Ragnar Locker – Malware analysis

seguranca-informatica.pt/ragnar-locker-malware-analysis/

August 19, 2021

The popularity of ransomware threats does not appear to be decreasing. Instead, more and sophisticated ransomware threats are being deployed. Ragnar Locker is a new data encryption malware in this style.

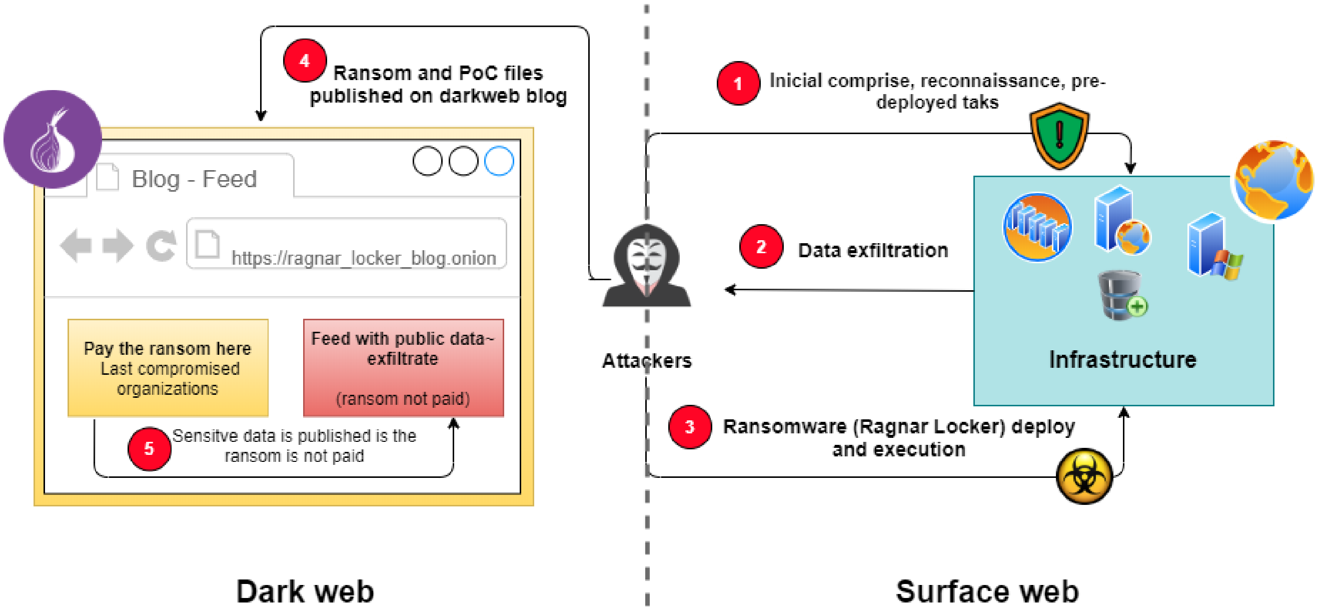
Ragnar Locker is ransomware that affects devices running Microsoft Windows operating systems. It was initially observed towards the end of December 2019 as part of a series of attacks against compromised networks.

In general, this malware is deployed manually after an initial compromise, network reconnaissance and pre-deployed tasks on the network. This shows that this is a more complex operation than most ransomware propagation campaigns.

Before starting the Ragnar Locker ransomware, attackers inject a module capable of collecting sensitive data from infected machines and upload it to their servers. Next, threat actors behind the malware notify the victim the files will be released to the public if the ransom is not paid.

Modus operandi

The next diagram shows how criminals are compromising infrastructures and organizations using this data encryption malware.



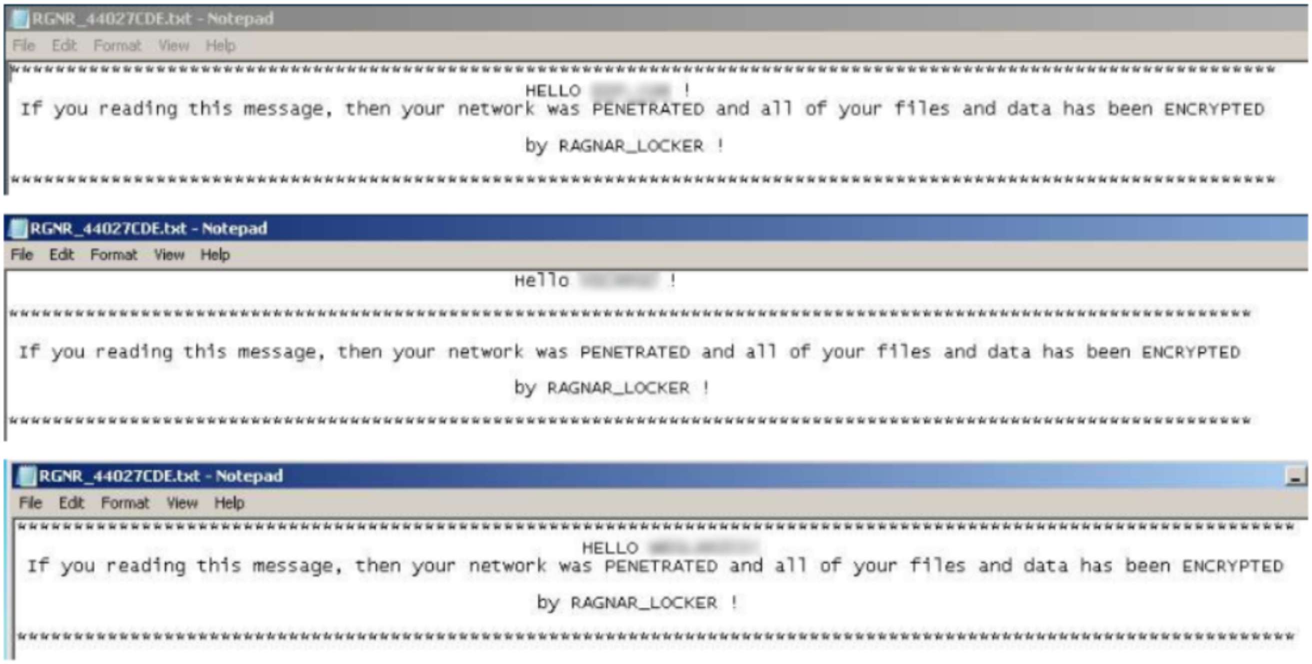
4 Ransom and PoC files published on darkweb blog
1 Inicial comprise, reconnaissance, pre-deployed taks
Blog - Feed
https://ragnar_locker_blog.onion
2 Data exfiltration
Pay the ransom here Last compromised organizations
Feed with public data~ exfiltrate (ransom not paid)
Attackers
Infrastructure
3 Ransomware (Ragnar Locker) deploy and execution
5 Sensitve data is published is the ransom is not paid
Dark web
Surface web

Figure 1: *High-level diagram of the Ragnar Locker infection chain.*

As highlighted in the diagram above, there is a group of steps executed by Ragnar Locker operators every time an organization or infrastructure is impacted. Digging into the details, attackers first compromise networks, infrastructures, and organizations using found vulnerabilities or even through social engineering such as phishing attacks, spear phishing and BEC attacks.

During the compromise process, reconnaissance, pre-deployment tasks, and data exfiltration are performed before executing the piece of ransomware (Figure 1 — labels 1 and 2). When the data exfiltration process is completed, a ransomware deployment is performed manually (label 3).

Notice that each malware sample is unique, with the specific ransom note hardcoded inside the malware. The affected group name, the links to the bitcoin wallet, and the links to a dark web blog are embedded inside the binary as presented below.



RGNR_44027CDE.txt - Notepad
File Edit Format View Help

```
*****************************************************************************************************
                                        HELLO [redacted] !
 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
                                        by RAGNAR_LOCKER !
*****************************************************************************************************
```

RGNR_44027CDE.txt - Notepad
File Edit Format View Help

```
                                        Hello [redacted] !
*****************************************************************************************************
 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
                                        by RAGNAR_LOCKER !
*****************************************************************************************************
```

RGNR_44027CDE.txt - Notepad
File Edit Format View Help

```
*****************************************************************************************************
                                        HELLO [redacted]
 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED
                                        by RAGNAR_LOCKER !
*****************************************************************************************************
```

Figure 2: *Parts of the ransom notes from the recent attacks.*

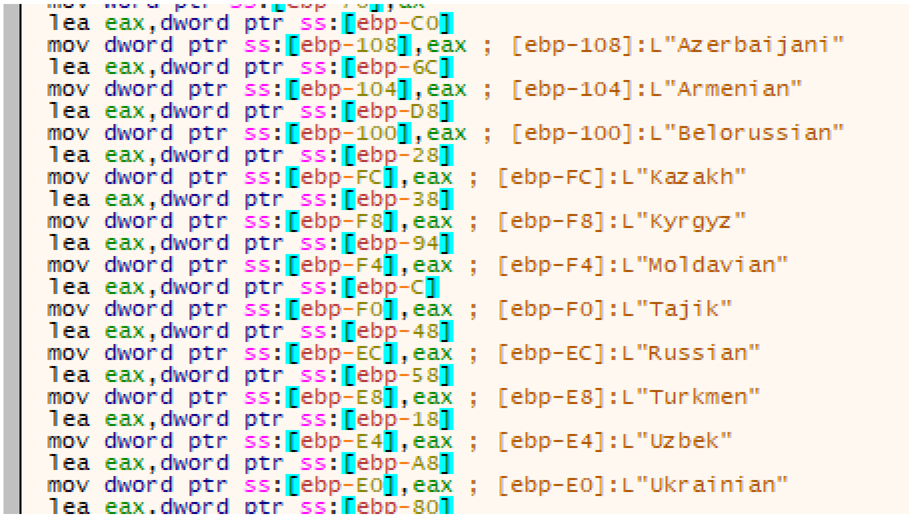
When the ransomware starts, it enumerates running processes and stops if some of these services contain specific strings, such as:

```
Vss
sql
memtas
mepocs
sophos
veeam
backup
pulseway
logme
logmein
connectwise
splashtop
Kaseya
```

Ransomware in this line often disables some services as a way to bypass security protections and also database and backup systems to increase the impact of the attack. Also, database and mail services are stopped so that their data can be encrypted during the infection process.

One of the particularities that spotlight Ragnar Locker is that it is targeting specifically remote management software often used by managed service providers (MSPs), such as the popular ConnectWise and Kaseya software.

This data encryption malware infects computers based on their language settings. When first started, Ragnar Locker checks the configured Windows language preferences. This piece of malware terminates the process if the setting is configured as one of the former USSR countries.

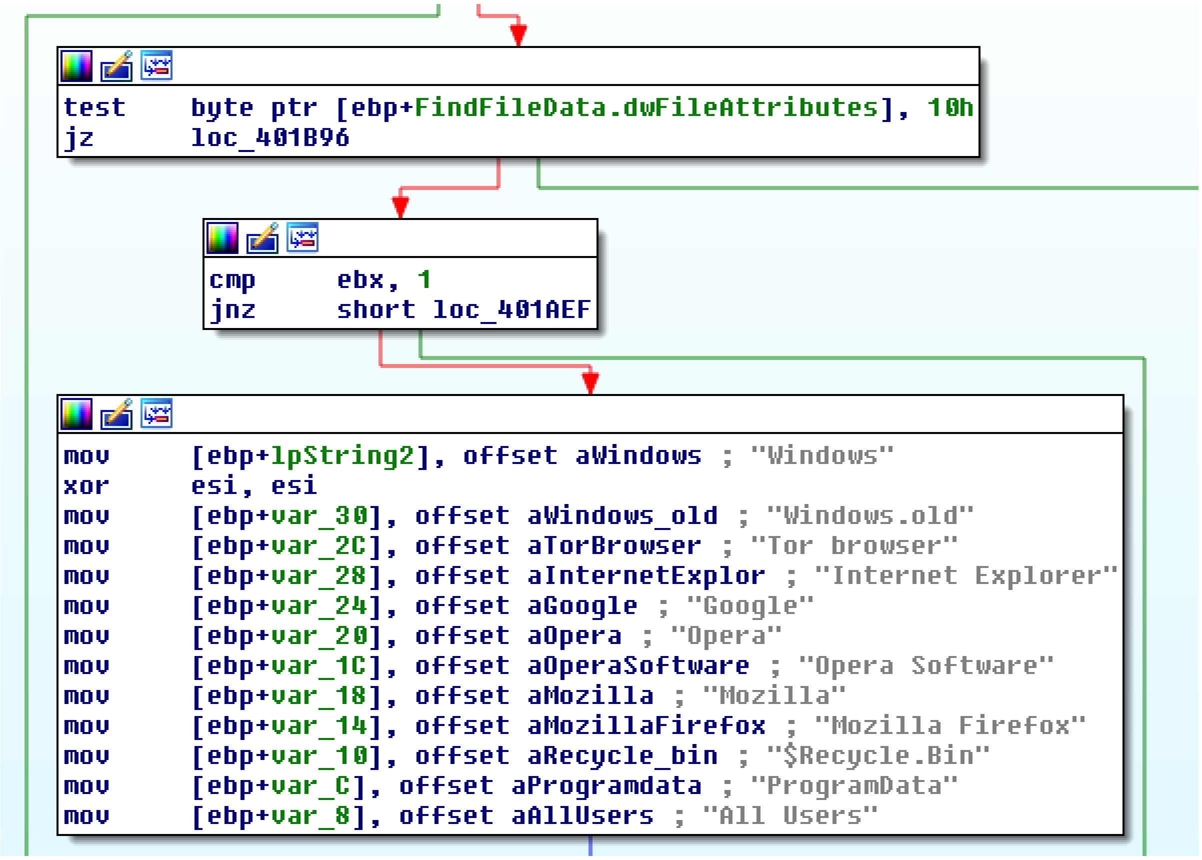


```
lea eax,dword ptr ss:[ebp-C0]
mov dword ptr ss:[ebp-108],eax ; [ebp-108]:L"Azerbaijani"
lea eax,dword ptr ss:[ebp-6C]
mov dword ptr ss:[ebp-104],eax ; [ebp-104]:L"Armenian"
lea eax,dword ptr ss:[ebp-D8]
mov dword ptr ss:[ebp-100],eax ; [ebp-100]:L"Belorussian"
lea eax,dword ptr ss:[ebp-28]
mov dword ptr ss:[ebp-FC],eax ; [ebp-FC]:L"Kazakh"
lea eax,dword ptr ss:[ebp-38]
mov dword ptr ss:[ebp-F8],eax ; [ebp-F8]:L"Kyrgyz"
lea eax,dword ptr ss:[ebp-94]
mov dword ptr ss:[ebp-F4],eax ; [ebp-F4]:L"Moldavian"
lea eax,dword ptr ss:[ebp-C]
mov dword ptr ss:[ebp-F0],eax ; [ebp-F0]:L"Tajik"
lea eax,dword ptr ss:[ebp-48]
mov dword ptr ss:[ebp-EC],eax ; [ebp-EC]:L"Russian"
lea eax,dword ptr ss:[ebp-58]
mov dword ptr ss:[ebp-E8],eax ; [ebp-E8]:L"Turkmen"
lea eax,dword ptr ss:[ebp-18]
mov dword ptr ss:[ebp-E4],eax ; [ebp-E4]:L"Uzbek"
lea eax,dword ptr ss:[ebp-A8]
mov dword ptr ss:[ebp-E0],eax ; [ebp-E0]:L"Ukrainian"
lea eax,dword ptr ss:[ebp-80]
```

Figure 3: *Ragnar Locker stops when executed on former USSR countries.*

After that, Ragnar Locker will begin the encryption process. When encrypting files, it will skip files in the following folders, file names and extensions.

One of the interesting findings is the “**Tor browser**” folder.



```
test    byte ptr [ebp+FindFileData.dwFileAttributes], 10h
jz      loc_401B96
```

```
cmp     ebx, 1
jnz     short loc_401AEF
```

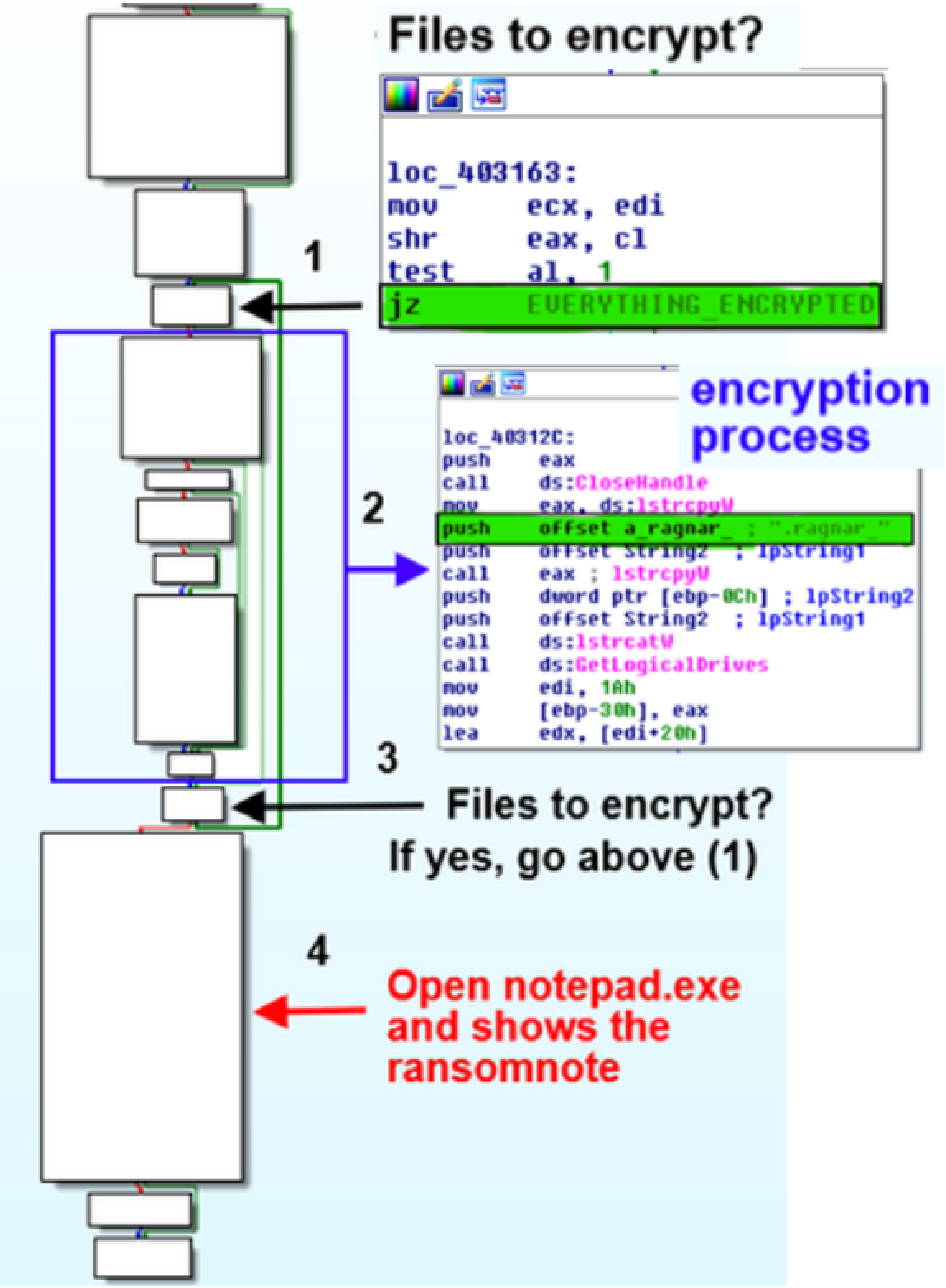
```
mov     [ebp+lpString2], offset aWindows ; "Windows"
xor     esi, esi
mov     [ebp+var_30], offset aWindows_old ; "Windows.old"
mov     [ebp+var_2C], offset aTorBrowser ; "Tor browser"
mov     [ebp+var_28], offset aInternetExplor ; "Internet Explorer"
mov     [ebp+var_24], offset aGoogle ; "Google"
mov     [ebp+var_20], offset aOpera ; "Opera"
mov     [ebp+var_1C], offset aOperaSoftware ; "Opera Software"
mov     [ebp+var_18], offset aMozilla ; "Mozilla"
mov     [ebp+var_14], offset aMozillaFirefox ; "Mozilla Firefox"
mov     [ebp+var_10], offset aRecycle_bin ; "$Recycle.Bin"
mov     [ebp+var_C], offset aProgramdata ; "ProgramData"
mov     [ebp+var_8], offset aAllUsers ; "All Users"
```

Figure 4: *Folders not encrypted by Ragnar Locker.*

This detail reveals this malware is also impacting security professionals and everyone that use this specific web browser to navigate in the dark web. The completed list can be observed in the following table.

```
kernel32.dll
Windows
Windows.old
Tor browser
Internet Explorer
Google
Opera
Opera Software
Mozilla
Mozilla Firefox
$Recycle.Bin
ProgramData
All Users
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
bootmgr
bootmgr.efi
bootmgfw.efi
desktop.ini
iconcache.db
ntldr
ntuser.dat
ntuser.dat.log
ntuser.ini
thumbs.db
.sys
.dll
.lnk
.msi
.drv
.exe
```

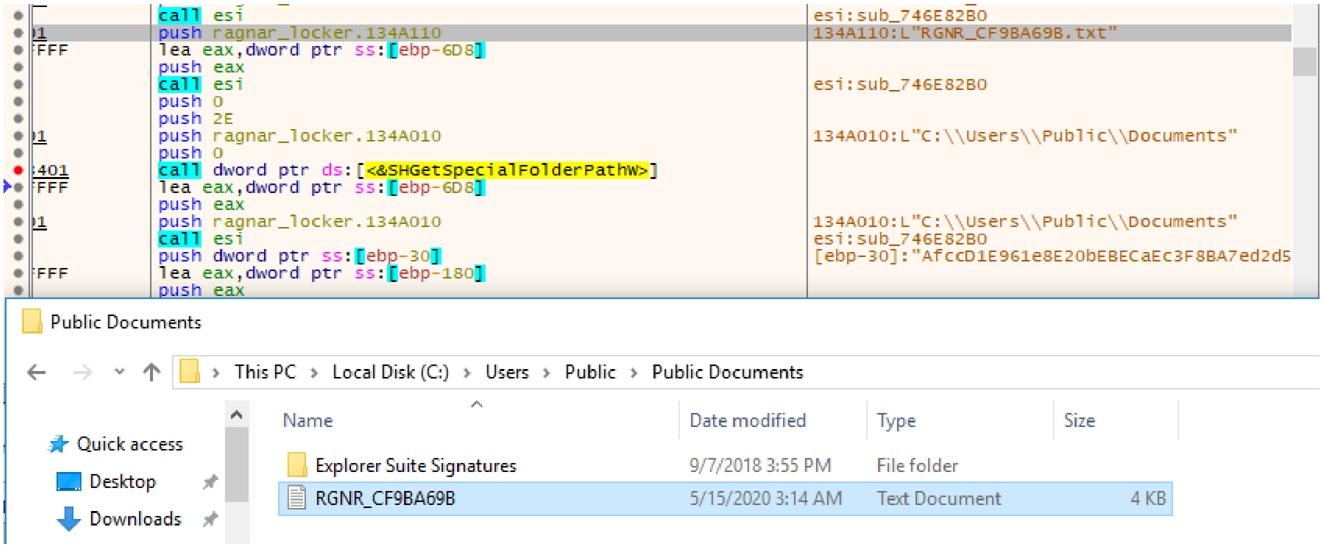
Ragnar Locker adds the hardcoded extension “**.ragnar_***” appended to the end of the file name and “*****” is replaced by a generated and unique ID. All the available files inside physical drives are encrypted and, in the end, the notepad.exe process is opened and showing the ransom note file created on the victim’s system directory, as shown in the diagram below.



```
loc_403163:
mov     ecx, edi
shr     eax, cl
test    al, 1
jz      EVERYTHING_ENCRYPTED
```

```
loc_40312C:
push    eax
call    ds:CloseHandle
mov     eax, ds:lstrcpyW
push    offset a_ragnar_ ; ".ragnar_"
push    offset String2  ; lpString1
call    eax ; lstrcpyW
push    dword ptr [ebp-0Ch] ; lpString2
push    offset String2  ; lpString1
call    ds:lstrcatW
call    ds:GetLogicalDrives
mov     edi, 1Ah
mov     [ebp-30h], eax
lea     edx, [edi+20h]
```

Figure 5: *Ragnar Locker encryption process.*



```
        call esi                                  esi:sub_746E82B0
1       push ragnar_locker.134A110                134A110:L"RGNR_CF9BA69B.txt"
FFF     lea eax,dword ptr ss:[ebp-6D8]
        push eax
        call esi                                  esi:sub_746E82B0
        push 0
        push 2E
1       push ragnar_locker.134A010                134A010:L"C:\\Users\\Public\\Documents"
        push 0
401     call dword ptr ds:[<&SHGetSpecialFolderPathW>]
FFF     lea eax,dword ptr ss:[ebp-6D8]
        push eax
1       push ragnar_locker.134A010                134A010:L"C:\\Users\\Public\\Documents"
        call esi                                  esi:sub_746E82B0
        push dword ptr ss:[ebp-30]                [ebp-30]:"AfccD1E961e8E20bEBECaEc3F8BA7ed2d5
FFF     lea eax,dword ptr ss:[ebp-180]
        push eax
```

Public Documents

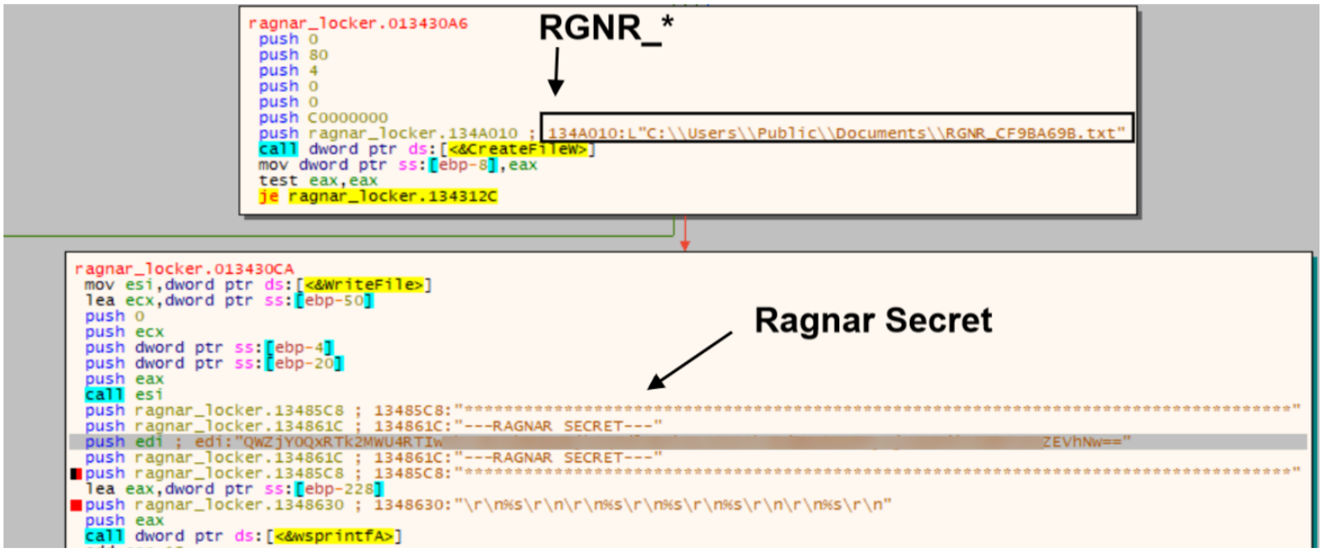
This PC › Local Disk (C:) › Users › Public › Public Documents

Name	Date modified	Type	Size
Explorer Suite Signatures	9/7/2018 3:55 PM	File folder	
RGNR_CF9BA69B	5/15/2020 3:14 AM	Text Document	4 KB

***Figure 6**: Ransom note created on “Public Documents” folder.*

In detail, a ransom note file is dropped every folder, not including those observed in Table 2.

The ransom note file starts with the “**RGNR_***” prefix, and the ID also used and appended to the encrypted files.

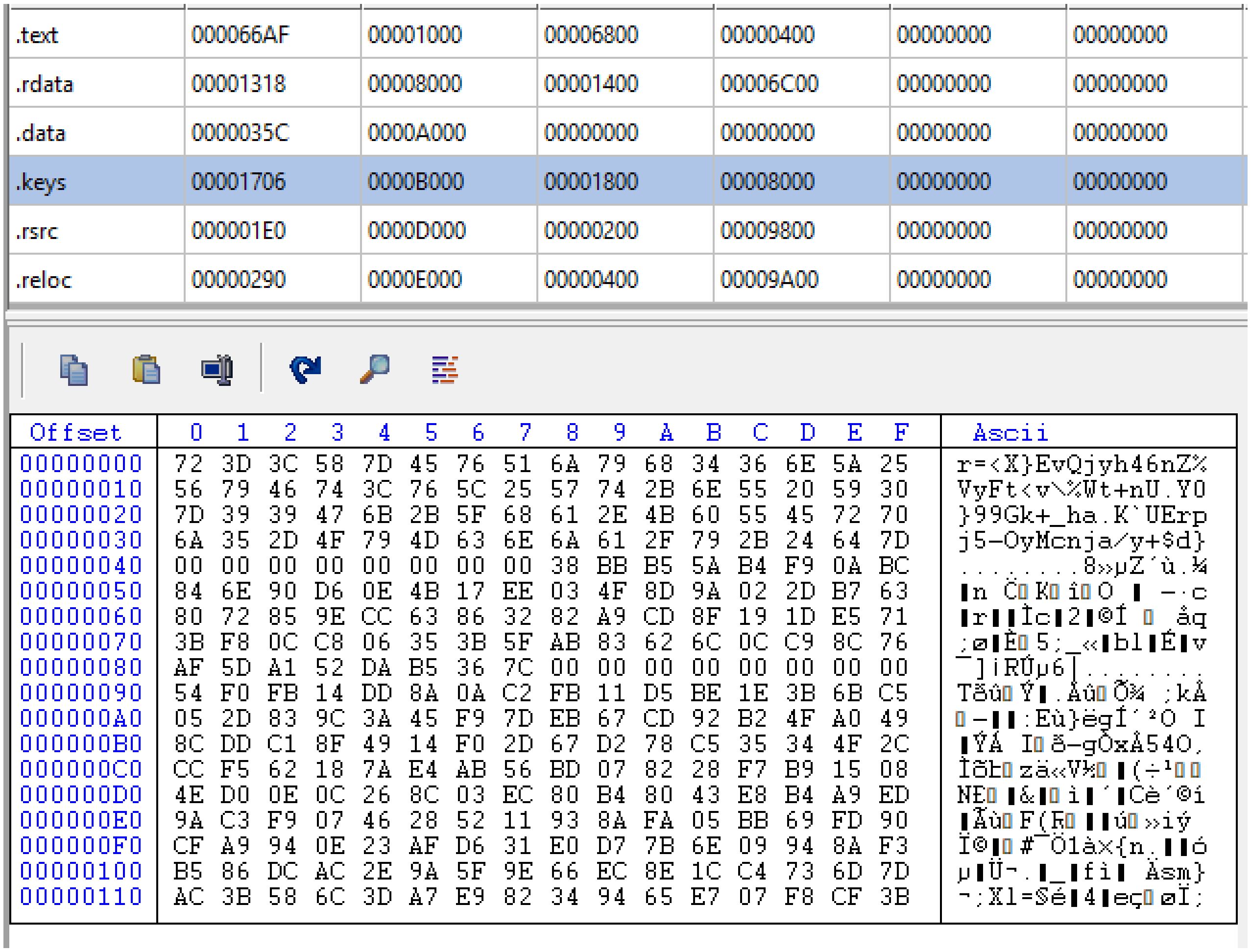


```
ragnar_locker.013430A6
 push 0
 push 80
 push 4
 push 0
 push 0
 push C0000000
 push ragnar_locker.134A010 ; 134A010:L"C:\\Users\\Public\\Documents\\RGNR_CF9BA69B.txt"
 call dword ptr ds:[<&CreateFileW>]
 mov dword ptr ss:[ebp-8],eax
 test eax,eax
 je ragnar_locker.134312C

ragnar_locker.013430CA
 mov esi,dword ptr ds:[<&WriteFile>]
 lea ecx,dword ptr ss:[ebp-50]
 push 0
 push ecx
 push dword ptr ss:[ebp-4]
 push dword ptr ss:[ebp-20]
 push eax
 call esi
 push ragnar_locker.13485C8 ; 13485C8:"****************************************************************************"
 push ragnar_locker.134861C ; 134861C:"---RAGNAR SECRET---"
 push edi ; edi:"QWZjYOQxRTk2MWU4RTIw[redacted]ZEVhNw=="
 push ragnar_locker.134861C ; 134861C:"---RAGNAR SECRET---"
 push ragnar_locker.13485C8 ; 13485C8:"****************************************************************************"
 lea eax,dword ptr ss:[ebp-228]
 push ragnar_locker.1348630 ; 1348630:"\r\n%s\r\n\r\n%s\r\n%s\r\n%s\r\n\r\n%s\r\n"
 push eax
 call dword ptr ds:[<&wsprintfA>]
```

***Figure 7:** Ransom note file and parts of “Ragnar Secret key” redacted.*

In order to encrypt the files, the malware gets and decodes the ransom note from the **.keys** sections, the public key and some configs.

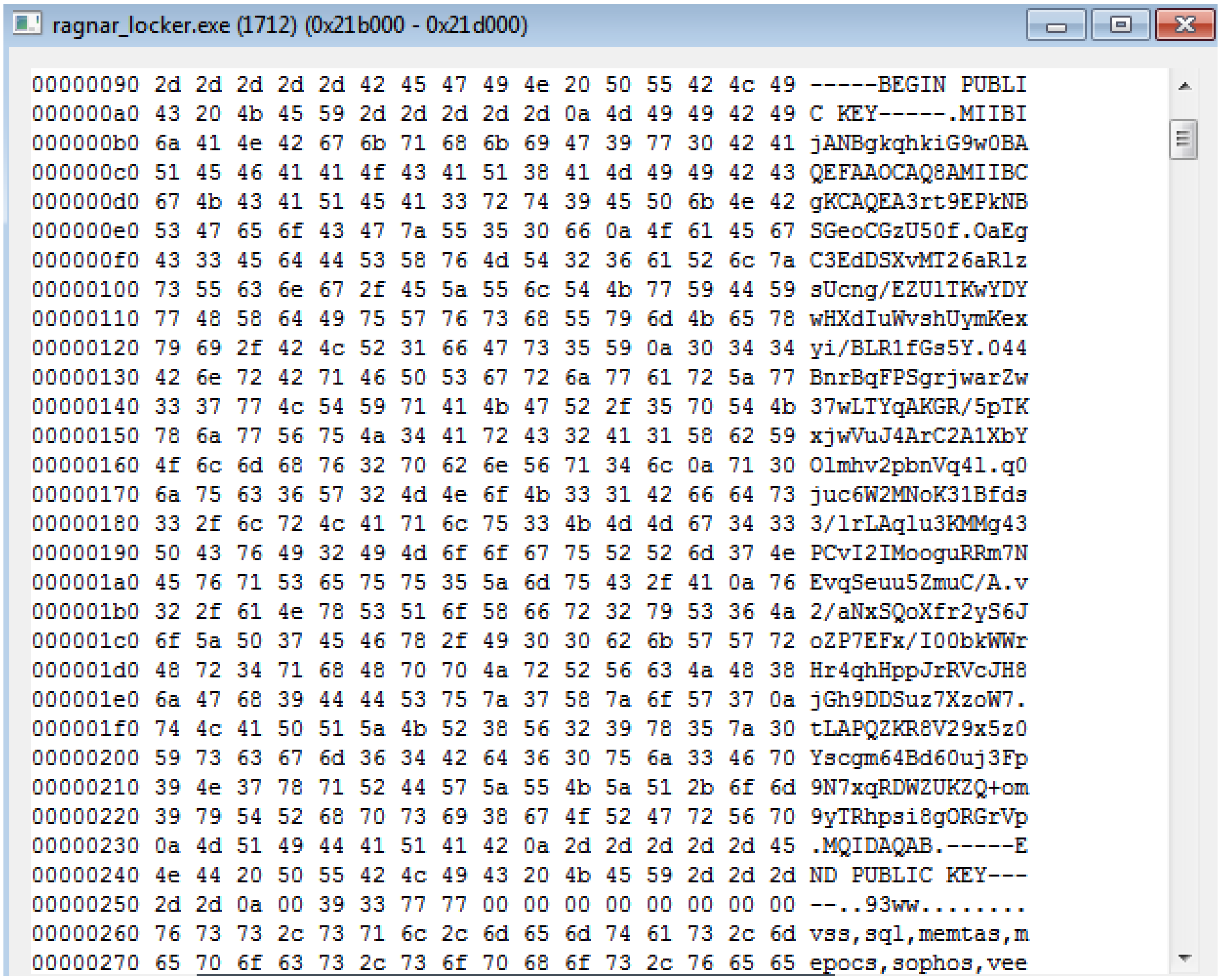


.text	000066AF	00001000	00006800	00000400	00000000	00000000
.rdata	00001318	00008000	00001400	00006C00	00000000	00000000
.data	0000035C	0000A000	00000000	00000000	00000000	00000000
.keys	00001706	0000B000	00001800	00008000	00000000	00000000
.rsrc	000001E0	0000D000	00000200	00009800	00000000	00000000
.reloc	00000290	0000E000	00000400	00009A00	00000000	00000000

```
 Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    Ascii
00000000  72 3D 3C 58 7D 45 76 51 6A 79 68 34 36 6E 5A 25   r=<X}EvQjyh46nZ%
00000010  56 79 46 74 3C 76 5C 25 57 74 2B 6E 55 20 59 30   VyFt<v\%Wt+nU.Y0
00000020  7D 39 39 47 6B 2B 5F 68 61 2E 4B 60 55 45 72 70   }99Gk+_ha.K`UErp
00000030  6A 35 2D 4F 79 4D 63 6E 6A 61 2F 79 2B 24 64 7D   j5-OyMcnja/y+$d}
00000040  00 00 00 00 00 00 00 00 38 BB B5 5A B4 F9 0A BC   ........8»µZ´ù.¼
00000050  84 6E 90 D6 0E 4B 17 EE 03 4F 8D 9A 02 2D B7 63   ▌n Ö▯K▯î▯O ▌ -·c
00000060  80 72 85 9E CC 63 86 32 82 A9 CD 8F 19 1D E5 71   ▌r▌▌Ìc▌2▌©Í ▯  åq
00000070  3B F8 0C C8 06 35 3B 5F AB 83 62 6C 0C C9 8C 76   ;ø▌È▯5;_«▌bl▌É▌v
00000080  AF 5D A1 52 DA B5 36 7C 00 00 00 00 00 00 00 00   ¯]¡RÚµ6|........
00000090  54 F0 FB 14 DD 8A 0A C2 FB 11 D5 BE 1E 3B 6B C5   Tðû▯Ý▌.Âû▯Õ¾ ;kÅ
000000A0  05 2D 83 9C 3A 45 F9 7D EB 67 CD 92 B2 4F A0 49   ▯-▌▌:Eù}ëgÍ´²O I
000000B0  8C DD C1 8F 49 14 F0 2D 67 D2 78 C5 35 34 4F 2C   ▌ÝÁ I▯ð-gÒxÅ54O,
000000C0  CC F5 62 18 7A E4 AB 56 BD 07 82 28 F7 B9 15 08   Ìõb▯zä«V½▯▌(÷¹▯▯
000000D0  4E D0 0E 0C 26 8C 03 EC 80 B4 80 43 E8 B4 A9 ED   NÐ▯▌&▌▯ì▌´▌Cè´©í
000000E0  9A C3 F9 07 46 28 52 11 93 8A FA 05 BB 69 FD 90   ▌Ãù▯F(R▯▌▌ú▯»iý
000000F0  CF A9 94 0E 23 AF D6 31 E0 D7 7B 6E 09 94 8A F3   Ï©▌▯#¯Ö1à×{n.▌▌ó
00000100  B5 86 DC AC 2E 9A 5F 9E 66 EC 8E 1C C4 73 6D 7D   µ▌Ü¬.▌_▌fì▌ Äsm}
00000110  AC 3B 58 6C 3D A7 E9 82 34 94 65 E7 07 F8 CF 3B   ¬;Xl=§é▌4▌eç▯øÏ;
```

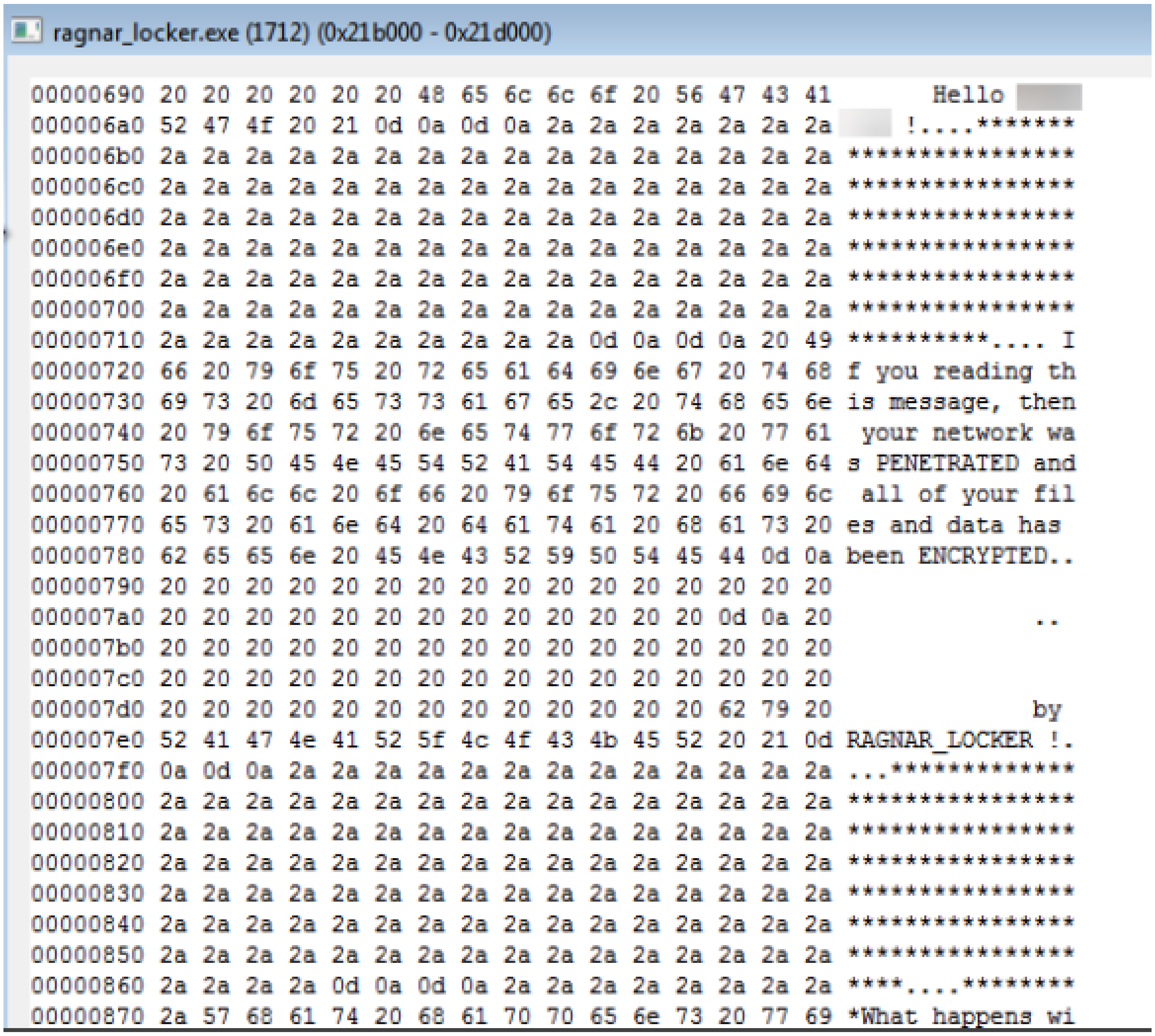
Figure 8: *PE file .keys sections with the ransom note, encryption public key and other configs encoded.*

This section is decoded in runtime and can be observed below.



ragnar_locker.exe (1712) (0x21b000 - 0x21d000)

```
00000090 2d 2d 2d 2d 2d 42 45 47 49 4e 20 50 55 42 4c 49 -----BEGIN PUBLI
000000a0 43 20 4b 45 59 2d 2d 2d 2d 2d 0a 4d 49 49 42 49 C KEY-----.MIIBI
000000b0 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 jANBgkqhkiG9w0BA
000000c0 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 QEFAAOCAQ8AMIIBC
000000d0 67 4b 43 41 51 45 41 33 72 74 39 45 50 6b 4e 42 gKCAQEA3rt9EPkNB
000000e0 53 47 65 6f 43 47 7a 55 35 30 66 0a 4f 61 45 67 SGeoCGzU50f.OaEg
000000f0 43 33 45 64 44 53 58 76 4d 54 32 36 61 52 6c 7a C3EdDSXvMT26aRlz
00000100 73 55 63 6e 67 2f 45 5a 55 6c 54 4b 77 59 44 59 sUcng/EZUlTKwYDY
00000110 77 48 58 64 49 75 57 76 73 68 55 79 6d 4b 65 78 wHXdIuWvshUymKex
00000120 79 69 2f 42 4c 52 31 66 47 73 35 59 0a 30 34 34 yi/BLR1fGs5Y.044
00000130 42 6e 72 42 71 46 50 53 67 72 6a 77 61 72 5a 77 BnrBqFPSgrjwarZw
00000140 33 37 77 4c 54 59 71 41 4b 47 52 2f 35 70 54 4b 37wLTYqAKGR/5pTK
00000150 78 6a 77 56 75 4a 34 41 72 43 32 41 31 58 62 59 xjwVuJ4ArC2A1XbY
00000160 4f 6c 6d 68 76 32 70 62 6e 56 71 34 6c 0a 71 30 Olmhv2pbnVq4l.q0
00000170 6a 75 63 36 57 32 4d 4e 6f 4b 33 31 42 66 64 73 juc6W2MNoK31Bfds
00000180 33 2f 6c 72 4c 41 71 6c 75 33 4b 4d 4d 67 34 33 3/lrLAqlu3KMMg43
00000190 50 43 76 49 32 49 4d 6f 6f 67 75 52 52 6d 37 4e PCvI2IMooguRRm7N
000001a0 45 76 71 53 65 75 75 35 5a 6d 75 43 2f 41 0a 76 EvqSeuu5ZmuC/A.v
000001b0 32 2f 61 4e 78 53 51 6f 58 66 72 32 79 53 36 4a 2/aNxSQoXfr2yS6J
000001c0 6f 5a 50 37 45 46 78 2f 49 30 30 62 6b 57 57 72 oZP7EFx/I00bkWWr
000001d0 48 72 34 71 68 48 70 70 4a 72 52 56 63 4a 48 38 Hr4qhHppJrRVcJH8
000001e0 6a 47 68 39 44 44 53 75 7a 37 58 7a 6f 57 37 0a jGh9DDSuz7XzoW7.
000001f0 74 4c 41 50 51 5a 4b 52 38 56 32 39 78 35 7a 30 tLAPQZKR8V29x5z0
00000200 59 73 63 67 6d 36 34 42 64 36 30 75 6a 33 46 70 Yscgm64Bd60uj3Fp
00000210 39 4e 37 78 71 52 44 57 5a 55 4b 5a 51 2b 6f 6d 9N7xqRDWZUKZQ+om
00000220 39 79 54 52 68 70 73 69 38 67 4f 52 47 72 56 70 9yTRhpsi8gORGrVp
00000230 0a 4d 51 49 44 41 51 41 42 0a 2d 2d 2d 2d 2d 45 .MQIDAQAB.-----E
00000240 4e 44 20 50 55 42 4c 49 43 20 4b 45 59 2d 2d 2d ND PUBLIC KEY---
00000250 2d 2d 0a 00 39 33 77 77 00 00 00 00 00 00 00 00 --..93ww........
00000260 76 73 73 2c 73 71 6c 2c 6d 65 6d 74 61 73 2c 6d vss,sql,memtas,m
00000270 65 70 6f 63 73 2c 73 6f 70 68 6f 73 2c 76 65 65 epocs,sophos,vee
```

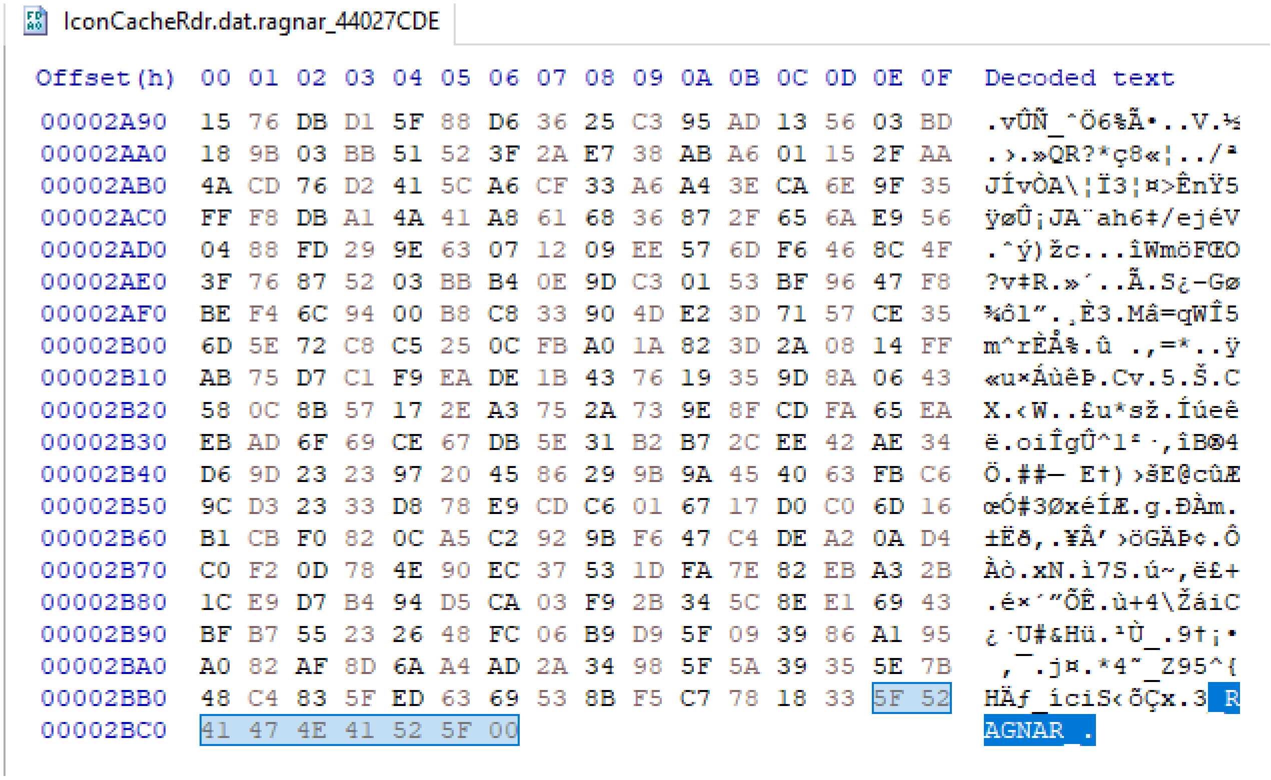


ragnar_locker.exe (1712) (0x21b000 - 0x21d000)

```
00000690 20 20 20 20 20 20 48 65 6c 6c 6f 20 56 47 43 41       Hello [redacted]
000006a0 52 47 4f 20 21 0d 0a 0d 0a 2a 2a 2a 2a 2a 2a 2a [redacted] !....*******
000006b0 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
000006c0 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
000006d0 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
000006e0 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
000006f0 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000700 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000710 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 0d 0a 20 49 **********.... I
00000720 66 20 79 6f 75 20 72 65 61 64 69 6e 67 20 74 68 f you reading th
00000730 69 73 20 6d 65 73 73 61 67 65 2c 20 74 68 65 6e is message, then
00000740 20 79 6f 75 72 20 6e 65 74 77 6f 72 6b 20 77 61  your network wa
00000750 73 20 50 45 4e 45 54 52 41 54 45 44 20 61 6e 64 s PENETRATED and
00000760 20 61 6c 6c 20 6f 66 20 79 6f 75 72 20 66 69 6c  all of your fil
00000770 65 73 20 61 6e 64 20 64 61 74 61 20 68 61 73 20 es and data has
00000780 62 65 65 6e 20 45 4e 43 52 59 50 54 45 44 0d 0a been ENCRYPTED..
00000790 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000007a0 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 20              ..
000007b0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000007c0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000007d0 20 20 20 20 20 20 20 20 20 20 20 20 20 62 79 20              by
000007e0 52 41 47 4e 41 52 5f 4c 4f 43 4b 45 52 20 21 0d RAGNAR_LOCKER !.
000007f0 0a 0d 0a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ...*************
00000800 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000810 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000820 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000830 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000840 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000850 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ****************
00000860 2a 2a 2a 2a 0d 0a 0d 0a 2a 2a 2a 2a 2a 2a 2a 2a ****....********
00000870 2a 57 68 61 74 20 68 61 70 70 65 6e 73 20 77 69 *What happens wi
```

***Figure 9**: Public key, configs and ransom note decoded during the malware execution.*

When a file is encrypted, the “**RAGNAR**” file marker is also added to the end of each encrypted file.



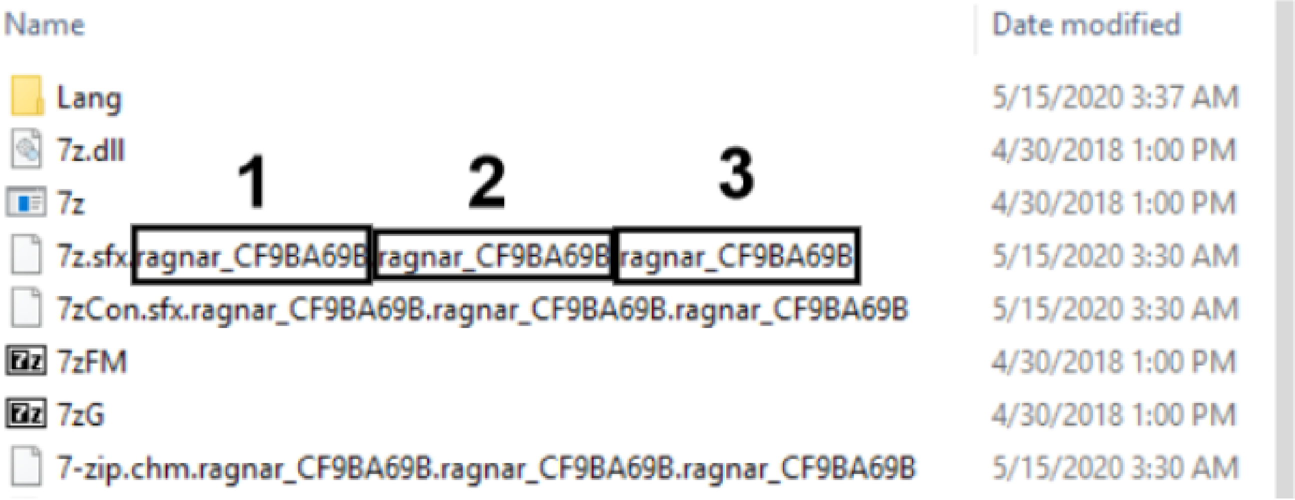
IconCacheRdr.dat.ragnar_44027CDE

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00002A90  15 76 DB D1 5F 88 D6 36 25 C3 95 AD 13 56 03 BD  .vÛÑ_ˆÖ6%Ã•..V.½
00002AA0  18 9B 03 BB 51 52 3F 2A E7 38 AB A6 01 15 2F AA  .›.»QR?*ç8«¦../ª
00002AB0  4A CD 76 D2 41 5C A6 CF 33 A6 A4 3E CA 6E 9F 35  JÍvÒA\¦Ï3¦¤>ÊnŸ5
00002AC0  FF F8 DB A1 4A 41 A8 61 68 36 87 2F 65 6A E9 56  ÿøÛ¡JA¨ah6‡/ejéV
00002AD0  04 88 FD 29 9E 63 07 12 09 EE 57 6D F6 46 8C 4F  .ˆý)žc...îWmöFŒO
00002AE0  3F 76 87 52 03 BB B4 0E 9D C3 01 53 BF 96 47 F8  ?v‡R.»´..Ã.S¿–Gø
00002AF0  BE F4 6C 94 00 B8 C8 33 90 4D E2 3D 71 57 CE 35  ¾ôl”.¸È3.Mâ=qWÎ5
00002B00  6D 5E 72 C8 C5 25 0C FB A0 1A 82 3D 2A 08 14 FF  m^rÈÅ%.û .‚=*..ÿ
00002B10  AB 75 D7 C1 F9 EA DE 1B 43 76 19 35 9D 8A 06 43  «u×ÁùêÞ.Cv.5.Š.C
00002B20  58 0C 8B 57 17 2E A3 75 2A 73 9E 8F CD FA 65 EA  X.‹W..£u*sž.Íúeê
00002B30  EB AD 6F 69 CE 67 DB 5E 31 B2 B7 2C EE 42 AE 34  ë.oiÎgÛ^1²·,îB®4
00002B40  D6 9D 23 23 97 20 45 86 29 9B 9A 45 40 63 FB C6  Ö.##— E†)›šE@cûÆ
00002B50  9C D3 23 33 D8 78 E9 CD C6 01 67 17 D0 C0 6D 16  œÓ#3ØxéÍÆ.g.ÐÀm.
00002B60  B1 CB F0 82 0C A5 C2 92 9B F6 47 C4 DE A2 0A D4  ±Ëð‚.¥Â’›öGÄÞ¢.Ô
00002B70  C0 F2 0D 78 4E 90 EC 37 53 1D FA 7E 82 EB A3 2B  Àò.xN.ì7S.ú~‚ë£+
00002B80  1C E9 D7 B4 94 D5 CA 03 F9 2B 34 5C 8E E1 69 43  .é×´”ÕÊ.ù+4\ŽáiC
00002B90  BF B7 55 23 26 48 FC 06 B9 D9 5F 09 39 86 A1 95  ¿·U#&Hü.¹Ù_.9†¡•
00002BA0  A0 82 AF 8D 6A A4 AD 2A 34 98 5F 5A 39 35 5E 7B   ‚¯.j¤.*4˜_Z95^{
00002BB0  48 C4 83 5F ED 63 69 53 8B F5 C7 78 18 33 5F 52  HÄƒ_íciS‹õÇx.3_R
00002BC0  41 47 4E 41 52 5F 00                             AGNAR_.
```

Figure 10: *“***RAGNAR***” marker appended at the end of the encrypted file.*

This ransomware is not equipped with a mechanism to detect whether the computer has already been compromised. A particularity is that if the malware reaches the same device more than once, it will encrypt the device over and over again. Figure 11 presents this detail, where the files were encrypted three times by Ragnar Locker.



Name	Date modified
Lang	5/15/2020 3:37 AM
7z.dll	4/30/2018 1:00 PM
7z	4/30/2018 1:00 PM
7z.sfx.ragnar_CF9BA69B.ragnar_CF9BA69B.ragnar_CF9BA69B	5/15/2020 3:30 AM
7zCon.sfx.ragnar_CF9BA69B.ragnar_CF9BA69B.ragnar_CF9BA69B	5/15/2020 3:30 AM
7zFM	4/30/2018 1:00 PM
7zG	4/30/2018 1:00 PM
7-zip.chm.ragnar_CF9BA69B.ragnar_CF9BA69B.ragnar_CF9BA69B	5/15/2020 3:30 AM

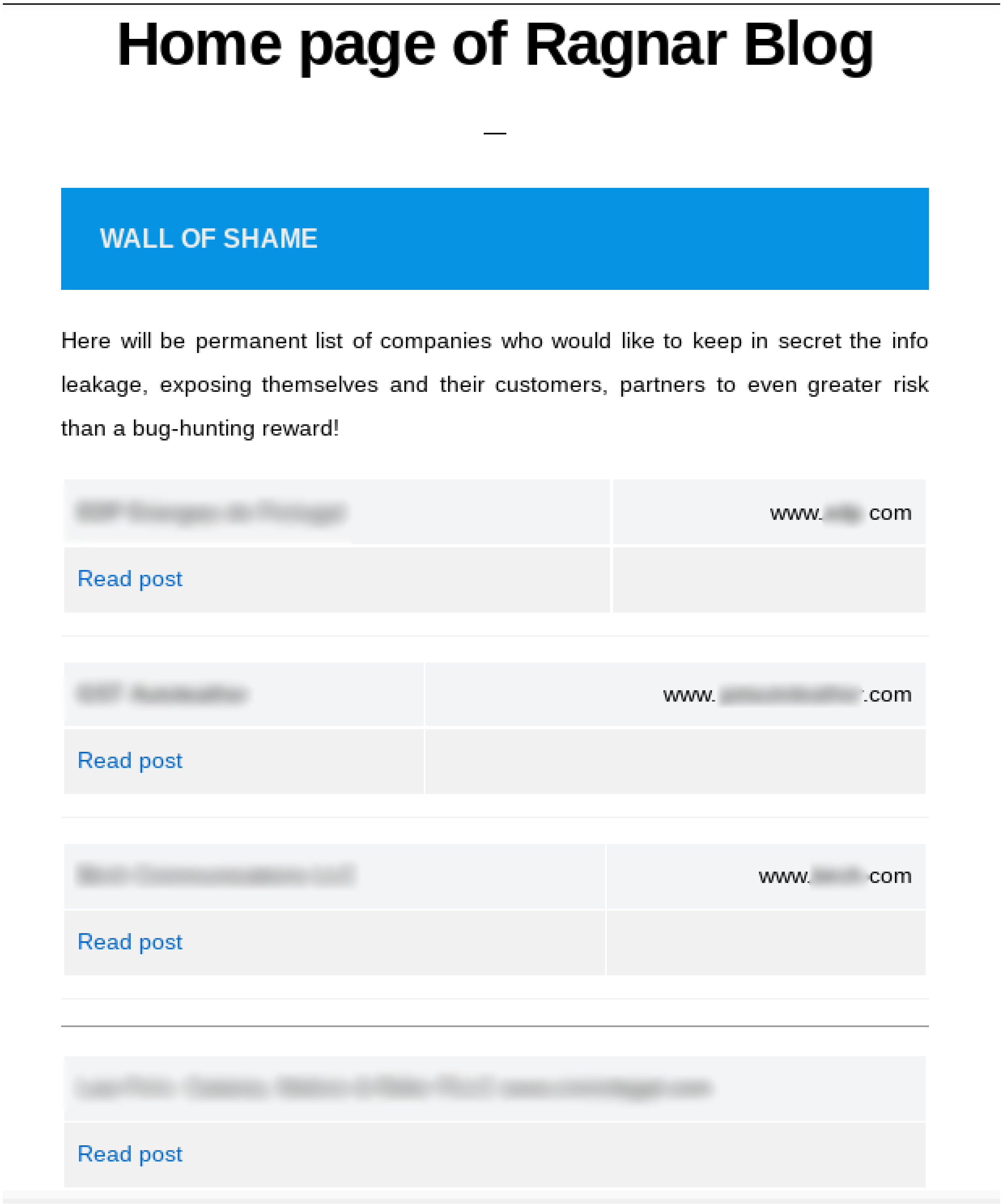
Figure 11: *The same device compromised three times by Ragnar Locker.*

Ragnar Locker and other mediatic ransomwares use several techniques and commands to damage the Windows shadow copies. With this process in place, repairing potential data encryption attacks is harder.

```
vssadmin delete shadows /all /quiet
wmic.exe shadowcopy delete
```

Ragnar blog, ransom page and chat

Proof-of-Concept (PoC) files and images are published on the group blog on the dark web (Figure 1 — label 4) after a compromise.



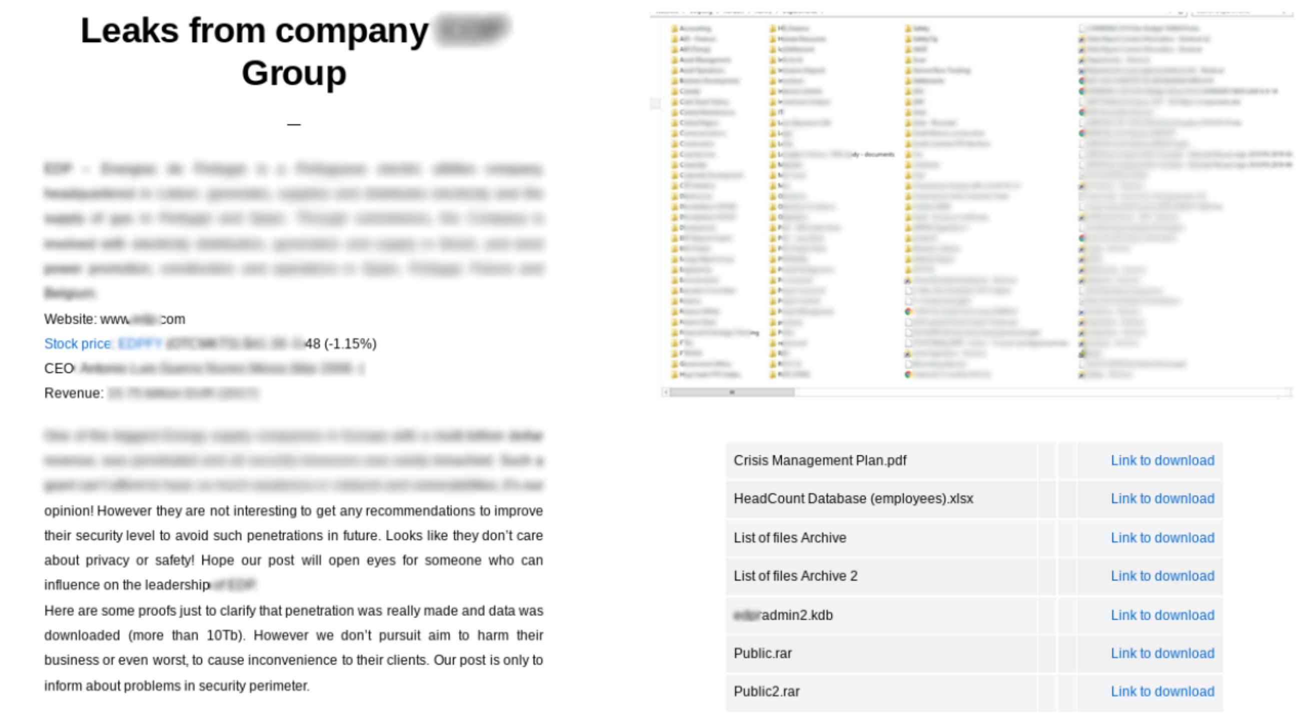
Home page of Ragnar Blog

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

[redacted]	www.[redacted].com
Read post	
[redacted]	www.[redacted].com
Read post	
[redacted]	www.[redacted].com
Read post	
[redacted]	
Read post	

Figure 12: *Ragnar Locker blog available on the dark web.*



Leaks from company [redacted] Group

–

[redacted]

Website: www.[redacted].com

Stock price: [redacted]48 (-1.15%)

CEO: [redacted]

Revenue: [redacted]

[redacted] opinion! However they are not interesting to get any recommendations to improve their security level to avoid such penetrations in future. Looks like they don't care about privacy or safety! Hope our post will open eyes for someone who can influence on the leadership [redacted]

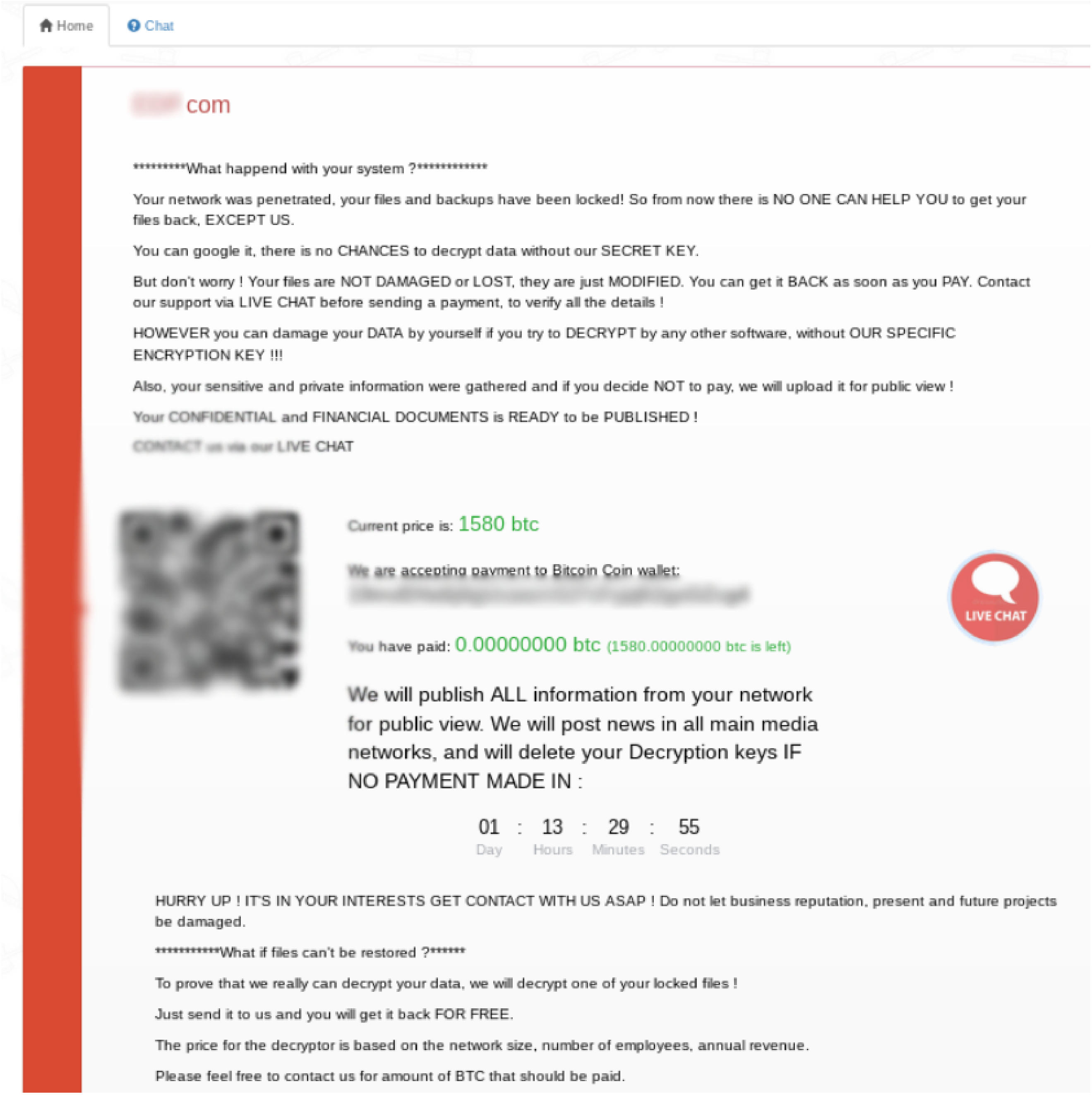
Here are some proofs just to clarify that penetration was really made and data was downloaded (more than 10Tb). However we don't pursuit aim to harm their business or even worst, to cause inconvenience to their clients. Our post is only to inform about problems in security perimeter.

[redacted]

Crisis Management Plan.pdf		Link to download
HeadCount Database (employees).xlsx		Link to download
List of files Archive		Link to download
List of files Archive 2		Link to download
[redacted]admin2.kdb		Link to download
Public.rar		Link to download
Public2.rar		Link to download

Figure 13: *A leak of a specific group compromised by Ragnar Locker operators in mid-April 2020.*

Inside the malware is hardcoded a link to a page with a countdown and the process to pay the ransom.



[redacted] com

*********What happend with your system ?************

Your network was penetrated, your files and backups have been locked! So from now there is NO ONE CAN HELP YOU to get your files back, EXCEPT US.

You can google it, there is no CHANCES to decrypt data without our SECRET KEY.

But don't worry ! Your files are NOT DAMAGED or LOST, they are just MODIFIED. You can get it BACK as soon as you PAY. Contact our support via LIVE CHAT before sending a payment, to verify all the details !

HOWEVER you can damage your DATA by yourself if you try to DECRYPT by any other software, without OUR SPECIFIC ENCRYPTION KEY !!!

Also, your sensitive and private information were gathered and if you decide NOT to pay, we will upload it for public view !

Your CONFIDENTIAL and FINANCIAL DOCUMENTS is READY to be PUBLISHED !

CONTACT us via our LIVE CHAT

Current price is: 1580 btc

We are accepting payment to Bitcoin Coin wallet:
[redacted]

You have paid: 0.00000000 btc (1580.00000000 btc is left)

We will publish ALL information from your network for public view. We will post news in all main media networks, and will delete your Decryption keys IF NO PAYMENT MADE IN :

01 : 13 : 29 : 55
Day Hours Minutes Seconds

HURRY UP ! IT'S IN YOUR INTERESTS GET CONTACT WITH US ASAP ! Do not let business reputation, present and future projects be damaged.

************What if files can't be restored ?******

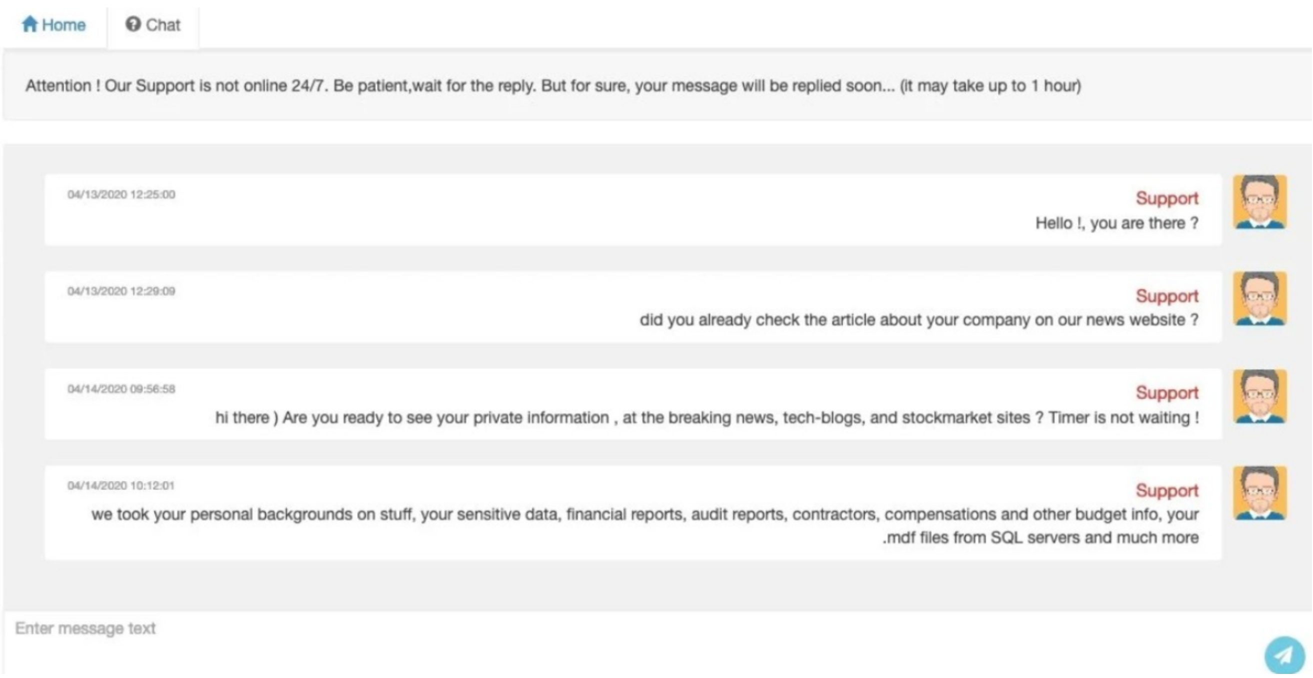
To prove that we really can decrypt your data, we will decrypt one of your locked files !

Just send it to us and you will get it back FOR FREE.

The price for the decryptor is based on the network size, number of employees, annual revenue.

Please feel free to contact us for amount of BTC that should be paid.

Figure 14: *Countdown page with the bitcoin wallet and chat button.*



Attention ! Our Support is not online 24/7. Be patient,wait for the reply. But for sure, your message will be replied soon... (it may take up to 1 hour)

04/13/2020 12:25:00
Support
Hello !, you are there ?

04/13/2020 12:29:09
Support
did you already check the article about your company on our news website ?

04/14/2020 09:56:58
Support
hi there) Are you ready to see your private information , at the breaking news, tech-blogs, and stockmarket sites ? Timer is not waiting !

04/14/2020 10:12:01
Support
we took your personal backgrounds on stuff, your sensitive data, financial reports, audit reports, contractors, compensations and other budget info, your .mdf files from SQL servers and much more

Figure 15: *Chat used to perform communications between ransomware operators and victims.*

Prevention measures

We are living in an era where ransomware continues to grow, and the number of attacks has increased especially during the COVID-19 pandemic. There is no magic solution to prevent attacks of this nature, however, there is a set of good practices that can be applied in order to minimize the impact of data encryption attack.

- The use of an antivirus is mandatory. This software should be regularly updated
- Patch updates regularly and update all the software including operating systems, network devices, applications, mobile phones and other software if applicable
- Maintain a proper backup and restore mechanism and made it mandatory
- Regularly test the recovery function of backup and restore procedures and also test the data integrity of backups
- Conduct simulated ransomware preparedness tests. This is a rule of thumb to check the response of your ecosystem against these kinds of attacks
- If you use Microsoft Office, install Microsoft Office viewers and always keep macros disabled by default
- Limit access to mapped drives whenever possible and keep file sharing disabled by default. In general, ransomware looks into shared drives and encrypts files available on the network
- Don’t enable remote services. The organizations with RDP, VPN, proxies and servers are to be provided with better IT security standards.

The article was initially published by Pedro Tavares on resources.infosecinstitute.com.

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.