec-a64a-0800277f9fb4.exe	5de0c75a-9593-11ec-a710-0800277f9fb4.exe
5ddf6c27-9593-11ec-a649-0800277f9fb4.exe	5de0c75a-9593-11ec-a711-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64a-0800277f9fb4.exe	5de0ee26-9593-11ec-a711-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64b-0800277f9fb4.exe	5de0ee26-9593-11ec-a712-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64c-0800277f9fb4.exe	5de1b1bd-9593-11ec-a715-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64d-0800277f9fb4.exe	5de1b1bd-9593-11ec-a716-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a64e-0800277f9fb4.exe	5de1eba9-9593-11ec-a716-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a64e-0800277f9fb4.exe	5de1eba9-9593-11ec-a717-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a64f-0800277f9fb4.exe	5de1eba9-9593-11ec-a718-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65a-0800277f9fb4.exe	5de002c6-9593-11ec-a6a0-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65b-0800277f9fb4.exe	5de002c6-9593-11ec-a6a1-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65c-0800277f9fb4.exe	5de002c6-9593-11ec-a6a2-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65d-0800277f9fb4.exe	5de002c6-9593-11ec-a6a3-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65e-0800277f9fb4.exe	5de002c6-9593-11ec-a6a4-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a65f-0800277f9fb4.exe	5de002c6-9593-11ec-a6a5-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a66a-0800277f9fb4.exe	5de002c6-9593-11ec-a6a6-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a650-0800277f9fb4.exe	5de002c6-9593-11ec-a6a7-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a651-0800277f9fb4.exe	5de002c6-9593-11ec-a6a8-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a652-0800277f9fb4.exe	5de002c6-9593-11ec-a6a9-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a653-0800277f9fb4.exe	5de002c6-9593-11ec-a6aa-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a654-0800277f9fb4.exe	5de002c6-9593-11ec-a6ab-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a655-0800277f9fb4.exe	5de002c6-9593-11ec-a6ac-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a656-0800277f9fb4.exe	5de002c6-9593-11ec-a6ae-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a657-0800277f9fb4.exe	5de002c6-9593-11ec-a6af-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a658-0800277f9fb4.exe	5de002c6-9593-11ec-a6b0-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a659-0800277f9fb4.exe	5de002c6-9593-11ec-a6b1-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a660-0800277f9fb4.exe	5de002c6-9593-11ec-a6b2-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a661-0800277f9fb4.exe	5de002c6-9593-11ec-a6b3-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a662-0800277f9fb4.exe	5de002c6-9593-11ec-a6b4-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a663-0800277f9fb4.exe	5de002c6-9593-11ec-a6b5-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a664-0800277f9fb4.exe	5de002c6-9593-11ec-a6b6-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a665-0800277f9fb4.exe	5de002c6-9593-11ec-a6b7-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a666-0800277f9fb4.exe	5de002c6-9593-11ec-a6b8-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a667-0800277f9fb4.exe	5de002c6-9593-11ec-a6b9-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a668-0800277f9fb4.exe	5de002c6-9593-11ec-a6ba-0800277f9fb4.exe
5ddfdbb0-9593-11ec-a669-0800277f9fb4.exe	5de002c6-9593-11ec-a6bb-0800277f9fb4.exe
5ddf6c27-9593-11ec-a64a-0800277f9fb4.exe	3218 K 02/24/22 0
Bytes: 4.65 G, files: 1526, folders: 0	

Self-copies made by HermeticRansom

To encrypt victims' data, HermeticRansom relies on a list of hard-coded files types, as follows:

A screenshot showing a list of file names with extensions. The files are named with a pattern: [vote2024forjib@protonmail.com].[extension]. The extensions include .exe, .encrypt, .encryp, .encrypted, and .encryptedJB. The list is truncated at the bottom.

Encrypted files with the new extension

The malware structures and methods are named in a sarcastic manner related to US presidential elections.

```
C_projects_403forBiden_wHiteHouse_FileName.len = os_Args.array->len;
if ( *((_DWORD *)&runtime_writeBarrier.enabled )
    runtime_gcWriteBarrier();
else
    C_projects_403forBiden_wHiteHouse_FileName.str = str;
typb = (unsigned __int128) C_projects_403forBiden_wHiteHouse_GoodOffice1();
i_2 = *((_DWORD *)&typb + 1);
```

Unstripped function names

HermeticRansom’ attribution

Given the circumstances under which HermeticRansom appeared, including the date, time and victims’ geo-locations, we have moderate confidence it is connected with HermeticWiper’s general objectives – destroying or otherwise making Windows systems unusable due to data loss.

Conclusions

HermeticRansom is an excellent example of a targeted attack preventing victims from using their data while also potentially acting as a smokescreen for further attacks. The simplicity of the code, along with the grammar and

spelling errors left in the ransom note, probably indicate that it was a last-minute operation, potentially deployed to boost the effectiveness of other cyber-attacks on Ukraine.

Indicators of compromise

HermeticRansom MD5

[d5d2c4ac6c724cd63b69ca054713e278](https://securelist.com/elections-goransom-and-hermeticwiper-attack/105960/#d5d2c4ac6c724cd63b69ca054713e278)

Source: <https://securelist.com/elections-goransom-and-hermeticwiper-attack/105960/>