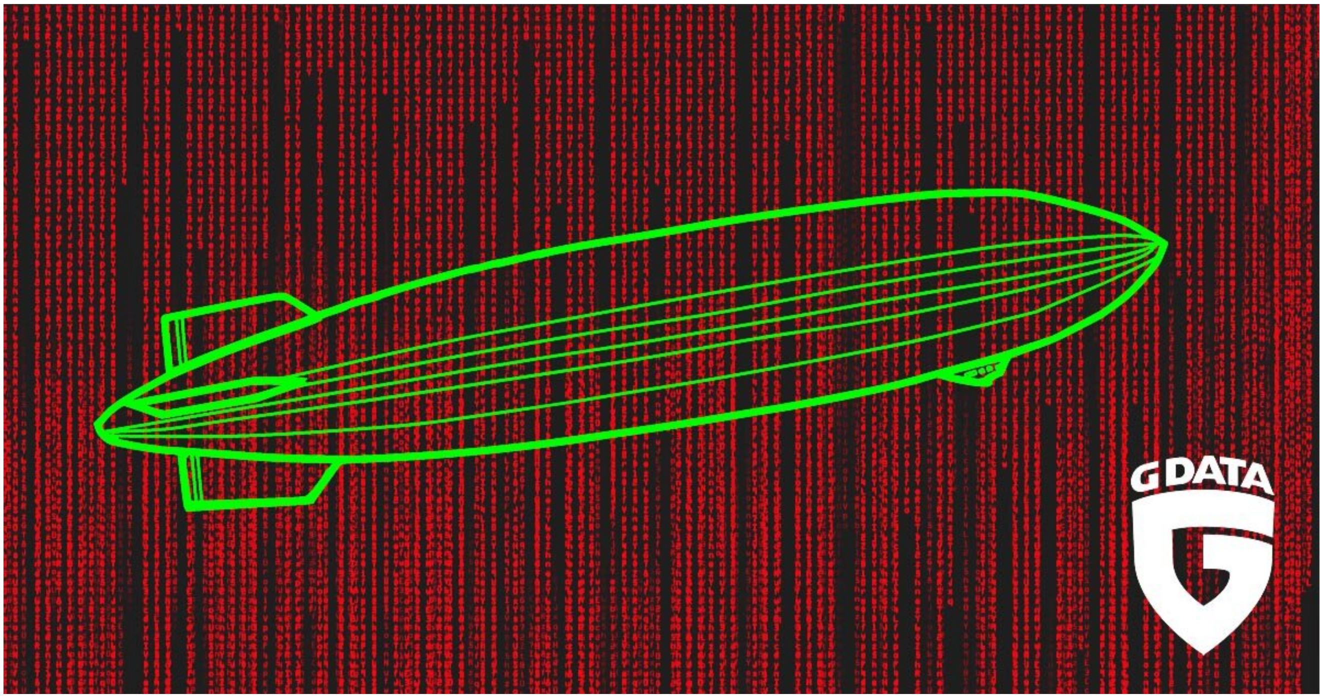
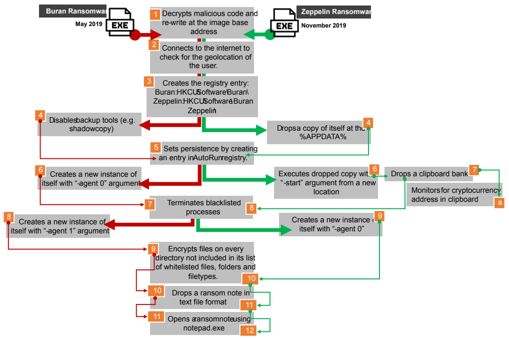
Ransomware on the Rise: Buran’s transformation into Zeppelin

gdatasoftware.com/blog/2020/06/35946-burans-transformation-into-zeppelin



Ransomware is still evolving. Evidence for this can be seen every day. Our analysts have taken a look at Buran and Zeppelin, a particularly devastating exhibit of this evolution.

Ransomware made a strong comeback in 2019 after its hiatus in 2018. Many high-profile attacks were reported by the end of 2019[1]. According to Emsisoft, in U.S. alone, the victims of ransomware include at least 113 government agencies, 89 educational establishments and 764 healthcare providers. The total amount of ransom demands tallies over $7.5 billion .[2]. In a report by Coveware, the average cost of ransom payment increased by 104% from third to fourth quarter of 2019[3]. It is therefore hardly surprising that cybercriminals are enticed once again into developing and creating new ransomware variants. Amongst the prevalent ransomware last year was the Buran ransomware that emerged early May 2019 and continues to proliferate until now. In a matter of just 9 months, this ransomware released over 5 updates by changing its code and attack vectors in order to stay stealthy and cause more damage. By the end of last year, a new variant of ransomware known as Zeppelin was released. Upon initial analysis of Zeppelin, certain behaviors and parts of its source code have been found to have similarities with Buran. This led us to identify Zeppelin as a new variant of Buran.


Buran Ransomwar
May 2019
EXE
Zeppelin Ransomwar
November 2019
EXE
1 Decrypts malicious code and re-write at the image base address
2 Connects to the internet to check for the geolocation of the user.
3 Creates the registry entry: Buran:HKCU\Software\Buran\ Zeppelin:HKCU\Software\Buran Zeppelin\
4 Disables backup tools (e.g. shadowcopy)
4 Dropsa copy of itself at the %APPDATA%
5 Sets persistence by creating an entry in AutoRun registry.
6 Creates a new instance of itself with "-agent 0" argument
6 Executes dropped copy with "-start" argument from a new location
7 Drops a clipboard bank
a Monitors for cryptocurrency address in clipboard
7 Terminates blacklisted processes
8
8 Creates a new instance of itself with "-agent 1" argument
9 Creates a new instance of itself with "-agent 0"
9 Encrypts files on every directory not included in its list of whitelisted files, folders and filetypes.
10
10 Drops a ransom note in text file format
11
11 Opens a ransomnote using notepad.exe
12

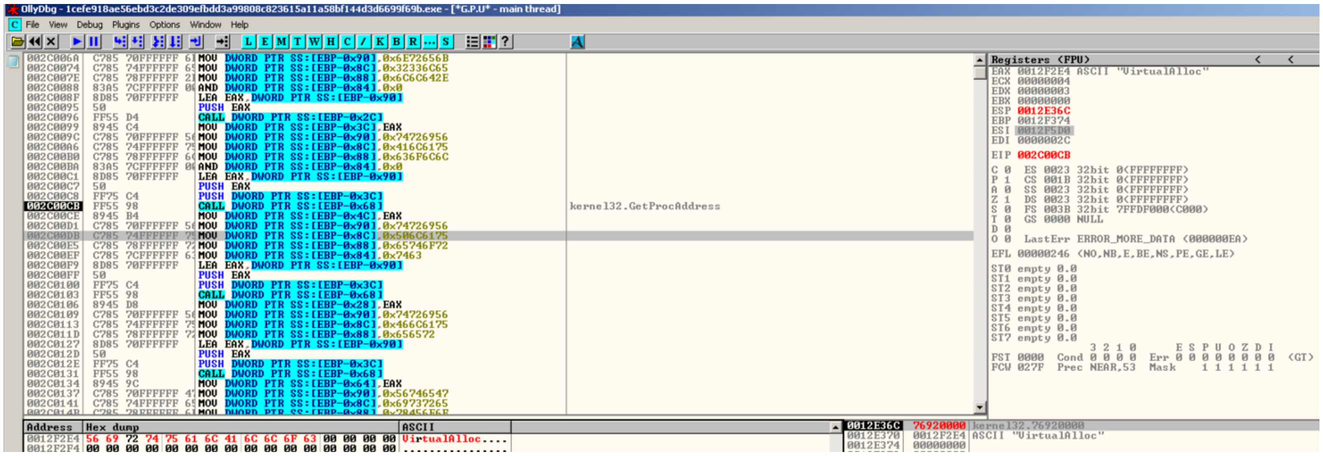
Buran and Zeppelin ransomware Overview

Attack Vector

Zeppelin is reaching its target networks primarily through phishing emails. These emails contain macro-enabled documents that will initiate the download and execution of the ransomware file on the victim's machine. Moreover, other Zeppelin samples were also distributed through malicious advertisements (malvertising) that are designed to trick its victims into clicking fake advertisements which will trigger the download of the malicious file. Lastly, Zeppelin, like other ransomware, utilizes the use of public remote desktop software via web interfaces to remotely control a victim's machine and execute the ransomware.

Installation

Like Buran, Zeppelin will allocate a space in memory. When executed, it will perform its decryption routine. However, compared to Buran's straight forward routine, Zeppelin has some changes to its code. For instance, it now harvests application programming interface(APIs) that it will use later by loading it in the stack. After decrypting, it will re-write the decrypted code to the base address of the file and execute it. It uses this obfuscation technique to make the analysis and signature detection of the file difficult.


OllyDbg - 1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b.exe - [*G.P.U* - main thread]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

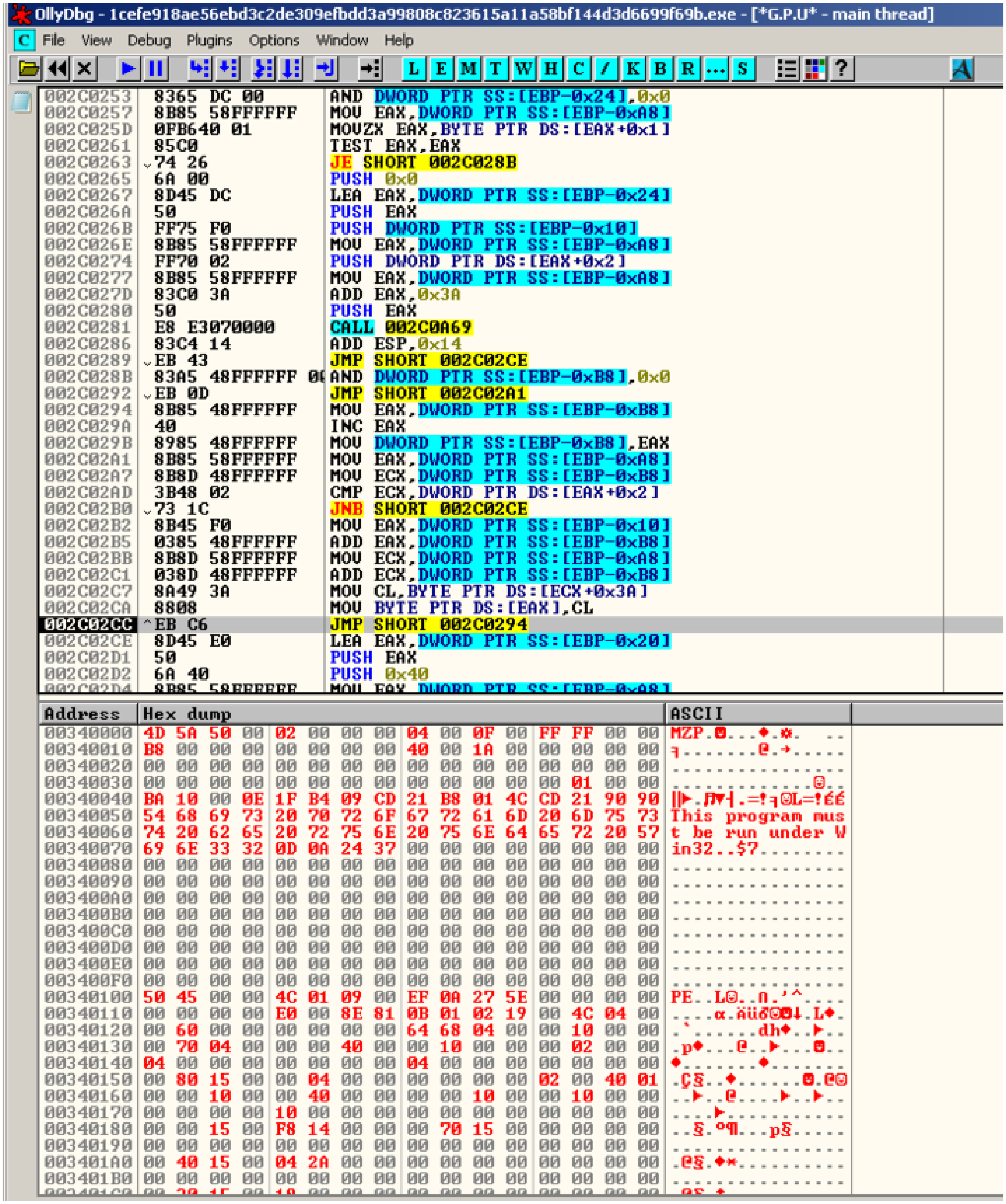
```
002C006A  C785 70FFFFFF 6 MOV DWORD PTR SS:[EBP-0x90],0x6E72656B
002C0074  C785 74FFFFFF 6 MOV DWORD PTR SS:[EBP-0x8C],0x32336C65
002C007E  C785 78FFFFFF 2 MOV DWORD PTR SS:[EBP-0x88],0x6C6C642E
002C0088  83A5 7CFFFFFF 0 AND DWORD PTR SS:[EBP-0x84],0x0
002C008F  8D85 70FFFFFF   LEA EAX,DWORD PTR SS:[EBP-0x90]
002C0095  50              PUSH EAX
002C0096  FF55 D4         CALL DWORD PTR SS:[EBP-0x2C]
002C0099  8945 C4         MOV DWORD PTR SS:[EBP-0x3C],EAX
002C009C  C785 70FFFFFF 5 MOV DWORD PTR SS:[EBP-0x90],0x74726956
002C00A6  C785 74FFFFFF 7 MOV DWORD PTR SS:[EBP-0x8C],0x416C6175
002C00B0  C785 78FFFFFF 6 MOV DWORD PTR SS:[EBP-0x88],0x636F6C6C
002C00BA  83A5 7CFFFFFF 0 AND DWORD PTR SS:[EBP-0x84],0x0
002C00C1  8D85 70FFFFFF   LEA EAX,DWORD PTR SS:[EBP-0x90]
002C00C7  50              PUSH EAX
002C00C8  FF75 C4         PUSH DWORD PTR SS:[EBP-0x3C]
002C00CB  FF55 98         CALL DWORD PTR SS:[EBP-0x68]            kernel32.GetProcAddress
002C00CE  8945 B4         MOV DWORD PTR SS:[EBP-0x4C],EAX
002C00D1  C785 70FFFFFF 5 MOV DWORD PTR SS:[EBP-0x90],0x74726956
002C00DB  C785 74FFFFFF 7 MOV DWORD PTR SS:[EBP-0x8C],0x506C6175
002C00E5  C785 78FFFFFF 7 MOV DWORD PTR SS:[EBP-0x88],0x65746F72
002C00EF  C785 7CFFFFFF 6 MOV DWORD PTR SS:[EBP-0x84],0x7463
002C00F9  8D85 70FFFFFF   LEA EAX,DWORD PTR SS:[EBP-0x90]
002C00FF  50              PUSH EAX
002C0100  FF75 C4         PUSH DWORD PTR SS:[EBP-0x3C]
002C0103  FF55 98         CALL DWORD PTR SS:[EBP-0x68]
002C0106  8945 D8         MOV DWORD PTR SS:[EBP-0x28],EAX
002C0109  C785 70FFFFFF 5 MOV DWORD PTR SS:[EBP-0x90],0x74726956
002C0113  C785 74FFFFFF 7 MOV DWORD PTR SS:[EBP-0x8C],0x466C6175
002C011D  C785 78FFFFFF 7 MOV DWORD PTR SS:[EBP-0x88],0x656572
002C0127  8D85 70FFFFFF   LEA EAX,DWORD PTR SS:[EBP-0x90]
002C012D  50              PUSH EAX
002C012E  FF75 C4         PUSH DWORD PTR SS:[EBP-0x3C]
002C0131  FF55 98         CALL DWORD PTR SS:[EBP-0x68]
002C0134  8945 9C         MOV DWORD PTR SS:[EBP-0x64],EAX
002C0137  C785 70FFFFFF 4 MOV DWORD PTR SS:[EBP-0x90],0x56746547
002C0141  C785 74FFFFFF 6 MOV DWORD PTR SS:[EBP-0x8C],0x69737265
002C014B  C785 78FFFFFF 6 MOV DWORD PTR SS:[EBP-0x88],0x78456E6F
```

```
Registers (FPU)
EAX 0012F2E4 ASCII "VirtualAlloc"
ECX 00000004
EDX 00000003
EBX 00000000
ESP 0012E36C
EBP 0012F374
ESI 0012F5D0
EDI 0000002C

EIP 002C00CB

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(C000)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_MORE_DATA (000000EA)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
                 3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                                         ASCII
0012F2E4 56 69 72 74 75 61 6C 41 6C 6C 6F 63 00 00 00 00 VirtualAlloc....
0012F2F4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
0012E36C  76920000  kernel32.76920000
0012E370  0012F2E4  ASCII "VirtualAlloc"
0012E374  00000000
```

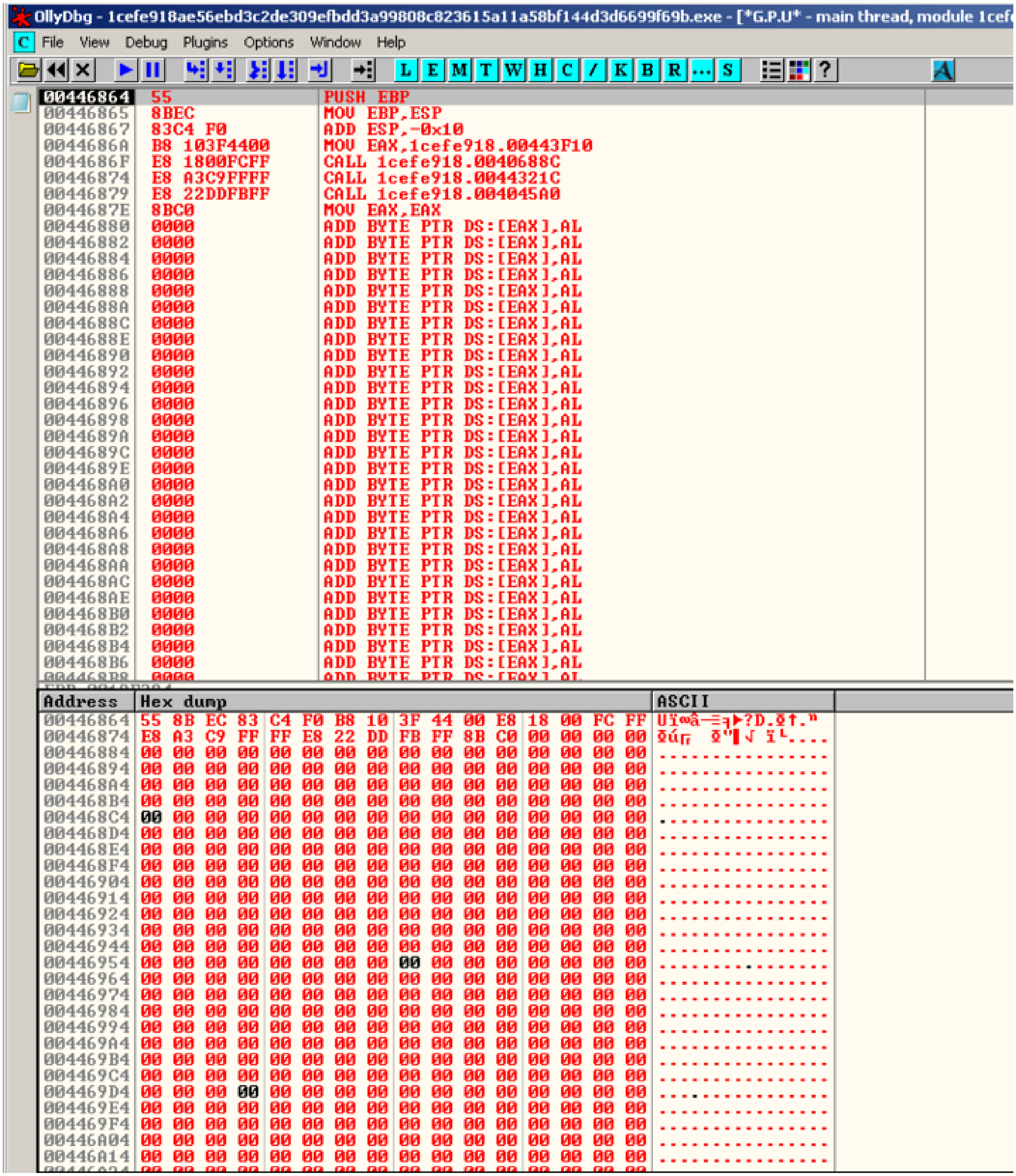
Harvesting of API


OllyDbg - 1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b.exe - [*G.P.U* - main thread]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
002C0253   8365 DC 00         AND DWORD PTR SS:[EBP-0x24],0x0
002C0257   8B85 58FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xA8]
002C025D   0FB640 01          MOVZX EAX,BYTE PTR DS:[EAX+0x1]
002C0261   85C0               TEST EAX,EAX
002C0263  ⌄74 26              JE SHORT 002C028B
002C0265   6A 00              PUSH 0x0
002C0267   8D45 DC            LEA EAX,DWORD PTR SS:[EBP-0x24]
002C026A   50                 PUSH EAX
002C026B   FF75 F0            PUSH DWORD PTR SS:[EBP-0x10]
002C026E   8B85 58FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xA8]
002C0274   FF70 02            PUSH DWORD PTR DS:[EAX+0x2]
002C0277   8B85 58FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xA8]
002C027D   83C0 3A            ADD EAX,0x3A
002C0280   50                 PUSH EAX
002C0281   E8 E3070000        CALL 002C0A69
002C0286   83C4 14            ADD ESP,0x14
002C0289  ⌄EB 43              JMP SHORT 002C02CE
002C028B   83A5 48FFFFFF 0(   AND DWORD PTR SS:[EBP-0xB8],0x0
002C0292  ⌄EB 0D              JMP SHORT 002C02A1
002C0294   8B85 48FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xB8]
002C029A   40                 INC EAX
002C029B   8985 48FFFFFF      MOV DWORD PTR SS:[EBP-0xB8],EAX
002C02A1   8B85 58FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xA8]
002C02A7   8B8D 48FFFFFF      MOV ECX,DWORD PTR SS:[EBP-0xB8]
002C02AD   3B48 02            CMP ECX,DWORD PTR DS:[EAX+0x2]
002C02B0  ⌄73 1C              JNB SHORT 002C02CE
002C02B2   8B45 F0            MOV EAX,DWORD PTR SS:[EBP-0x10]
002C02B5   0385 48FFFFFF      ADD EAX,DWORD PTR SS:[EBP-0xB8]
002C02BB   8B8D 58FFFFFF      MOV ECX,DWORD PTR SS:[EBP-0xA8]
002C02C1   038D 48FFFFFF      ADD ECX,DWORD PTR SS:[EBP-0xB8]
002C02C7   8A49 3A            MOV CL,BYTE PTR DS:[ECX+0x3A]
002C02CA   8808               MOV BYTE PTR DS:[EAX],CL
002C02CC  ^EB C6              JMP SHORT 002C0294
002C02CE   8D45 E0            LEA EAX,DWORD PTR SS:[EBP-0x20]
002C02D1   50                 PUSH EAX
002C02D2   6A 40              PUSH 0x40
002C02D4   8B85 58FFFFFF      MOV EAX,DWORD PTR SS:[EBP-0xA8]
```

```
Address  Hex dump                                         ASCII
00340000 4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00  MZP.☻...♦.☼.  ..
00340010 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00  ╕.......@.→.....
00340020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00340030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  .............☺..
00340040 BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90  ║►.♫▼┤.=!╕☺L=!ÉÉ
00340050 54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73  This program mus
00340060 74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57  t be run under W
00340070 69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00  in32..$7........
00340080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00340090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003400F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00340100 50 45 00 00 4C 01 09 00 EF 0A 27 5E 00 00 00 00  PE..L☺.∩.'^....
00340110 00 00 00 00 E0 00 8E 81 0B 01 02 19 00 4C 04 00  ....α.Äü♂☺☻↓.L♦.
00340120 00 60 00 00 00 00 00 00 64 68 04 00 00 10 00 00  .`......dh♦..►..
00340130 00 70 04 00 00 00 40 00 00 10 00 00 00 02 00 00  .p♦...@..►...☻..
00340140 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ♦.......♦.......
00340150 00 80 15 00 00 04 00 00 00 00 00 00 02 00 40 01  .Ç§..♦......☻.@☺
00340160 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00  ..►..@....►..►..
00340170 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ....►...........
00340180 00 00 15 00 F8 14 00 00 00 70 15 00 00 00 00 00  ..§.°¶...p§.....
00340190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003401A0 00 40 15 00 04 2A 00 00 00 00 00 00 00 00 00 00  .@§.♦*..........
003401B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Jump at the decrypted PE file code

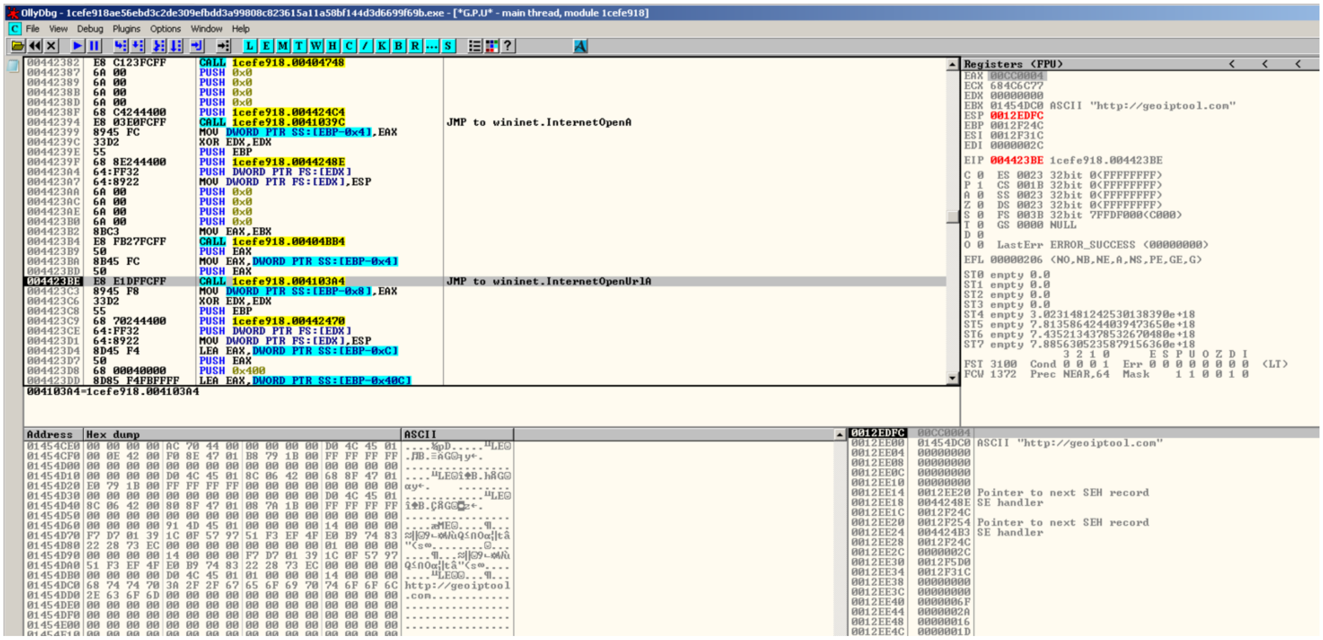


OllyDbg - 1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b.exe - [*G.P.U* - main thread, module 1cef
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
00446864  55            PUSH EBP
00446865  8BEC          MOV EBP,ESP
00446867  83C4 F0       ADD ESP,-0x10
0044686A  B8 103F4400   MOV EAX,1cefe918.00443F10
0044686F  E8 1800FCFF   CALL 1cefe918.0040688C
00446874  E8 A3C9FFFF   CALL 1cefe918.0044321C
00446879  E8 22DDFBFF   CALL 1cefe918.004045A0
0044687E  8BC0          MOV EAX,EAX
00446880  0000          ADD BYTE PTR DS:[EAX],AL
00446882  0000          ADD BYTE PTR DS:[EAX],AL
00446884  0000          ADD BYTE PTR DS:[EAX],AL
00446886  0000          ADD BYTE PTR DS:[EAX],AL
00446888  0000          ADD BYTE PTR DS:[EAX],AL
0044688A  0000          ADD BYTE PTR DS:[EAX],AL
0044688C  0000          ADD BYTE PTR DS:[EAX],AL
0044688E  0000          ADD BYTE PTR DS:[EAX],AL
00446890  0000          ADD BYTE PTR DS:[EAX],AL
00446892  0000          ADD BYTE PTR DS:[EAX],AL
00446894  0000          ADD BYTE PTR DS:[EAX],AL
00446896  0000          ADD BYTE PTR DS:[EAX],AL
00446898  0000          ADD BYTE PTR DS:[EAX],AL
0044689A  0000          ADD BYTE PTR DS:[EAX],AL
0044689C  0000          ADD BYTE PTR DS:[EAX],AL
0044689E  0000          ADD BYTE PTR DS:[EAX],AL
004468A0  0000          ADD BYTE PTR DS:[EAX],AL
004468A2  0000          ADD BYTE PTR DS:[EAX],AL
004468A4  0000          ADD BYTE PTR DS:[EAX],AL
004468A6  0000          ADD BYTE PTR DS:[EAX],AL
004468A8  0000          ADD BYTE PTR DS:[EAX],AL
004468AA  0000          ADD BYTE PTR DS:[EAX],AL
004468AC  0000          ADD BYTE PTR DS:[EAX],AL
004468AE  0000          ADD BYTE PTR DS:[EAX],AL
004468B0  0000          ADD BYTE PTR DS:[EAX],AL
004468B2  0000          ADD BYTE PTR DS:[EAX],AL
004468B4  0000          ADD BYTE PTR DS:[EAX],AL
004468B6  0000          ADD BYTE PTR DS:[EAX],AL
```

```
Address   Hex dump                                         ASCII
00446864  55 8B EC 83 C4 F0 B8 10 3F 44 00 E8 18 00 FC FF  Uï∞â─≡╕▶?D.Φ↑.ⁿ
00446874  E8 A3 C9 FF FF E8 22 DD FB FF 8B C0 00 00 00 00  Φú╔  Φ"▌√ ï└....
00446884  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446894  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468A4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468B4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468C4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468D4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468E4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004468F4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446904  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446914  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446924  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446934  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446944  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446954  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446964  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446974  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446984  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446994  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469A4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469B4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469C4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469D4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469E4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004469F4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446A04  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00446A14  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

The main similarities of Zeppelin with Buran are its several system checks. It will first attempt to connect to the internet to make a query to hxxp://*geoiptool.com.* This isa valid web service that checks the geolocation of a system with the use of an IP address,to verify where the file is currently being executed. If found to be running in either Ukraine, Belarus, Kazakhstan or Russian Federation, it won’t proceed with its infection and terminate instantly. The malware authors did this to make sure that the ransomware won’t infect any user living at the mentioned countries. This could be a hint that the ransomware originated from any of these countries.



OllyDbg - 1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b.exe - [*G.P.U* - main thread, module 1cefe918]

C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

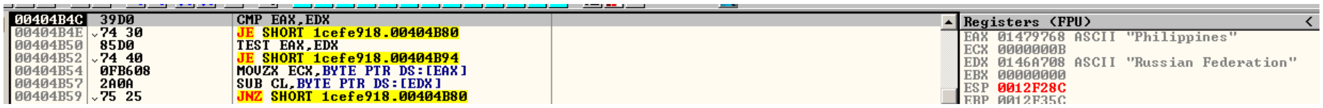
```
00442382  E8 C123FCFF      CALL 1cefe918.00404748
00442387  6A 00            PUSH 0x0
00442389  6A 00            PUSH 0x0
0044238B  6A 00            PUSH 0x0
0044238D  6A 00            PUSH 0x0
0044238F  68 C4244400      PUSH 1cefe918.004424C4
00442394  E8 03E0FCFF      CALL 1cefe918.0041039C               JMP to wininet.InternetOpenA
00442399  8945 FC          MOV DWORD PTR SS:[EBP-0x4],EAX
0044239C  33D2             XOR EDX,EDX
0044239E  55               PUSH EBP
0044239F  68 8E244400      PUSH 1cefe918.0044248E
004423A4  64:FF32          PUSH DWORD PTR FS:[EDX]
004423A7  64:8922          MOV DWORD PTR FS:[EDX],ESP
004423AA  6A 00            PUSH 0x0
004423AC  6A 00            PUSH 0x0
004423AE  6A 00            PUSH 0x0
004423B0  6A 00            PUSH 0x0
004423B2  8BC3             MOV EAX,EBX
004423B4  E8 FB27FCFF      CALL 1cefe918.00404BB4
004423B9  50               PUSH EAX
004423BA  8B45 FC          MOV EAX,DWORD PTR SS:[EBP-0x4]
004423BD  50               PUSH EAX
004423BE  E8 E1DFFCFF      CALL 1cefe918.004103A4               JMP to wininet.InternetOpenUrlA
004423C3  8945 F8          MOV DWORD PTR SS:[EBP-0x8],EAX
004423C6  33D2             XOR EDX,EDX
004423C8  55               PUSH EBP
004423C9  68 70244400      PUSH 1cefe918.00442470
004423CE  64:FF32          PUSH DWORD PTR FS:[EDX]
004423D1  64:8922          MOV DWORD PTR FS:[EDX],ESP
004423D4  8D45 F4          LEA EAX,DWORD PTR SS:[EBP-0xC]
004423D7  50               PUSH EAX
004423D8  68 00040000      PUSH 0x400
004423DD  8D85 F4FBFFFF    LEA EAX,DWORD PTR SS:[EBP-0x40C]
004103A4=1cefe918.004103A4
```

```
Registers (FPU)
EAX 00CC0004
ECX 684C6C77
EDX 00000000
EBX 01454DC0 ASCII "http://geoiptool.com"
ESP 0012EDFC
EBP 0012F24C
ESI 0012F31C
EDI 0000002C

EIP 004423BE 1cefe918.004423BE

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(C000)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 3.0231481242530138390e+18
ST5 empty 7.8135864244039473650e+18
ST6 empty 7.4352134378532670480e+18
ST7 empty 7.8856305235879156360e+18
               3 2 1 0      E S P U O Z D I
FST 3100  Cond 0 0 0 1  Err 0 0 0 0 0 0 0 0  (LT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```

```
Address  Hex dump                                         ASCII
01454CE0 00 00 00 00 AC 70 44 00 00 00 00 00 D0 4C 45 01 ....¼pD.....╨LE☺
01454CF0 00 0E 42 00 F0 8E 47 01 B8 79 1B 00 FF FF FF FF .♫B.≡ÄG☺╕y←.
01454D00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01454D10 00 00 00 00 D0 4C 45 01 8C 06 42 00 68 8F 47 01 ....╨LE☺î♠B.hÅG☺
01454D20 E0 79 1B 00 FF FF FF FF 00 00 00 00 00 00 00 00 αy←.    ........
01454D30 00 00 00 00 00 00 00 00 00 00 00 00 D0 4C 45 01 ............╨LE☺
01454D40 8C 06 42 00 80 8F 47 01 08 7A 1B 00 FF FF FF FF î♠B.ÇÅG☺◘z←.
01454D50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01454D60 00 00 00 00 91 4D 45 01 00 00 00 00 14 00 00 00 ....æME☺....¶...
01454D70 F7 D7 01 39 1C 0F 57 97 51 F3 EF 4F E0 B9 74 83 ≈╫☺9∟☼WùQ≤∩Oα╣tâ
01454D80 22 28 73 EC 00 00 00 00 00 00 00 01 00 00 00 00 "(s∞........☺....
01454D90 00 00 00 00 14 00 00 00 F7 D7 01 39 1C 0F 57 97 ....¶...≈╫☺9∟☼Wù
01454DA0 51 F3 EF 4F E0 B9 74 83 22 28 73 EC 00 00 00 00 Q≤∩Oα╣tâ"(s∞....
01454DB0 00 00 00 00 D0 4C 45 01 01 00 00 00 14 00 00 00 ....╨LE☺☺...¶...
01454DC0 68 74 74 70 3A 2F 2F 67 65 6F 69 70 74 6F 6F 6C http://geoiptool
01454DD0 2E 63 6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 .com............
01454DE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01454DF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01454E00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
0012EDFC  00CC0004
0012EE00  01454DC0  ASCII "http://geoiptool.com"
0012EE04  00000000
0012EE08  00000000
0012EE0C  00000000
0012EE10  00000000
0012EE14  0012EE20  Pointer to next SEH record
0012EE18  0044248E  SE handler
0012EE1C  0012F24C
0012EE20  0012F254  Pointer to next SEH record
0012EE24  004424B3  SE handler
0012EE28  0012F24C
0012EE2C  0000002C
0012EE30  0012F5D0
0012EE34  0012F31C
0012EE38  00000000
0012EE3C  00000000
0012EE40  0000006F
0012EE44  0000002A
0012EE48  00000016
0012EE4C  0000001D
```

Harvesting of API

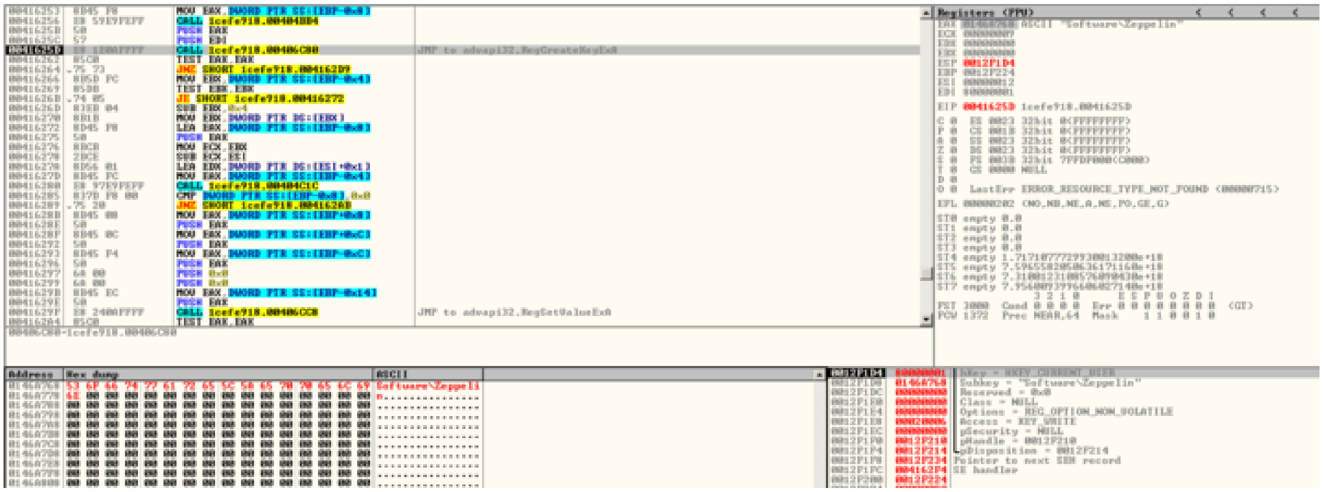


```
00404B4C   39D0        CMP EAX,EDX
00404B4E  ˅74 30       JE SHORT 1cefe918.00404B80
00404B50   85D0        TEST EAX,EDX
00404B52  ˅74 40       JE SHORT 1cefe918.00404B94
00404B54   0FB608      MOVZX ECX,BYTE PTR DS:[EAX]
00404B57   2A0A        SUB CL,BYTE PTR DS:[EDX]
00404B59  ˅75 25       JNZ SHORT 1cefe918.00404B80
```

```
Registers (FPU)
EAX 01479768 ASCII "Philippines"
ECX 0000000B
EDX 0146A708 ASCII "Russian Federation"
EBX 00000000
ESP 0012F28C
EBP 0012F35C
```

Country Protection Check

Zeppelin also creates a registry key that will be used to store data. In the early variants of Zeppelin, it still creates a “Buran” registry key which was later changed to Zeppelin. This is one of the links between Buran and Zeppelin. Compared to Buran, which just creates several instances of itself, Zeppelin drops an executable file inside the %APPDATA% directory with a filename randomly chosen from a list of possible names. To ensure its persistence, it adds an autorun key to the registry that points to the path of the dropped file.



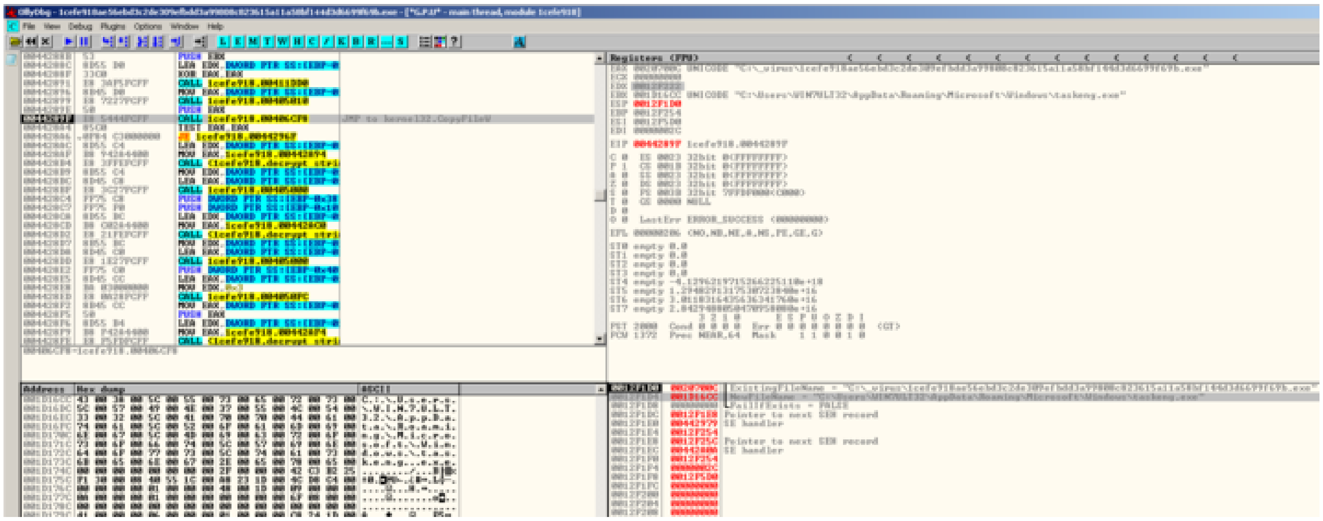
```
CALL 1cefe918.00406C80               JMP to advapi32.RegCreateKeyExA
...
CALL 1cefe918.00406CC8               JMP to advapi32.RegSetValueExA
TEST EAX,EAX
```

```
Registers (FPU)
EAX [illegible] ASCII "Software\Zeppelin"
...
O 0  LastErr ERROR_RESOURCE_TYPE_NOT_FOUND (00000715)
```

```
Address  Hex dump                                         ASCII
[illegible] 53 6F 66 74 77 61 72 65 5C 5A 65 70 70 65 6C 69 Software\Zeppeli
[illegible] 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 n...............
```

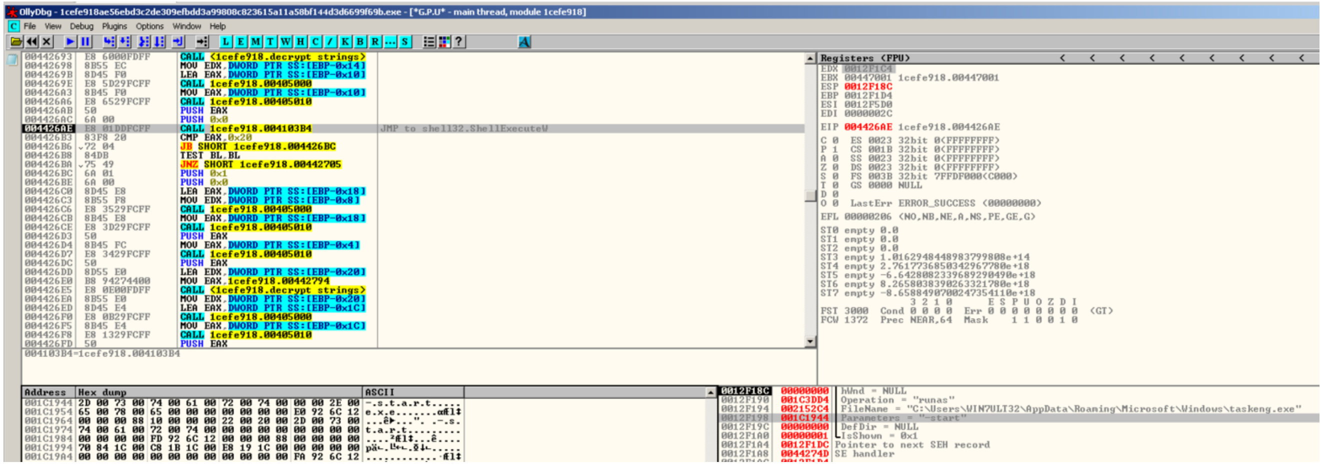
```
hKey = HKEY_CURRENT_USER
Subkey = "Software\Zeppelin"
Reserved = 0x0
Class = NULL
Options = REG_OPTION_NON_VOLATILE
Access = KEY_WRITE
pSecurity = NULL
pHandle = 0012F210
pDisposition = 0012F214
Pointer to next SEH record
SE handler
```

Zeppelin Registry Entry



Creation of a copy of itself in a different location

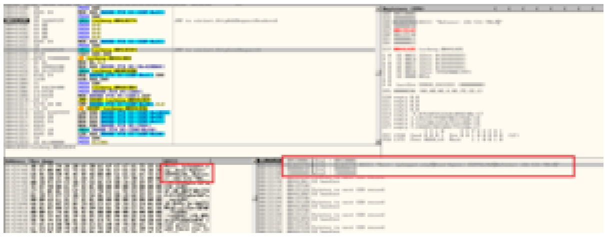
Compared to Buran, which just creates several instances of itself, Zeppelin drops an executable file inside the %APPDATA% directory with a filename randomly chosen from a list of possible names. To ensure its persistence, it adds an autorun key to the registry that points to the path of the dropped file. The dropped file is a copy of itself which will be executed by using the “Shell Execute” API with “-start” argument.



```
OllyDbg - 1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b.exe - [*G.P.U* - main thread, module 1cefe918]

00442693   E8 6000FDFF      CALL <1cefe918.decrypt strings>
00442698   8B55 EC          MOV EDX,DWORD PTR SS:[EBP-0x14]
0044269B   8D45 F0          LEA EAX,DWORD PTR SS:[EBP-0x10]
0044269E   E8 5D29FCFF      CALL 1cefe918.00405000
004426A3   8B45 F0          MOV EAX,DWORD PTR SS:[EBP-0x10]
004426A6   E8 6529FCFF      CALL 1cefe918.00405010
004426AB   50               PUSH EAX
004426AC   6A 00            PUSH 0x0
004426AE   E8 01DDFCFF      CALL 1cefe918.004103B4                JMP to shell32.ShellExecuteW
004426B3   83F8 20          CMP EAX,0x20
004426B6  ^72 04            JB SHORT 1cefe918.004426BC
004426B8   84DB             TEST BL,BL
004426BA  ^75 49            JNZ SHORT 1cefe918.00442705
004426BC   6A 01            PUSH 0x1
004426BE   6A 00            PUSH 0x0
004426C0   8D45 E8          LEA EAX,DWORD PTR SS:[EBP-0x18]
004426C3   8B55 F8          MOV EDX,DWORD PTR SS:[EBP-0x8]
004426C6   E8 3529FCFF      CALL 1cefe918.00405000
004426CB   8B45 E8          MOV EAX,DWORD PTR SS:[EBP-0x18]
004426CE   E8 3D29FCFF      CALL 1cefe918.00405010
004426D3   50               PUSH EAX
004426D4   8B45 FC          MOV EAX,DWORD PTR SS:[EBP-0x4]
004426D7   E8 3429FCFF      CALL 1cefe918.00405010
004426DC   50               PUSH EAX
004426DD   8D55 E0          LEA EDX,DWORD PTR SS:[EBP-0x20]
004426E0   B8 94274400      MOV EAX,1cefe918.00442794
004426E5   E8 0E00FDFF      CALL <1cefe918.decrypt strings>
004426EA   8B55 E0          MOV EDX,DWORD PTR SS:[EBP-0x20]
004426ED   8D45 E4          LEA EAX,DWORD PTR SS:[EBP-0x1C]
004426F0   E8 0B29FCFF      CALL 1cefe918.00405000
004426F5   8B45 E4          MOV EAX,DWORD PTR SS:[EBP-0x1C]
004426F8   E8 1329FCFF      CALL 1cefe918.00405010
004426FD   50               PUSH EAX
004103B4=1cefe918.004103B4

Registers (FPU)
EDX 0012F1C4
EBX 00447001 1cefe918.00447001
ESP 0012F18C
EBP 0012F1D4
ESI 0012F5D0
EDI 0000002C

EIP 004426AE 1cefe918.004426AE

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(C000)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 1.0162948448983799808e+14
ST4 empty 2.7617736850342967780e+18
ST5 empty -6.6428082339689290490e+18
ST6 empty 8.2658038390263321780e+18
ST7 empty -8.6588490700247354110e+18
               3 2 1 0      E S P U O Z D I
FST 3000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0

Address   Hex dump                                         ASCII
001C1944  2D 00 73 00 74 00 61 00 72 00 74 00 00 00 2E 00  -.s.t.a.r.t.....
001C1954  65 00 78 00 65 00 00 00 00 00 00 00 E0 92 6C 12  e.x.e.......αÆl‡
001C1964  00 00 00 88 10 00 00 00 22 00 20 00 2D 00 73 00  ...ê►...". .-.s.
001C1974  74 00 61 00 72 00 74 00 00 00 00 00 00 00 00 00  t.a.r.t.........
001C1984  00 00 00 00 FD 92 6C 12 00 00 00 88 00 00 00 00  ....²Æl‡...ê....
001C1994  70 84 1C 00 C8 1B 1C 00 E8 19 1C 00 00 00 00 00  pä∟.╚←∟.Φ↓∟.....
001C19A4  00 00 00 00 00 00 00 00 00 00 00 00 FA 92 6C 12  ............·Æl‡

0012F18C   00000000  ┌hWnd = NULL
0012F190   001C3DD4  │Operation = "runas"
0012F194   002152C4  │FileName = "C:\Users\WIN7ULT32\AppData\Roaming\Microsoft\Windows\taskeng.exe"
0012F198   001C1944  │Parameters = "-start"
0012F19C   00000000  │DefDir = NULL
0012F1A0   00000001  └IsShown = 0x1
0012F1A4   0012F1DC  Pointer to next SEH record
0012F1A8   0044274D  SE handler
```

Execution of its copy with “-start”

Second Instance

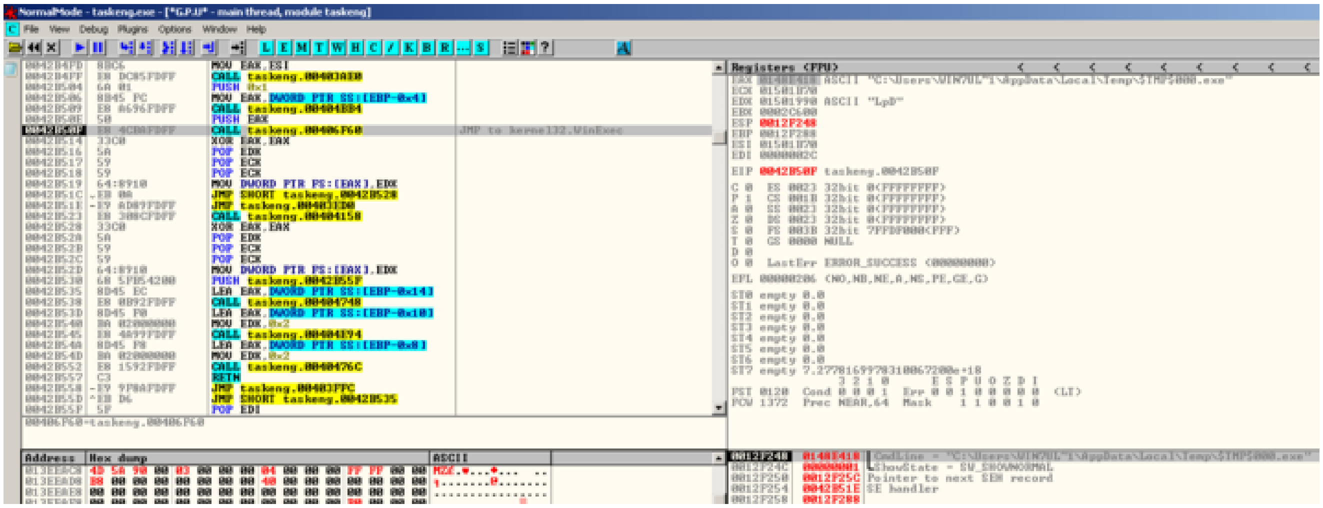


Discovery of victim’s IP address using iplogger.org

Upon execution of the dropped copy, it will decrypt the contents of its ransom note, then store it in an allocated memory space for later use. Meanwhile, it will connect once again to the Internet and make a query to geoiptools.com to recheck where it was executed. After that, it will initiate a connection to iplogger.org, once again a legitimate web service used to track IP addresses, with the user-agent field id set to “ZEPPELIN” and the referrer field containing the unique ID of the victim. The malware author can use the IPLogger service to view the list of victims Zeppelin ransomware has.

The processes running in the victim’s system will be checked against a list of applications associated with monitoring system processes and services, database, backups and web services. If the name of the process can be found in the list, Zeppelin will force terminate the said processes, to ensure that maximum number of important data files will be encrypted.

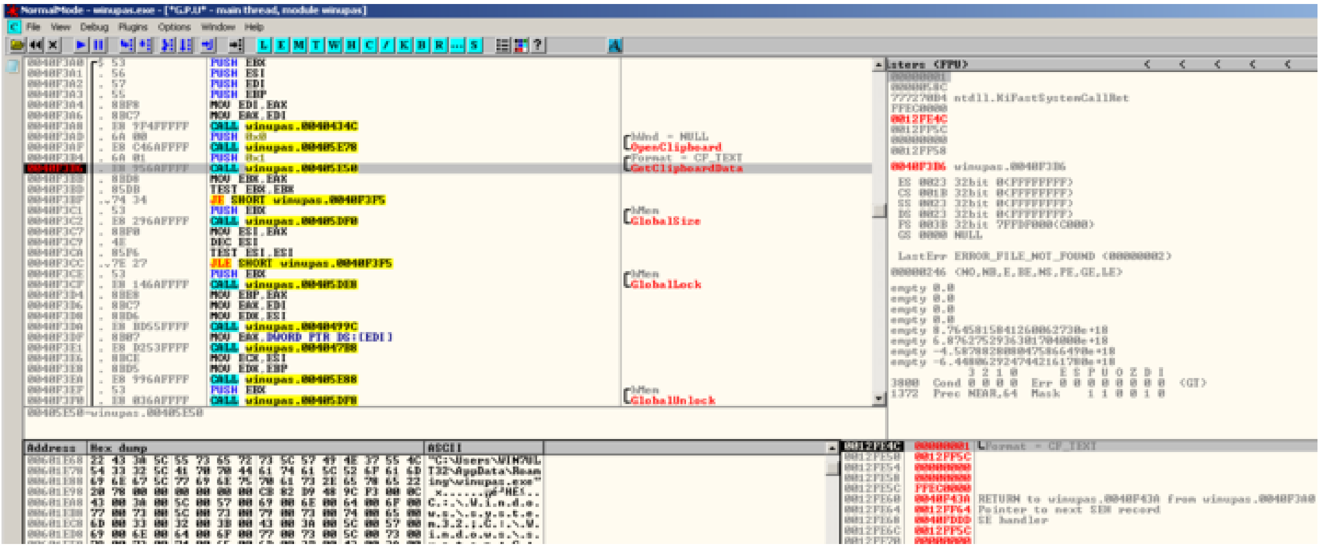
agntsvc.exe
agntsvc.exeagntsvc.exe
agntsvc.exeencsvc.exe
agntsvc.exeisqlplussvc.exe
anvir.exe
anvir64.exe
apache.exe
backup.exe
ccleaner.exe
ccleaner64.exe
dbeng50.exe
dbsnmp.exe
encsvc.exe
far.exe
procexp.exe
regedit.exe
sqbcoreservice.exe
msaccess.exe
msftesql.exe
mspub.exe
mydesktopqos.exe
mydesktopservice.exe
mysqld-nt.exe
mysqld-opt.exe
mysqld.exe
ncsvc.exe
ocautoupds.exe
ocomm.exe
ocssd.exe
oracle.exe
u8.exe
ufida.exe
visio.exe
xfssvccon.exe
sql.exe
sqlagent.exe
sqlbrowser.exe
sqlserver.exe
sqlservr.exe
sqlwriter.exe
synctime.exe
taskkill.exe
tasklist.exe
taskmgr.exe
tbirdconfig.exe
tomcat.exe
tomcat6.exe
firefoxconfig.exe
infopath.exe
isqlplussvc.exe
kingdee.exe



NormalMode - taskeng.exe - [*G.P.U* - main thread, module taskeng]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
0042B4FD   8BC6            MOV EAX,ESI
0042B4FF   E8 DC85FDFF     CALL taskeng.00403AE0
0042B504   6A 01           PUSH 0x1
0042B506   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-0x4]
0042B509   E8 A696FDFF     CALL taskeng.00404BB4
0042B50E   50              PUSH EAX
0042B50F   E8 4C8AFDFF     CALL taskeng.00406F60                 JMP to kernel32.WinExec
0042B514   33C0            XOR EAX,EAX
0042B516   5A              POP EDX
0042B517   59              POP ECX
0042B518   59              POP ECX
0042B519   64:8910         MOV DWORD PTR FS:[EAX],EDX
0042B51C  -EB 0A           JMP SHORT taskeng.0042B528
0042B51E  -E9 AD89FDFF     JMP taskeng.00403ED0
0042B523   E8 308CFDFF     CALL taskeng.00404158
0042B528   33C0            XOR EAX,EAX
0042B52A   5A              POP EDX
0042B52B   59              POP ECX
0042B52C   59              POP ECX
0042B52D   64:8910         MOV DWORD PTR FS:[EAX],EDX
0042B530   68 5FB54200     PUSH taskeng.0042B55F
0042B535   8D45 EC         LEA EAX,DWORD PTR SS:[EBP-0x14]
0042B538   E8 0892FDFF     CALL taskeng.00404748
0042B53D   8D45 F0         LEA EAX,DWORD PTR SS:[EBP-0x10]
0042B540   BA 02000000     MOV EDX,0x2
0042B545   E8 4A99FDFF     CALL taskeng.00404E94
0042B54A   8D45 F8         LEA EAX,DWORD PTR SS:[EBP-0x8]
0042B54D   BA 02000000     MOV EDX,0x2
0042B552   E8 1592FDFF     CALL taskeng.0040476C
0042B557   C3              RETN
0042B558  -E9 9F8AFDFF     JMP taskeng.00403FFC
0042B55D  ^EB D6           JMP SHORT taskeng.0042B535
0042B55F   5F              POP EDI
00406F60=taskeng.00406F60

Registers (FPU)
EAX 0140E410 ASCII "C:\Users\WIN7UL~1\AppData\Local\Temp\$TMP$000.exe"
ECX 01501B70
EDX 01501990 ASCII "LpD"
EBX 0002C600
ESP 0012F248
EBP 0012F288
ESI 01501B70
EDI 0000002C

EIP 0042B50F taskeng.0042B50F

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 7.2778169978310067200e+18
               3 2 1 0      E S P U O Z D I
FST 0120  Cond 0 0 0 1  Err 0 0 1 0 0 0 0 0  (LT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0

Address   Hex dump                                         ASCII
013EEAC8  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZE.♥...♦...  ..
013EEAD8  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ╕.......@.......
013EEAE8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

0012F248  0140E410  CmdLine = "C:\Users\WIN7UL~1\AppData\Local\Temp\$TMP$000.exe"
0012F24C  00000001  ShowState = SW_SHOWNORMAL
0012F250  0012F25C  Pointer to next SEH record
0012F254  0042B51E  SE handler
0012F258  0012F288
```

Drops clipboard banker



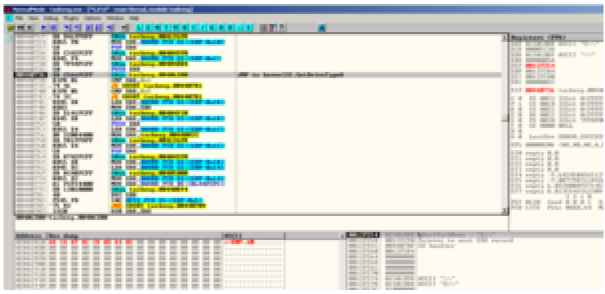
NormalMode - winupas.exe - [*G.P.U* - main thread, module winupas]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
0040F3A0  /$ 53            PUSH EBX
0040F3A1  |. 56            PUSH ESI
0040F3A2  |. 57            PUSH EDI
0040F3A3  |. 55            PUSH EBP
0040F3A4  |. 8BF8          MOV EDI,EAX
0040F3A6  |. 8BC7          MOV EAX,EDI
0040F3A8  |. E8 9F4FFFFF   CALL winupas.0040434C
0040F3AD  |. 6A 00         PUSH 0x0                          ┌hWnd = NULL
0040F3AF  |. E8 C46AFFFF   CALL winupas.00405E78             └OpenClipboard
0040F3B4  |. 6A 01         PUSH 0x1                          ┌Format = CF_TEXT
0040F3B6  |. E8 956AFFFF   CALL winupas.00405E50             └GetClipboardData
0040F3BB  |. 8BD8          MOV EBX,EAX
0040F3BD  |. 85DB          TEST EBX,EBX
0040F3BF  |.v74 34         JE SHORT winupas.0040F3F5
0040F3C1  |. 53            PUSH EBX                          ┌hMem
0040F3C2  |. E8 296AFFFF   CALL winupas.00405DF0             └GlobalSize
0040F3C7  |. 8BF0          MOV ESI,EAX
0040F3C9  |. 4E            DEC ESI
0040F3CA  |. 85F6          TEST ESI,ESI
0040F3CC  |.v7E 27         JLE SHORT winupas.0040F3F5
0040F3CE  |. 53            PUSH EBX                          ┌hMem
0040F3CF  |. E8 146AFFFF   CALL winupas.00405DE8             └GlobalLock
0040F3D4  |. 8BE8          MOV EBP,EAX
0040F3D6  |. 8BC7          MOV EAX,EDI
0040F3D8  |. 8BD6          MOV EDX,ESI
0040F3DA  |. E8 BD55FFFF   CALL winupas.0040499C
0040F3DF  |. 8B07          MOV EAX,DWORD PTR DS:[EDI]
0040F3E1  |. E8 D253FFFF   CALL winupas.004047B8
0040F3E6  |. 8BCE          MOV ECX,ESI
0040F3E8  |. 8BD5          MOV EDX,EBP
0040F3EA  |. E8 996AFFFF   CALL winupas.00405E88
0040F3EF  |. 53            PUSH EBX                          ┌hMem
0040F3F0  |. E8 036AFFFF   CALL winupas.00405DF8             └GlobalUnlock
00405E50=winupas.00405E50

isters (FPU)
00000001
00000F8C
777270B4 ntdll.KiFastSystemCallRet
FFEC0000
0012FE4C
0012FF5C
00000000
0012FF58

0040F3B6 winupas.0040F3B6
 ES 0023 32bit 0(FFFFFFFF)
 CS 001B 32bit 0(FFFFFFFF)
 SS 0023 32bit 0(FFFFFFFF)
 DS 0023 32bit 0(FFFFFFFF)
 FS 003B 32bit 7FFDF000(C000)
 GS 0000 NULL

 LastErr ERROR_FILE_NOT_FOUND (00000002)
00000246 (NO,NB,E,BE,NS,PE,GE,LE)
empty 0.0
empty 0.0
empty 0.0
empty 0.0
empty 8.7645815841260062730e+18
empty 6.8762752936301704000e+18
empty -4.5878828000475866490e+18
empty -6.4480629247442161700e+18
             3 2 1 0      E S P U O Z D I
3800  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
1372  Prec NEAR,64  Mask    1 1 0 0 1 0

Address   Hex dump                                         ASCII
00681E68  22 43 3A 5C 55 73 65 72 73 5C 57 49 4E 37 55 4C  "C:\Users\WIN7UL
00681E78  54 33 32 5C 41 70 70 44 61 74 61 5C 52 6F 61 6D  T32\AppData\Roam
00681E88  69 6E 67 5C 77 69 6E 75 70 61 73 2E 65 78 65 22  ing\winupas.exe"
00681E98  20 78 00 00 00 00 00 00 C8 82 D9 48 9C F3 00 0C   x......╚é┘H£≤..
00681EA8  43 00 3A 00 5C 00 57 00 69 00 6E 00 64 00 6F 00  C.:.\.W.i.n.d.o.
00681EB8  77 00 73 00 5C 00 73 00 79 00 73 00 74 00 65 00  w.s.\.s.y.s.t.e.
00681EC8  6D 00 33 00 32 00 3B 00 43 00 3A 00 5C 00 57 00  m.3.2.;.C.:.\.W.
00681ED8  69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 73 00  i.n.d.o.w.s.\.s.

0012FE4C  00000001  └Format = CF_TEXT
0012FE50  0012FF5C
0012FE54  00000000
0012FE58  00000000
0012FE5C  FFEC0000
0012FE60  0040F43A  RETURN to winupas.0040F43A from winupas.0040F3A0
0012FE64  0012FF64  Pointer to next SEH record
0012FE68  0040FDDD  SE handler
0012FE6C  0012FF5C
```

Monitors clipboard for cryptocurrency address

The second instance of Zeppelin enables the malware author to drop a version of Clipbanker in the %appdata%\local\temp directory and execute it as “winupas.exe”. This clipbanker is responsible for monitoring the system’s clipboard for any strings that matches a cryptocurrency address. If a match is identified, clipbanker will replace the string to that of the malware author’s cryptocurrency address so that any amount of cryptocurrency to be transferred will be redirected to the malware author’s address. After that, Zeppelin will create another instance of itself with “-agent 0” argument.

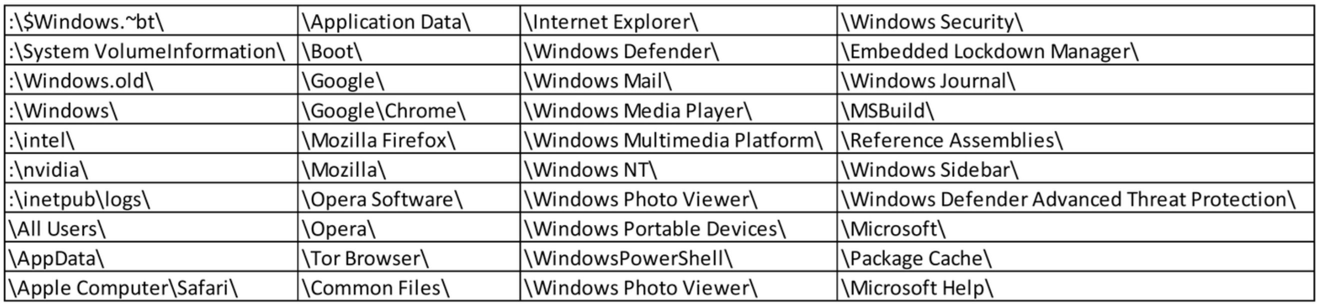
Third instance



Listing of all available drives

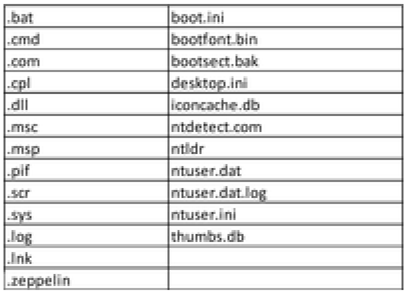
The third instance of Zeppelin is mainly for file encryption. First it will check available drives in the system by iterating drives from Z:\ to A:\. It only looks for certain drive types which are: unknown, removable, fixed, remote and RAM disk drives.

Then, all directories except Windows Operating System-related, Internet browsers and among other folders, will be traversed to encrypt all files in it. These whitelisted folders and its files are avoided to ensure the proper execution of the malware.



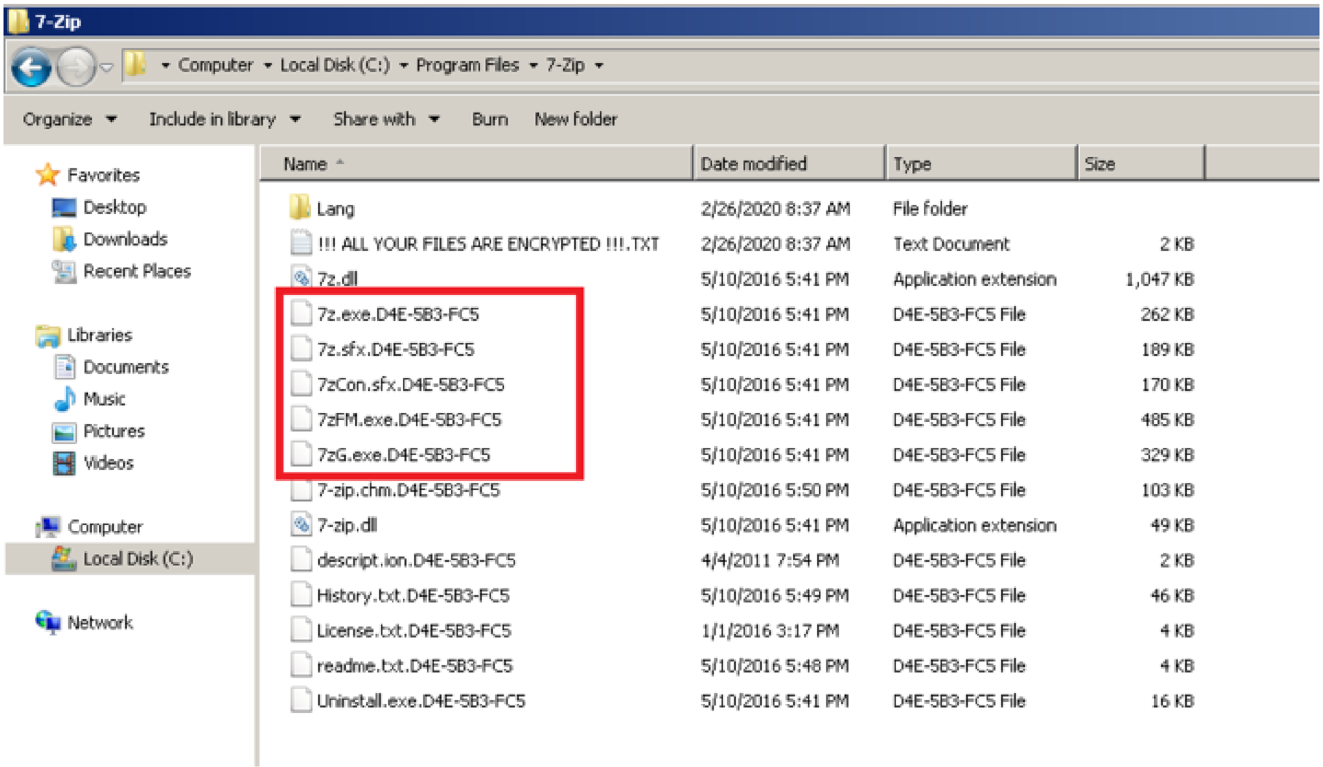
:\$Windows.~bt\	\Application Data\	\Internet Explorer\	\Windows Security\
:\System VolumeInformation\	\Boot\	\Windows Defender\	\Embedded Lockdown Manager\
:\Windows.old\	\Google\	\Windows Mail\	\Windows Journal\
:\Windows\	\Google\Chrome\	\Windows Media Player\	\MSBuild\
:\intel\	\Mozilla Firefox\	\Windows Multimedia Platform\	\Reference Assemblies\
:\nvidia\	\Mozilla\	\Windows NT\	\Windows Sidebar\
:\inetpub\logs\	\Opera Software\	\Windows Photo Viewer\	\Windows Defender Advanced Threat Protection\
\All Users\	\Opera\	\Windows Portable Devices\	\Microsoft\
\AppData\	\Tor Browser\	\WindowsPowerShell\	\Package Cache\
\Apple Computer\Safari\	\Common Files\	\Windows Photo Viewer\	\Microsoft Help\

Whitelisted File Paths



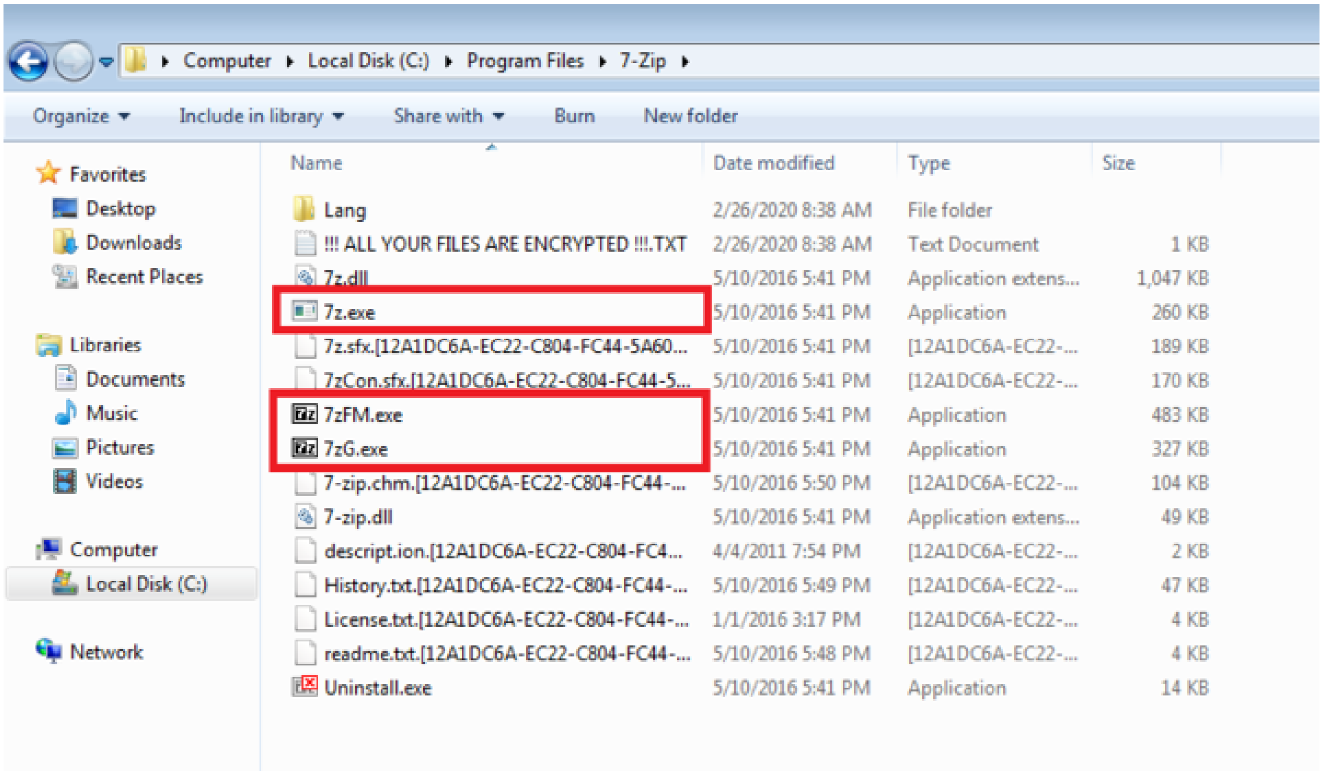
.bat	boot.ini
.cmd	bootfont.bin
.com	bootsect.bak
.cpl	desktop.ini
.dll	iconcache.db
.msc	ntdetect.com
.msp	ntldr
.pif	ntuser.dat
.scr	ntuser.dat.log
.sys	ntuser.ini
.log	thumbs.db
.lnk	
.zeppelin	

One of the evident changes in Zeppelin is that the infection coverage is wider as it infects more filetypes than Buran. For instance, Zeppelin not only infects document files but also executable files with ".exe" extension. This makes Zeppelin more destructive than Buran as it renders the victim's machine pretty much unusable by encrypting all software installed, unless the installation path is included in the whitelisted file paths. Every Zeppelin encrypted file can easily be distinguished by an infection marker "ZEPPELIN" that can be seen at the beginning of the file's content. This infection marker makes it distinct from Buran, but at the same time an indication that they are from the same family as they both leave infection markers at the start of each file using the same encryption routine. After all files in the directory are encrypted, a ransom note in text file format will be dropped. Lastly, it will open a ransom note using notepad.exe to inform the victim of the infection.



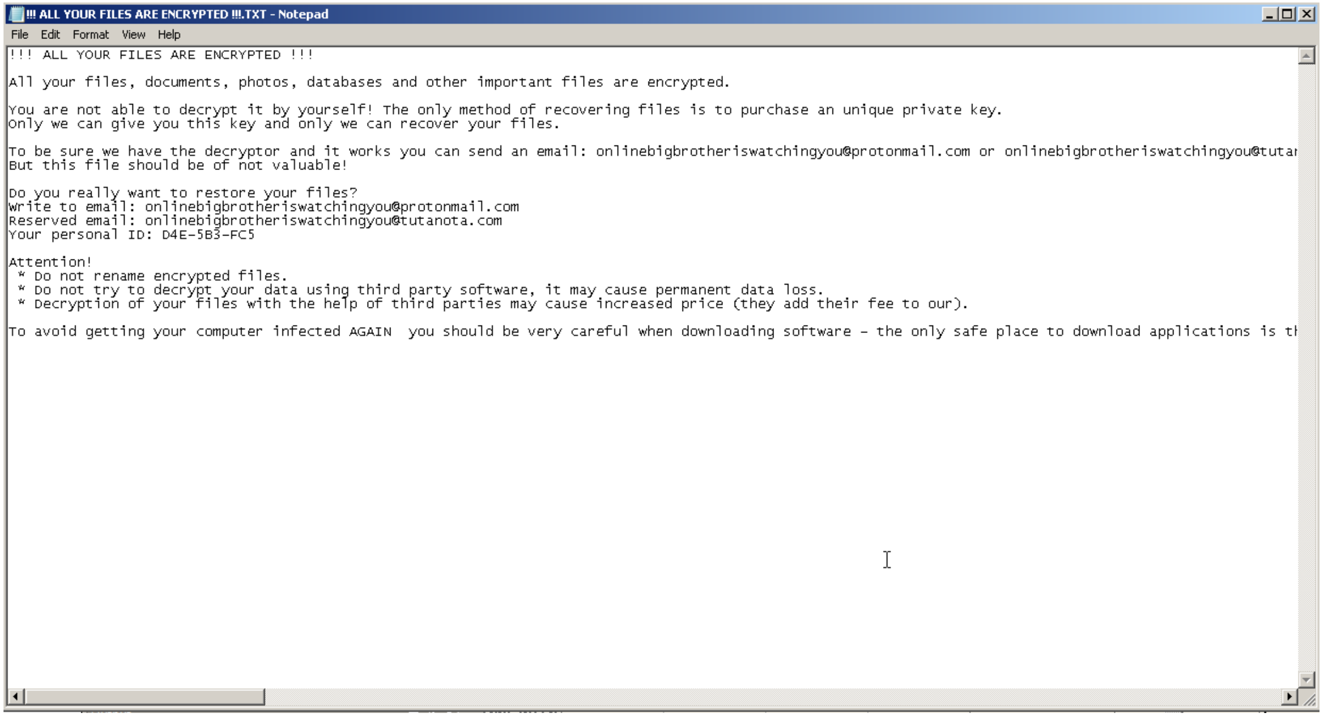
Name	Date modified	Type	Size
Lang	2/26/2020 8:37 AM	File folder	
!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT	2/26/2020 8:37 AM	Text Document	2 KB
7z.dll	5/10/2016 5:41 PM	Application extension	1,047 KB
7z.exe.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	262 KB
7z.sfx.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	189 KB
7zCon.sfx.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	170 KB
7zFM.exe.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	485 KB
7zG.exe.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	329 KB
7-zip.chm.D4E-5B3-FC5	5/10/2016 5:50 PM	D4E-5B3-FC5 File	103 KB
7-zip.dll	5/10/2016 5:41 PM	Application extension	49 KB
descript.ion.D4E-5B3-FC5	4/4/2011 7:54 PM	D4E-5B3-FC5 File	2 KB
History.txt.D4E-5B3-FC5	5/10/2016 5:49 PM	D4E-5B3-FC5 File	46 KB
License.txt.D4E-5B3-FC5	1/1/2016 3:17 PM	D4E-5B3-FC5 File	4 KB
readme.txt.D4E-5B3-FC5	5/10/2016 5:48 PM	D4E-5B3-FC5 File	4 KB
Uninstall.exe.D4E-5B3-FC5	5/10/2016 5:41 PM	D4E-5B3-FC5 File	16 KB

Zeppelin Encryption including .exe files



Name	Date modified	Type	Size
Lang	2/26/2020 8:38 AM	File folder	
!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT	2/26/2020 8:38 AM	Text Document	1 KB
7z.dll	5/10/2016 5:41 PM	Application extens...	1,047 KB
7z.exe	5/10/2016 5:41 PM	Application	260 KB
7z.sfx.[12A1DC6A-EC22-C804-FC44-5A60...	5/10/2016 5:41 PM	[12A1DC6A-EC22-...	189 KB
7zCon.sfx.[12A1DC6A-EC22-C804-FC44-5...	5/10/2016 5:41 PM	[12A1DC6A-EC22-...	170 KB
7zFM.exe	5/10/2016 5:41 PM	Application	483 KB
7zG.exe	5/10/2016 5:41 PM	Application	327 KB
7-zip.chm.[12A1DC6A-EC22-C804-FC44-...	5/10/2016 5:50 PM	[12A1DC6A-EC22-...	104 KB
7-zip.dll	5/10/2016 5:41 PM	Application extens...	49 KB
descript.ion.[12A1DC6A-EC22-C804-FC4...	4/4/2011 7:54 PM	[12A1DC6A-EC22-...	2 KB
History.txt.[12A1DC6A-EC22-C804-FC44-...	5/10/2016 5:49 PM	[12A1DC6A-EC22-...	47 KB
License.txt.[12A1DC6A-EC22-C804-FC44-...	1/1/2016 3:17 PM	[12A1DC6A-EC22-...	4 KB
readme.txt.[12A1DC6A-EC22-C804-FC44-...	5/10/2016 5:48 PM	[12A1DC6A-EC22-...	4 KB
Uninstall.exe	5/10/2016 5:41 PM	Application	14 KB

Buran Encryption



!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT - Notepad
File Edit Format View Help

```
!!! ALL YOUR FILES ARE ENCRYPTED !!!

All your files, documents, photos, databases and other important files are encrypted.

You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an email: onlinebigbrotheriswatchingyou@protonmail.com or onlinebigbrotheriswatchingyou@tutar
But this file should be of not valuable!

Do you really want to restore your files?
Write to email: onlinebigbrotheriswatchingyou@protonmail.com
Reserved email: onlinebigbrotheriswatchingyou@tutanota.com
Your personal ID: D4E-5B3-FC5

Attention!
 * Do not rename encrypted files.
 * Do not try to decrypt your data using third party software, it may cause permanent data loss.
 * Decryption of your files with the help of third parties may cause increased price (they add their fee to our).

To avoid getting your computer infected AGAIN  you should be very careful when downloading software - the only safe place to download applications is th
```

Ransom Note displayed by Zeppelin

Conclusion

In this day where we create faster solutions and detections, malware authors also adapt to this by creating and releasing more malware updates to make sure that it stays relevant. This is evident in ransomware campaigns as malware authors get an extra motivation by gaining huge sums of money in exchange for file recovery. Normally, ransomware only infects document files which is also the case with Buran. However, Zeppelin takes things a step further by targeting not only document related files but also applications and tools installed in the victim's system . This extent of damage gives Zeppelin more leverage for the victim to pay the ransom. With this, delivering more advanced detections and solutions that will withstand fast-paced changes of ransomware is needed. Just like G Data's DeepRay technology that uses artificial intelligence and machine learning to protect its user from such sophisticated tactics of criminal hackers.

Information for fellow researchers

G DATA Detections:

Buran: Win32.Trojan-Ransom.Buran.A
Zeppelin: Win32.Trojan-Ransom.Zeppelin.A

IOC

Buran:
7f0dcd4b9d8881fd0c42a6d605f843c496b7ed1fc3ae3a29d0bd37e851eaadfb

Zeppelin:
1cefe918ae56ebd3c2de309efbdd3a99808c823615a11a58bf144d3d6699f69b

References

[1] hxxps://www.symantec.com/blogs/expert-perspectives/ransomware-activity-declines-remains-dangerous-threat

[2] hxxps://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

[3] hxxps://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

G DATA Security Lab
Virus-Analyst Team