Elections GoRansom – a smoke screen for the HermeticWiper attack

securelist.com/elections-goransom-and-hermeticwiper-attack/105960/

Authors

Expert GReAT

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.

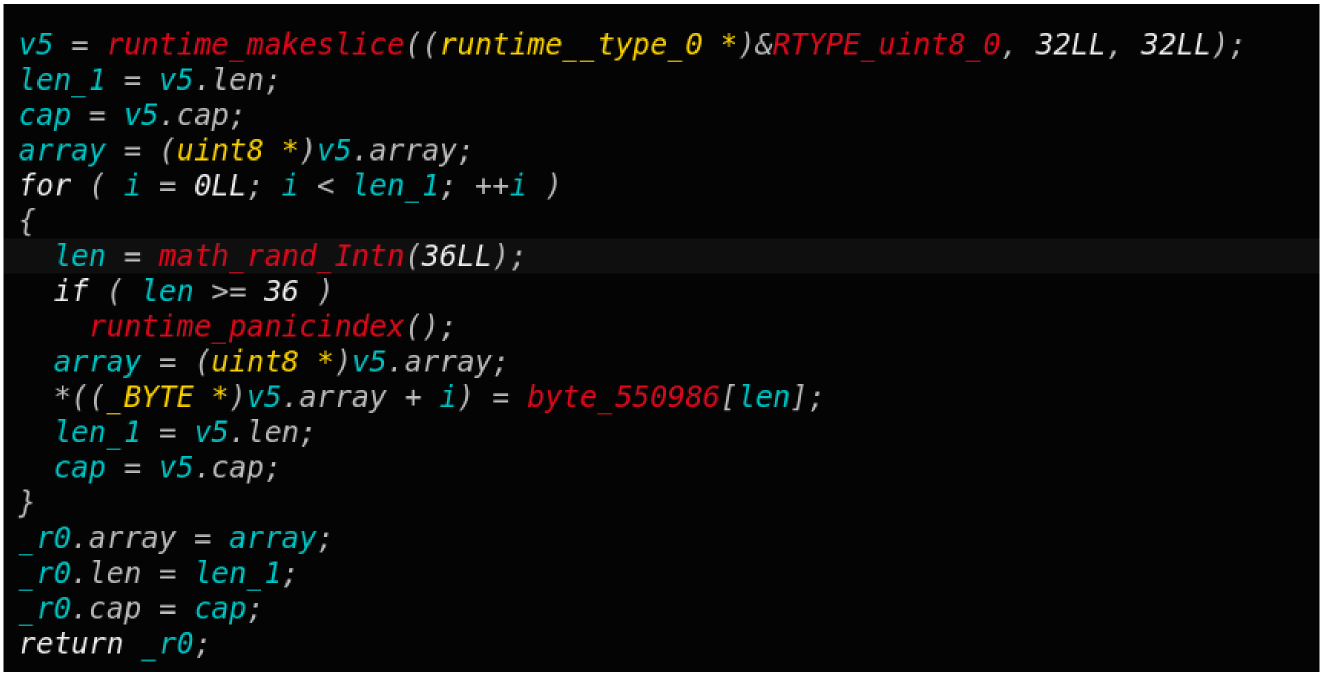
In this report, we present our analysis of HermeticRansom, which we also call Elections GoRansom.

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

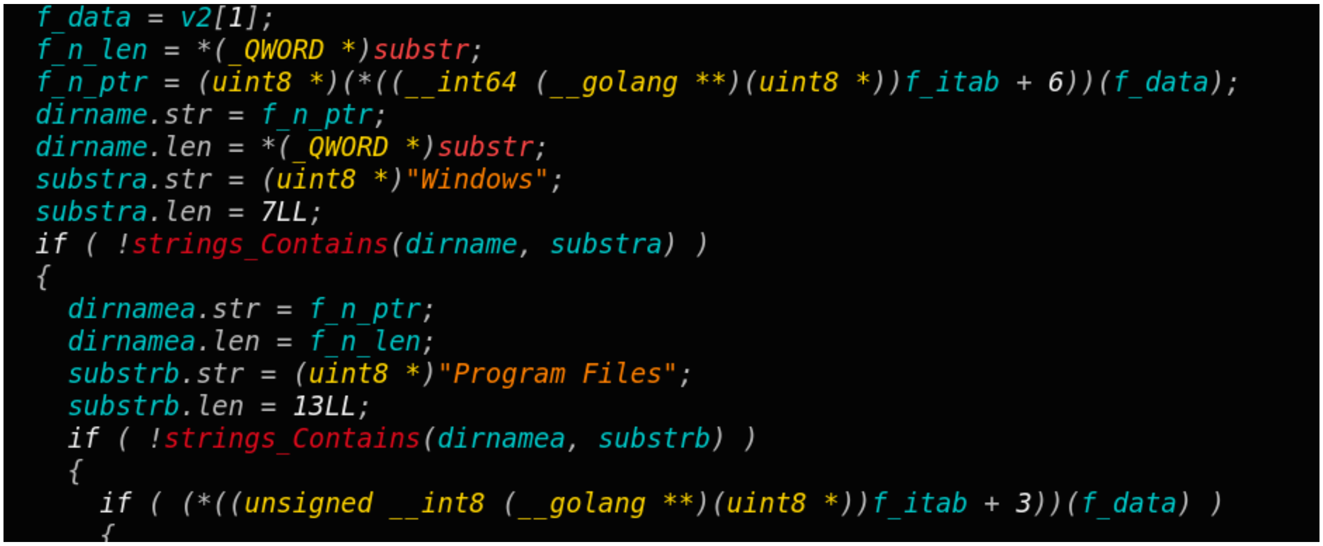
The malware is created in Golang and uses no anti-analysis components as string encryption, function names stripping, etc. After execution, it creates an ID which is later used as the key from the array of Latin alphabet characters and numbers using a standard Golang rand function:



```
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

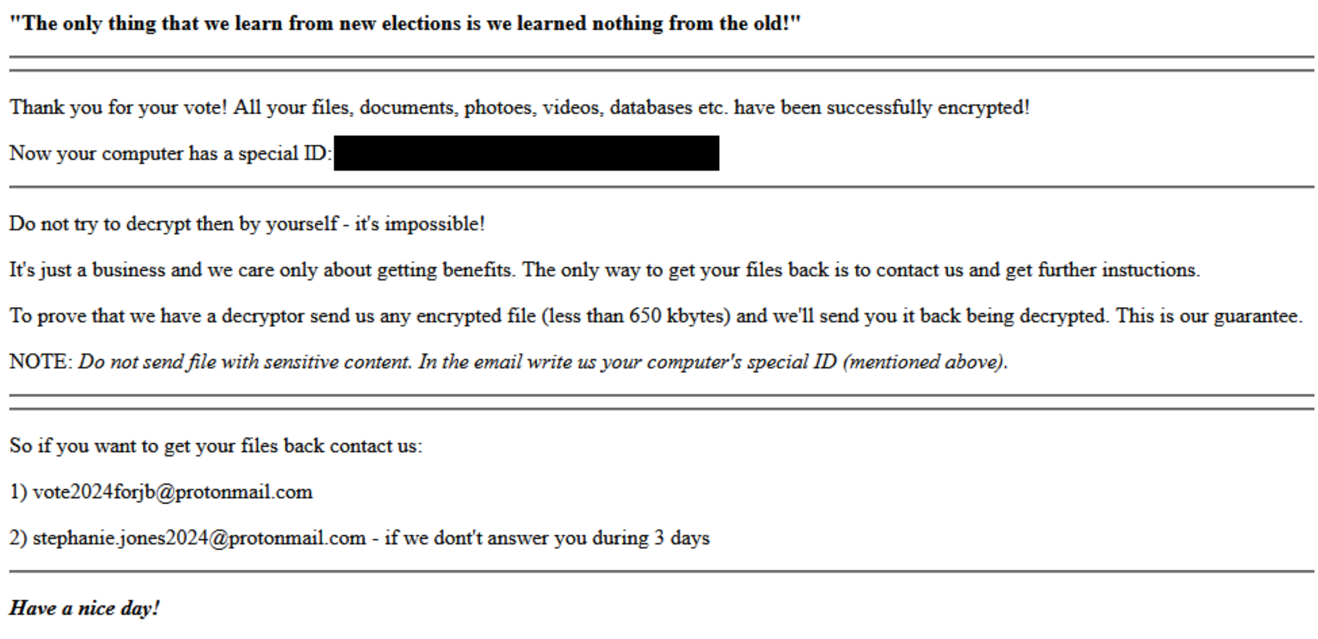
Then the malware identifies hard drives present on the infected system and collects a list of directories and files, excluding the Windows and Program Files folders.



```
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(dirnamea, 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, 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:

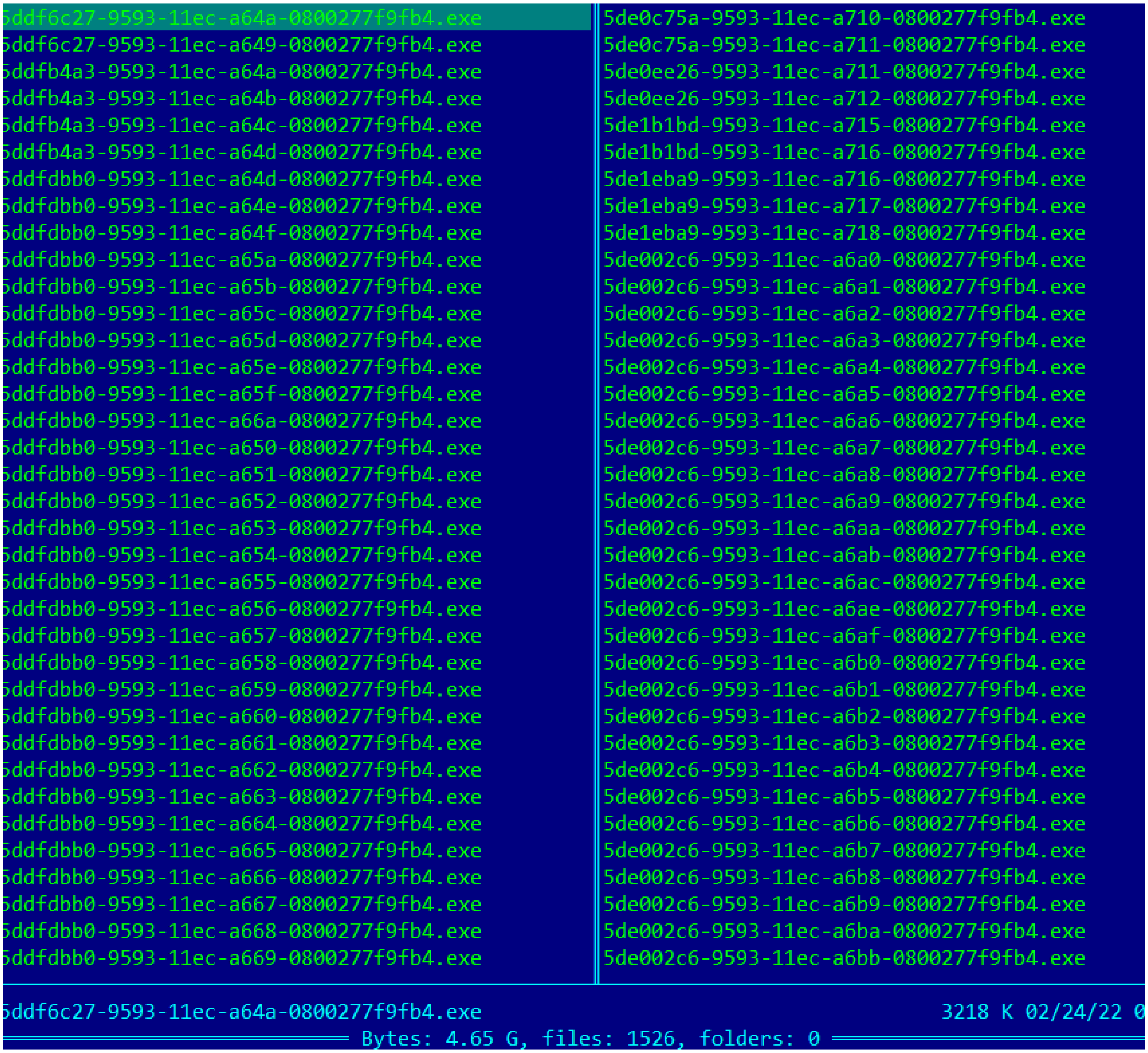
1) vote2024forjb@protonmail.com

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

Have a nice day!

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.

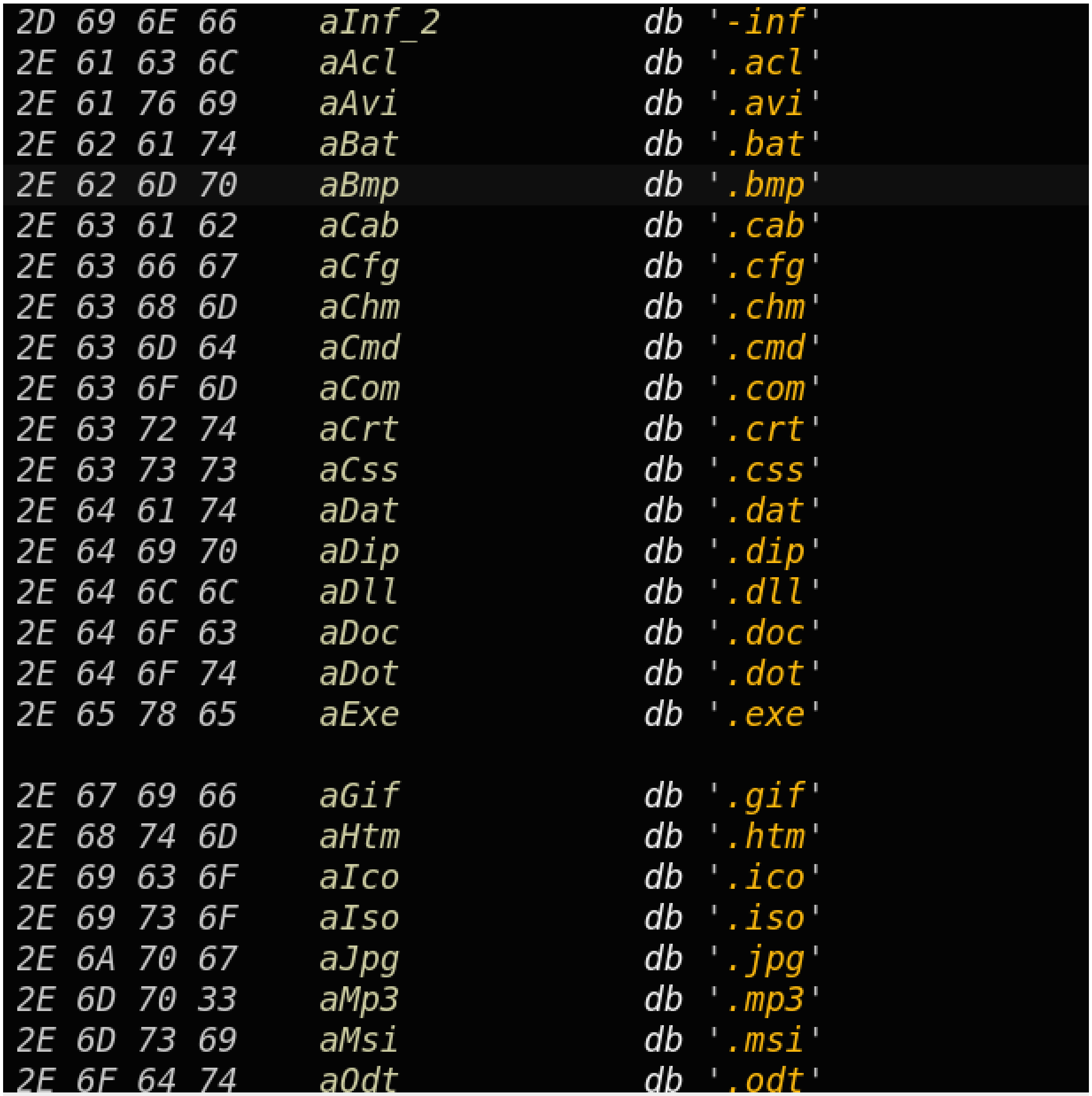


```
5ddf6c27-9593-11ec-a64a-0800277f9fb4.exe  5de0c75a-9593-11ec-a710-0800277f9fb4.exe
5ddf6c27-9593-11ec-a649-0800277f9fb4.exe  5de0c75a-9593-11ec-a711-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64a-0800277f9fb4.exe  5de0ee26-9593-11ec-a711-0800277f9fb4.exe
5ddfb4a3-9593-11ec-a64b-0800277f9fb4.exe  5de0ee26-9593-11ec-a712-0800277f9fb4.exe
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-a64d-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:

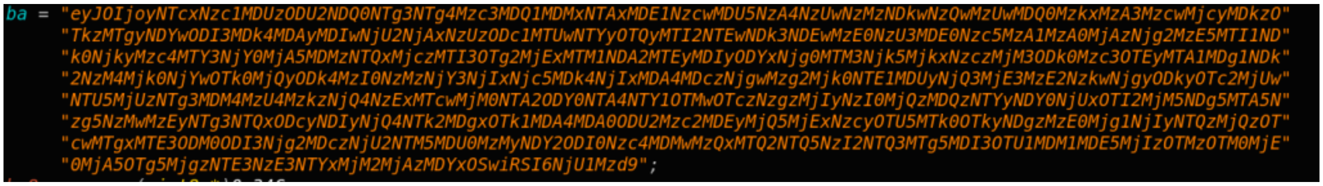


```
2D 69 6E 66     aInf_2          db '-inf'
2E 61 63 6C     aAcl            db '.acl'
2E 61 76 69     aAvi            db '.avi'
2E 62 61 74     aBat            db '.bat'
2E 62 6D 70     aBmp            db '.bmp'
2E 63 61 62     aCab            db '.cab'
2E 63 66 67     aCfg            db '.cfg'
2E 63 68 6D     aChm            db '.chm'
2E 63 6D 64     aCmd            db '.cmd'
2E 63 6F 6D     aCom            db '.com'
2E 63 72 74     aCrt            db '.crt'
2E 63 73 73     aCss            db '.css'
2E 64 61 74     aDat            db '.dat'
2E 64 69 70     aDip            db '.dip'
2E 64 6C 6C     aDll            db '.dll'
2E 64 6F 63     aDoc            db '.doc'
2E 64 6F 74     aDot            db '.dot'
2E 65 78 65     aExe            db '.exe'

2E 67 69 66     aGif            db '.gif'
2E 68 74 6D     aHtm            db '.htm'
2E 69 63 6F     aIco            db '.ico'
2E 69 73 6F     aIso            db '.iso'
2E 6A 70 67     aJpg            db '.jpg'
2E 6D 70 33     aMp3            db '.mp3'
2E 6D 73 69     aMsi            db '.msi'
2E 6F 64 74     aOdt            db '.odt'
```

List of hardcoded file extensions to encrypt

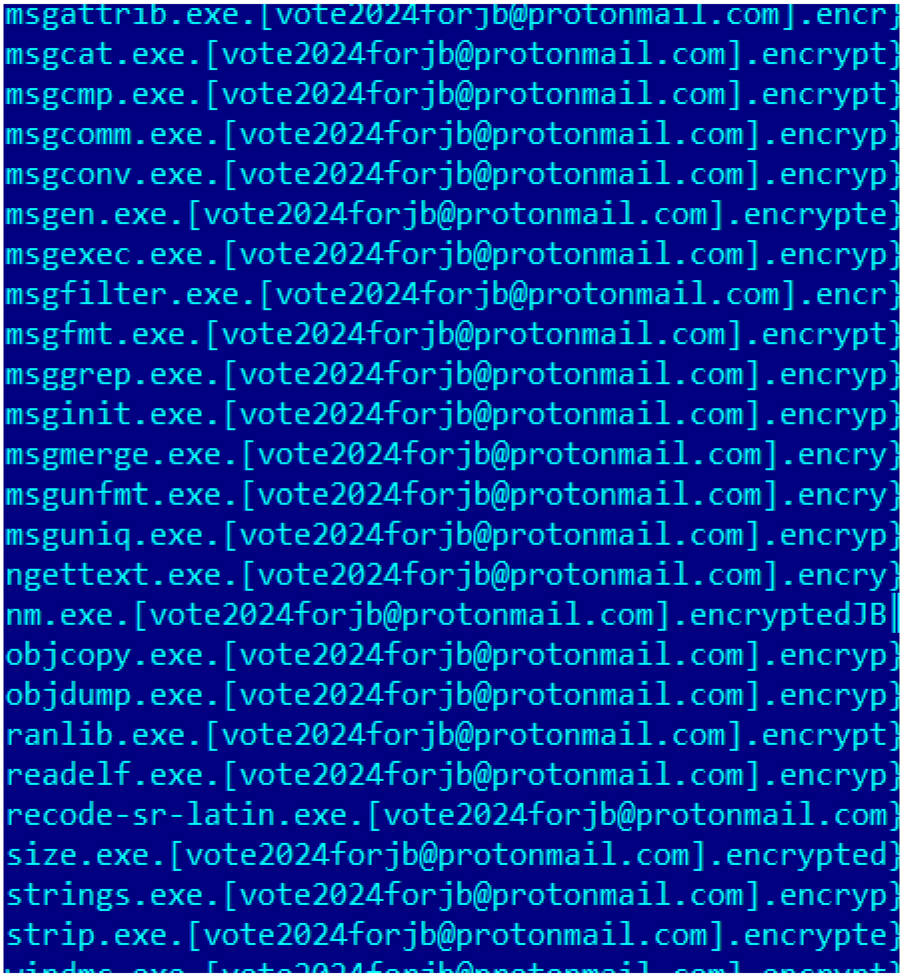
Files are encrypted using the AES algorithm with the generated key. Then the AES key is encrypted with RSA-OAEP. OAEP is parameterized with a hash function that is used as a random oracle. The hashing function is SHA-256. The RSA public key is hard-coded as a base64 blob. After decoding the key in JSON format, it is converted to a byte array:



```
ba = "eyJOIjoyNTcxNzc1MDUzODU2NDQ0NTg3NTg4Mzc3MDQ1MDMxNTAxMDE1NzcwMDU5NzA4NzUwNzMzNDkwNzQwMzUwMDQ0MzkxMzA3MzcwMjcyMDkzO"
     "TkzMTgyNDYwODI3MDk4MDAyMDIwNjU2NjAxNzUzODc1MTUwNTYyOTQyMTI2NTEwNDk3NDEwMzE0NzU3MDE0Nzc5MzA1MzA0MjAzNjg2MzE5MTI1ND"
     "k0NjkyMzc4MTY3NjY0MjA5MDMzNTQxMjczMTI3OTg2MjExMTM1NDA2MTEyMDIyODYxNjg0MTM3Njk5MjkxNzczMjM3ODk0Mzc3OTEyMTA1MDg1NDk"
     "2NzM4Mjk0NjYwOTk0MjQyODk4MzI0NzMzNjY3NjIxNjc5MDk4NjIxMDA4MDczNjgwMzg2Mjk0NTE1MDUyNjQ3MjE3MzE2NzkwNjgyODkyOTc2MjUw"
     "NTU5MjUzNTg3MDM4MzU4MzkzNjQ4NzExMTcwMjM0NTA2ODY0NTA4NTY1OTMwOTczNzgzMjIyNzI0MjQzMDQzNTYyNDY0NjUxOTI2MjM5NDg5MTA5N"
     "zg5NzMwMzEyNTg3NTQxODcyNDIyNjQ4NTk2MDgxOTk1MDA4MDA0ODU2Mzc2MDEyMjQ5MjExNzcyOTU5MTk0OTkyNDgzMzE0Mjg1NjIyNTQzMjQzOT"
     "cwMTgxMTE3ODM0ODI3Njg2MDczNjU2NTM5MDU0MzMyNDY2ODI0Nzc4MDMwMzQxMTQ2NTQ5NzI2NTQ3MTg5MDI3OTU1MDM1MDE5MjIzOTMzOTM0MjE"
     "0MjA5OTg5MjgzNTE3NzE3NTYxMjM2MjAzMDYxOSwiRSI6NjU1Mzd9";
```

Hardcoded encryption public key

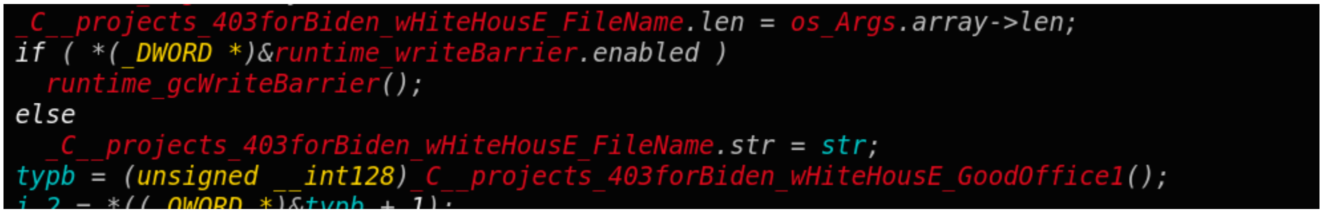
Once files are encrypted, HermeticRansom appends a “.encryptedJB” extension to each. Also the ProtonMail email address is appended to the filename:



```
msgattrib.exe.[vote2024forjb@protonmail.com].encr
msgcat.exe.[vote2024forjb@protonmail.com].encrypt
msgcmp.exe.[vote2024forjb@protonmail.com].encrypt
msgcomm.exe.[vote2024forjb@protonmail.com].encryp
msgconv.exe.[vote2024forjb@protonmail.com].encryp
msgen.exe.[vote2024forjb@protonmail.com].encrypte
msgexec.exe.[vote2024forjb@protonmail.com].encryp
msgfilter.exe.[vote2024forjb@protonmail.com].encr
msgfmt.exe.[vote2024forjb@protonmail.com].encrypt
msggrep.exe.[vote2024forjb@protonmail.com].encryp
msginit.exe.[vote2024forjb@protonmail.com].encryp
msgmerge.exe.[vote2024forjb@protonmail.com].encry
msgunfmt.exe.[vote2024forjb@protonmail.com].encry
msguniq.exe.[vote2024forjb@protonmail.com].encryp
ngettext.exe.[vote2024forjb@protonmail.com].encry
nm.exe.[vote2024forjb@protonmail.com].encryptedJB
objcopy.exe.[vote2024forjb@protonmail.com].encryp
objdump.exe.[vote2024forjb@protonmail.com].encryp
ranlib.exe.[vote2024forjb@protonmail.com].encrypt
readelf.exe.[vote2024forjb@protonmail.com].encryp
recode-sr-latin.exe.[vote2024forjb@protonmail.com
size.exe.[vote2024forjb@protonmail.com].encrypted
strings.exe.[vote2024forjb@protonmail.com].encryp
strip.exe.[vote2024forjb@protonmail.com].encrypte
windmc.exe.[vote2024forjb@protonmail.com].encrypt
```

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 = *((_QWORD *)&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

- Malware Descriptions
- Malware Technologies
- Ransomware
- Targeted attacks
- Wiper

Authors

GReAT

Elections GoRansom – a smoke screen for the HermeticWiper attack

Your email address will not be published. Required fields are marked *