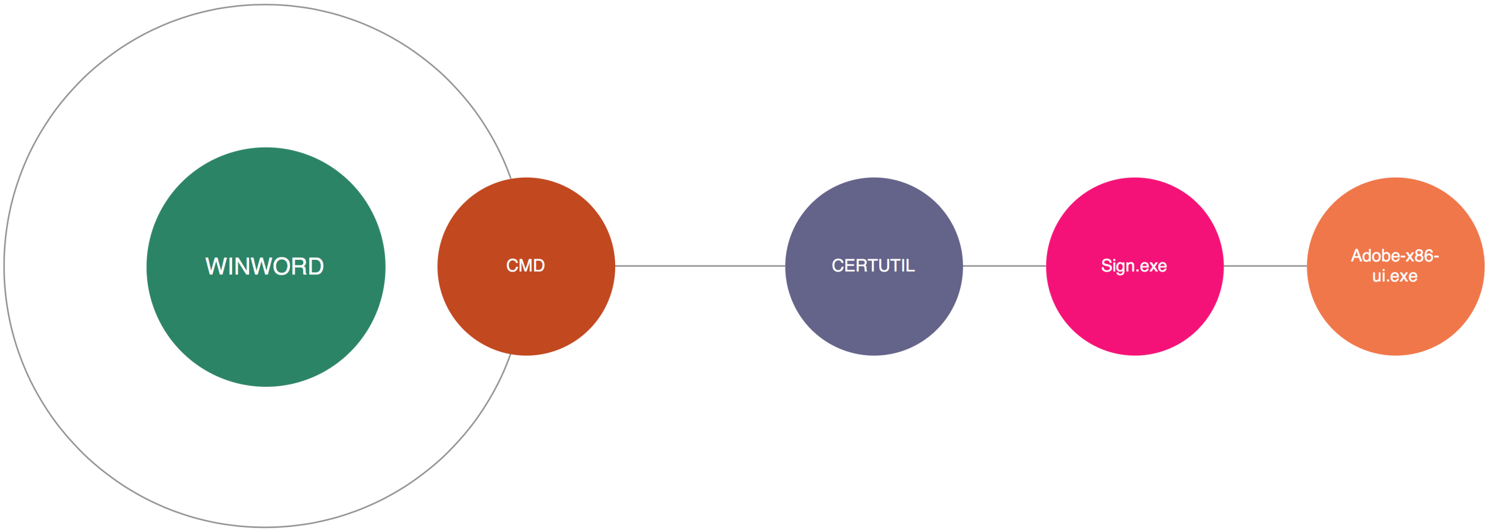
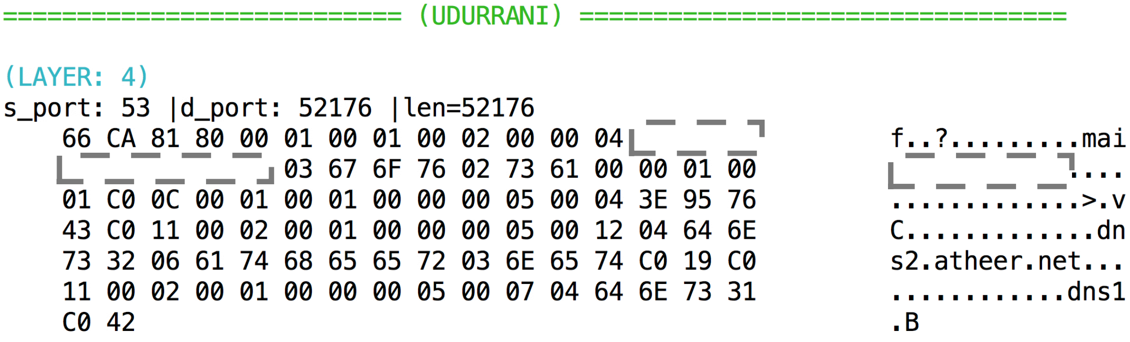
Basic Flow

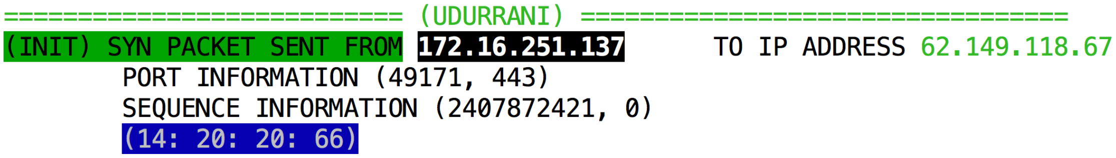


```
cmd.exe /c certutil -decode C:\Users\shm0\AppData\Local\Temp\\Signature.crt C:\Users\shm0\AppData\Local\Temp\\Sign.exe
certutil  -decode C:\Users\shm0\AppData\Local\Temp\\Signature.crt C:\Users\shm0\AppData\Local\Temp\\Sign.exe
cmd.exe /c C:\Users\shm0\AppData\Local\Temp\\Sign.exe

cmd.exe is using CreateProcessW WITH bInheritHandles -> TRUE for inheritable handles and EXTENDED_STARTUPINFO_PRESENT where STARTUPINFOEX structure is populated:

typedef struct _STARTUPINFOEX {
  STARTUPINFO                 StartupInfo;
  PPROC_THREAD_ATTRIBUTE_LIST lpAttributeList;
} STARTUPINFOEX, *LPSTARTUPINFOEX;


typedef struct _STARTUPINFO {
  DWORD  cb;
  LPTSTR lpReserved;
  LPTSTR lpDesktop;
  LPTSTR lpTitle;
  DWORD  dwX;
  DWORD  dwY;
  DWORD  dwXSize;
  DWORD  dwYSize;
  DWORD  dwXCountChars;
  DWORD  dwYCountChars;
  DWORD  dwFillAttribute;
  DWORD  dwFlags;
  WORD   wShowWindow;
  WORD   cbReserved2;
  LPBYTE lpReserved2;
  HANDLE hStdInput;
  HANDLE hStdOutput;
  HANDLE hStdError;
} STARTUPINFO, *LPSTARTUPINFO;
```

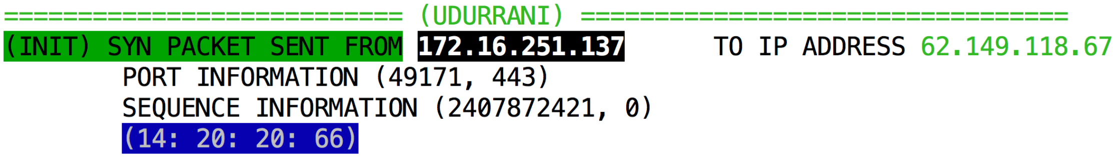
DNS & TCP



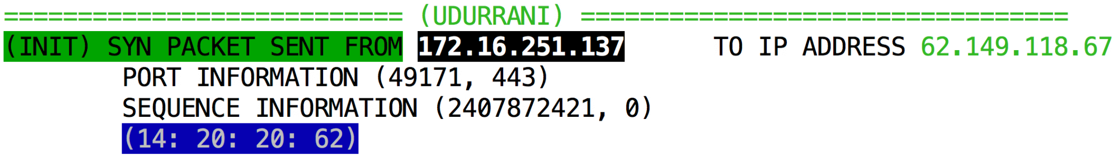
```
=========================== (UDURRANI) =================================

(LAYER: 4)
s_port: 53 |d_port: 52176 |len=52176
    66 CA 81 80 00 01 00 01 00 02 00 00 04 [redacted]          f..?.........mai
    [redacted] 03 67 6F 76 02 73 61 00 00 01 00               [redacted]....
    01 C0 0C 00 01 00 01 00 00 00 05 00 04 3E 95 76          ..............>.v
    43 C0 11 00 02 00 01 00 00 00 05 00 12 04 64 6E          C.............dn
    73 32 06 61 74 68 65 65 72 03 6E 65 74 C0 19 C0          s2.atheer.net...
    11 00 02 00 01 00 00 00 05 00 07 04 64 6E 73 31          ............dns1
    C0 42                                                    .B
```



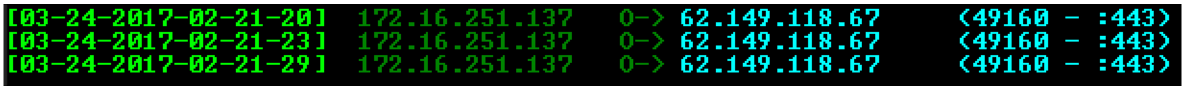
```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.251.137      TO IP ADDRESS 62.149.118.67
        PORT INFORMATION (49171, 443)
        SEQUENCE INFORMATION (2407872421, 0)
        (14: 20: 20: 66)
```



```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.251.137      TO IP ADDRESS 62.149.118.67
        PORT INFORMATION (49171, 443)
        SEQUENCE INFORMATION (2407872421, 0)
        (14: 20: 20: 66)
```

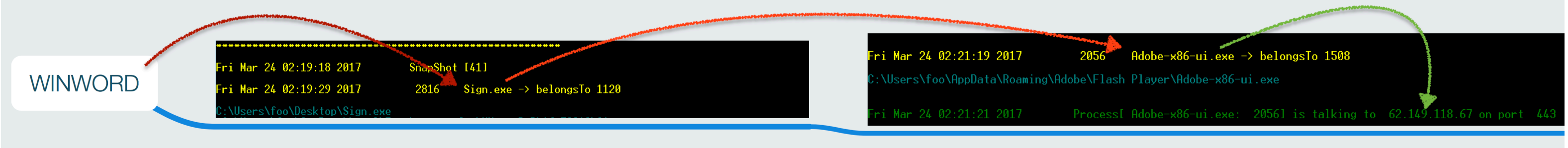


```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.251.137      TO IP ADDRESS 62.149.118.67
        PORT INFORMATION (49171, 443)
        SEQUENCE INFORMATION (2407872421, 0)
        (14: 20: 20: 62)
```



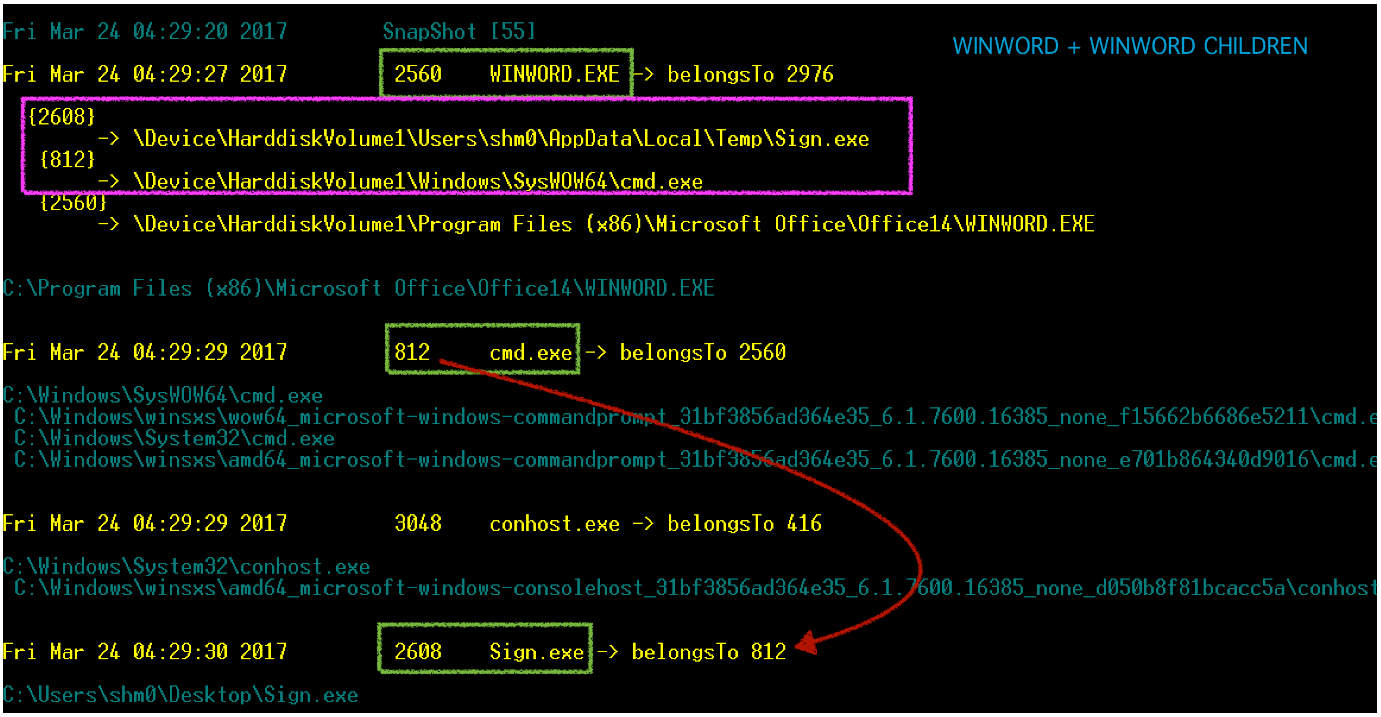
```
[03-24-2017-02-21-20]  172.16.251.137   0-> 62.149.118.67     <49160 - :443>
[03-24-2017-02-21-23]  172.16.251.137   0-> 62.149.118.67     <49160 - :443>
[03-24-2017-02-21-29]  172.16.251.137   0-> 62.149.118.67     <49160 - :443>
```

Dynamic Analysis View

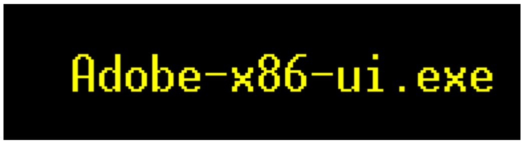


```
************************************************************
Fri Mar 24 02:19:18 2017        SnapShot [41]
Fri Mar 24 02:19:29 2017         2816    Sign.exe -> belongsTo 1120
C:\Users\foo\Desktop\Sign.exe
```

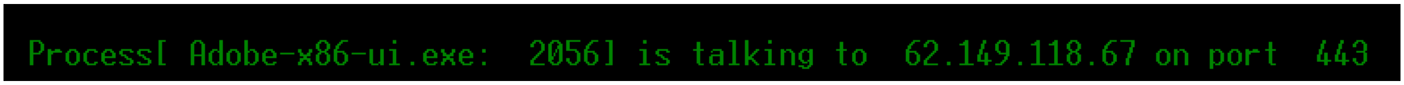
```
Fri Mar 24 02:21:19 2017         2056    Adobe-x86-ui.exe -> belongsTo 1508
C:\Users\foo\AppData\Roaming\Adobe\Flash Player\Adobe-x86-ui.exe

Fri Mar 24 02:21:21 2017        Process[ Adobe-x86-ui.exe:  2056] is talking to  62.149.118.67 on port  443
```



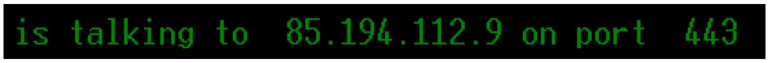
```
Fri Mar 24 04:29:20 2017        SnapShot [55]
Fri Mar 24 04:29:27 2017         2560    WINWORD.EXE -> belongsTo 2976
 {2608}
      -> \Device\HarddiskVolume1\Users\shm0\AppData\Local\Temp\Sign.exe
  {812}
      -> \Device\HarddiskVolume1\Windows\SysWOW64\cmd.exe
  {2560}
      -> \Device\HarddiskVolume1\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE

C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE

Fri Mar 24 04:29:29 2017         812     cmd.exe -> belongsTo 2560

C:\Windows\SysWOW64\cmd.exe
 C:\Windows\winsxs\wow64_microsoft-windows-commandprompt_31bf3856ad364e35_6.1.7600.16385_none_f15662b6686e5211\cmd.e
 C:\Windows\System32\cmd.exe
 C:\Windows\winsxs\amd64_microsoft-windows-commandprompt_31bf3856ad364e35_6.1.7600.16385_none_e701b864340d9016\cmd.e

Fri Mar 24 04:29:29 2017         3048    conhost.exe -> belongsTo 416

C:\Windows\System32\conhost.exe
 C:\Windows\winsxs\amd64_microsoft-windows-consolehost_31bf3856ad364e35_6.1.7600.16385_none_d050b8f81bcacc5a\conhost

Fri Mar 24 04:29:30 2017         2608    Sign.exe -> belongsTo 812

C:\Users\shm0\Desktop\Sign.exe
```



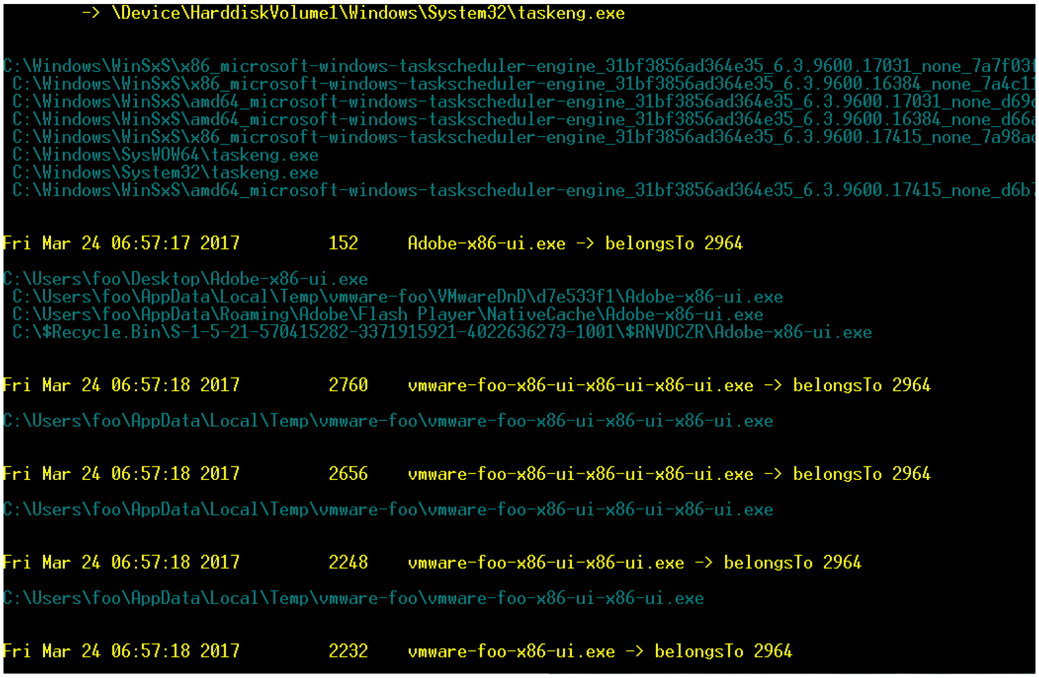
```
Adobe-x86-ui.exe
```



```
Process[ Adobe-x86-ui.exe:  2056] is talking to  62.149.118.67 on port  443
```



```
is talking to  85.194.112.9 on port  443
```



```
        -> \Device\HarddiskVolume1\Windows\System32\taskeng.exe


C:\Windows\WinSxS\x86_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.17031_none_7a7f03
 C:\Windows\WinSxS\x86_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.16384_none_7a4c1
 C:\Windows\WinSxS\amd64_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.17031_none_d69
 C:\Windows\WinSxS\amd64_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.16384_none_d66
 C:\Windows\WinSxS\x86_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.17415_none_7a98a
 C:\Windows\SysWOW64\taskeng.exe
 C:\Windows\System32\taskeng.exe
 C:\Windows\WinSxS\amd64_microsoft-windows-taskscheduler-engine_31bf3856ad364e35_6.3.9600.17415_none_d6b


Fri Mar 24 06:57:17 2017         152     Adobe-x86-ui.exe -> belongsTo 2964

C:\Users\foo\Desktop\Adobe-x86-ui.exe
 C:\Users\foo\AppData\Local\Temp\vmware-foo\VMwareDnD\d7e533f1\Adobe-x86-ui.exe
 C:\Users\foo\AppData\Roaming\Adobe\Flash Player\NativeCache\Adobe-x86-ui.exe
 C:\$Recycle.Bin\S-1-5-21-570415282-3371915921-4022636273-1001\$RNVDCZR\Adobe-x86-ui.exe


Fri Mar 24 06:57:18 2017         2760    vmware-foo-x86-ui-x86-ui-x86-ui.exe -> belongsTo 2964

C:\Users\foo\AppData\Local\Temp\vmware-foo\vmware-foo-x86-ui-x86-ui-x86-ui.exe


Fri Mar 24 06:57:18 2017         2656    vmware-foo-x86-ui-x86-ui-x86-ui.exe -> belongsTo 2964

C:\Users\foo\AppData\Local\Temp\vmware-foo\vmware-foo-x86-ui-x86-ui-x86-ui.exe


Fri Mar 24 06:57:18 2017         2248    vmware-foo-x86-ui-x86-ui.exe -> belongsTo 2964

C:\Users\foo\AppData\Local\Temp\vmware-foo\vmware-foo-x86-ui-x86-ui.exe


Fri Mar 24 06:57:18 2017         2232    vmware-foo-x86-ui.exe -> belongsTo 2964
```

Binary Info

```
files\Adobe-x86-ui.exe, 55808, 4ed42233962a89deaa89fd7b989db081
files\Sign.exe, 115712, 3cd5fa46507657f723719b7809d2d1f9
```

Sign.exe (Compiled)

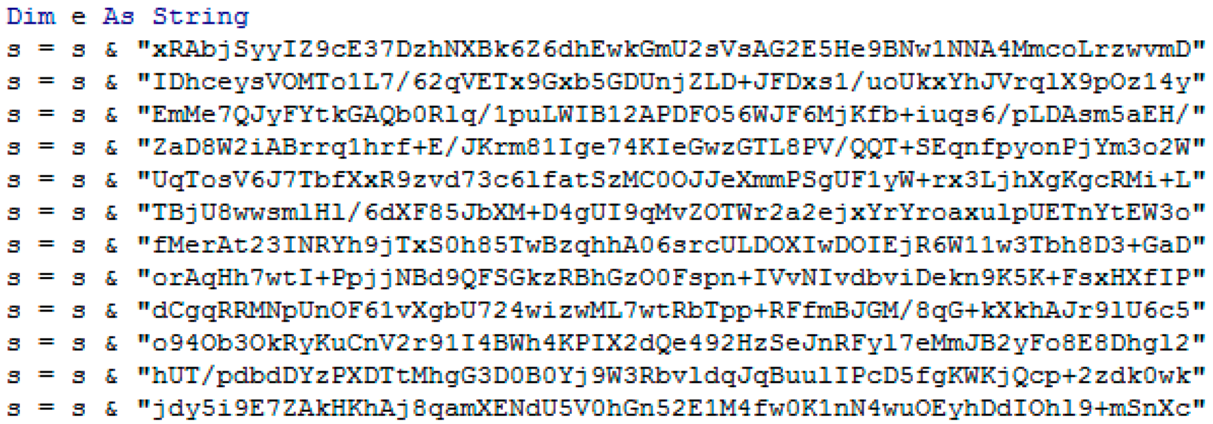
```
Thu Mar 23 13:48:12 2017
```

Adobe-x86-ui.exe (Compiled)

```
Thu Mar 23 13:48:12 2017
```

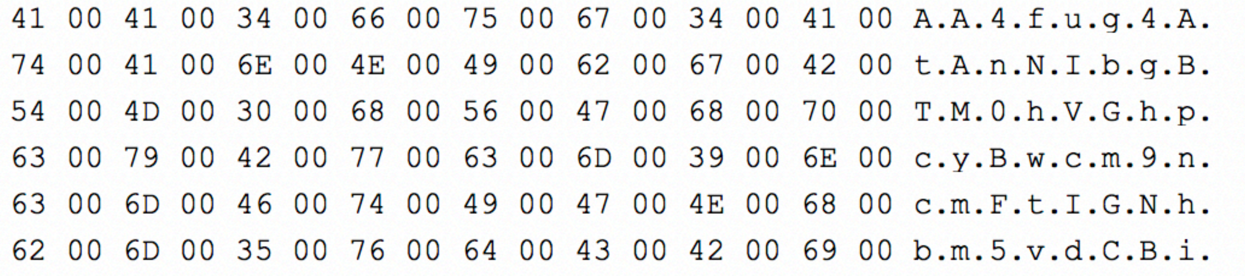
WINWORD DOCUMENT:

Word document is equipped with a heavily obfuscated macro.



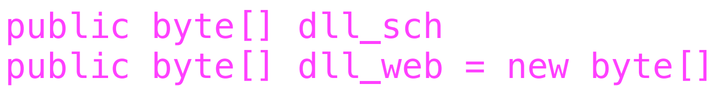
```
Dim e As String
s = s & "xRAbjSyyIZ9cE37DzhNXBk6Z6dhEwkGmU2sVsAG2E5He9BNw1NNA4MmcoLrzwvmD"
s = s & "IDhceysVOMTo1L7/62qVETx9Gxb5GDUnjZLD+JFDxs1/uoUkxYhJVrqlX9pOz14y"
s = s & "EmMe7QJyFYtkGAQb0Rlq/1puLWIB12APDFO56WJF6MjKfb+iuqs6/pLDAsm5aEH/"
s = s & "ZaD8W2iABrrq1hrf+E/JKrm81Ige74KIeGwzGTL8PV/QQT+SEqnfpyonPjYm3o2W"
s = s & "UqTosV6J7TbfXxR9zvd73c61fatSzMC0OJJeXmmPSgUF1yW+rx3LjhXgKgcRMi+L"
s = s & "TBjU8wwsmlHl/6dXF85JbXM+D4gUI9qMvZOTWr2a2ejxYrYroaxulpUETnYtEW3o"
s = s & "fMerAt23INRYh9jTxS0h85TwBzqhhA06srcULDOXIwDOIEjR6W11w3Tbh8D3+GaD"
s = s & "orAqHh7wtI+PpjjNBd9QFSGkzRBhGzO0Fspn+IVvNIvdbviDekn9K5K+FsxHXfIP"
s = s & "dCgqRRMNpUnOF61vXgbU724wizwML7wtRbTpp+RFfmBJGM/8qG+kXkhAJr91U6c5"
s = s & "o94Ob3OkRyKuCnV2r91I4BWh4KPIX2dQe492HzSeJnRFyl7eMmJB2yFo8E8Dhgl2"
s = s & "hUT/pdbdDYzPXDTtMhgG3D0B0Yj9W3RbvldqJqBuulIPcD5fgKWKjQcp+2zdk0wk"
s = s & "jdy5i9E7ZAkHKhAj8qamXENdU5V0hGn52E1M4fw0K1nN4wuOEyhDdIOhl9+mSnXc"
```

Eventually strings are flipped via StrReverse()
It converts the following payload into first stage binary called Sign.exe. Payload is pretty huge so I cant put all of it here. Following is just one of the screen shot.

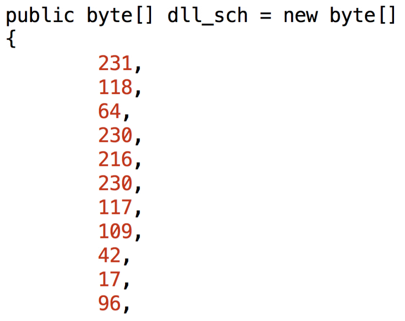


```
41 00 41 00 34 00 66 00 75 00 67 00 34 00 41 00 A.A.4.f.u.g.4.A.
74 00 41 00 6E 00 4E 00 49 00 62 00 67 00 42 00 t.A.n.N.I.b.g.B.
54 00 4D 00 30 00 68 00 56 00 47 00 68 00 70 00 T.M.0.h.V.G.h.p.
63 00 79 00 42 00 77 00 63 00 6D 00 39 00 6E 00 c.y.B.w.c.m.9.n.
63 00 6D 00 46 00 74 00 49 00 47 00 4E 00 68 00 c.m.F.t.I.G.N.h.
62 00 6D 00 35 00 76 00 64 00 43 00 42 00 69 00 b.m.5.v.d.C.B.i.
```

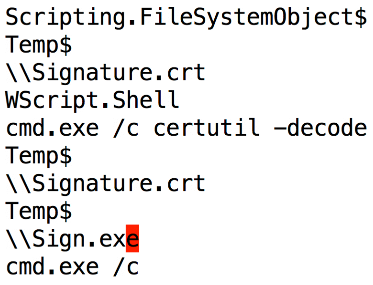
Sign.exe is a .net binary. It has a class called PAYLOAD with a dropper functionality. it also creates 2 DLL files



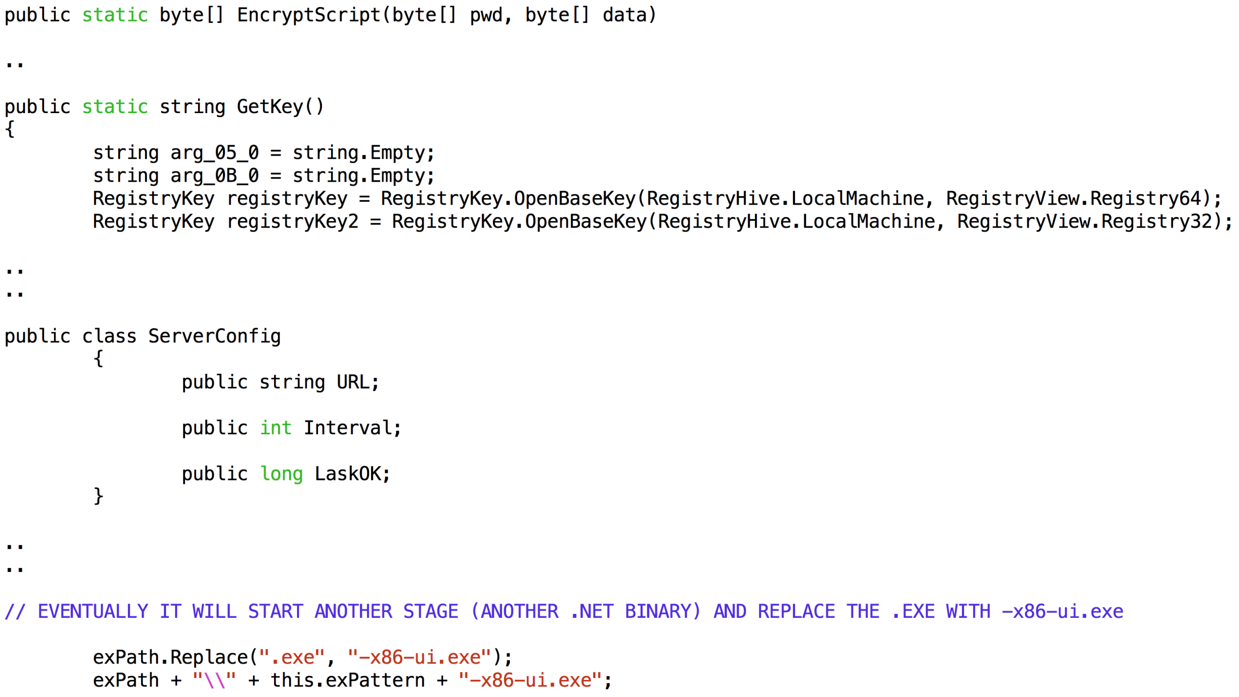
```
public byte[] dll_sch
public byte[] dll_web = new byte[]
```



```
public byte[] dll_sch = new byte[]
{
        231,
        118,
        64,
        230,
        216,
        230,
        117,
        109,
        42,
        17,
        96,
```



```
Scripting.FileSystemObject$
Temp$
\\Signature.crt
WScript.Shell
cmd.exe /c certutil -decode
Temp$
\\Signature.crt
Temp$
\\Sign.exe
cmd.exe /c
```



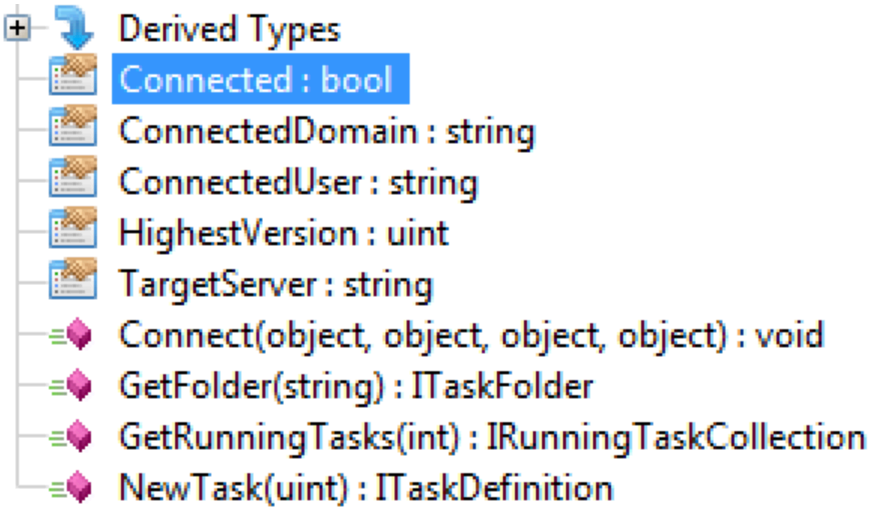
```
public static byte[] EncryptScript(byte[] pwd, byte[] data)

..

public static string GetKey()
{
        string arg_05_0 = string.Empty;
        string arg_0B_0 = string.Empty;
        RegistryKey registryKey = RegistryKey.OpenBaseKey(RegistryHive.LocalMachine, RegistryView.Registry64);
        RegistryKey registryKey2 = RegistryKey.OpenBaseKey(RegistryHive.LocalMachine, RegistryView.Registry32);

..
..

public class ServerConfig
        {
                public string URL;

                public int Interval;

                public long LaskOK;
        }

..
..

// EVENTUALLY IT WILL START ANOTHER STAGE (ANOTHER .NET BINARY) AND REPLACE THE .EXE WITH -x86-ui.exe

        exPath.Replace(".exe", "-x86-ui.exe");
        exPath + "\\" + this.exPattern + "-x86-ui.exe";
```

This stage will drop Adobe-x86-ui.exe (C:\Users\foo\AppData\Roaming\Adobe\Flash Player) and 2 helper DLL's, with following hashes.

4F13BEC852002EA7208DEAF82B53F90D
E845D2AA781579F97BD67C2E4970C476

Summary:

Attack is meant to exfiltrate corporate information to a CnC. Most probably to make use of it in future or to better understand the corporate network.



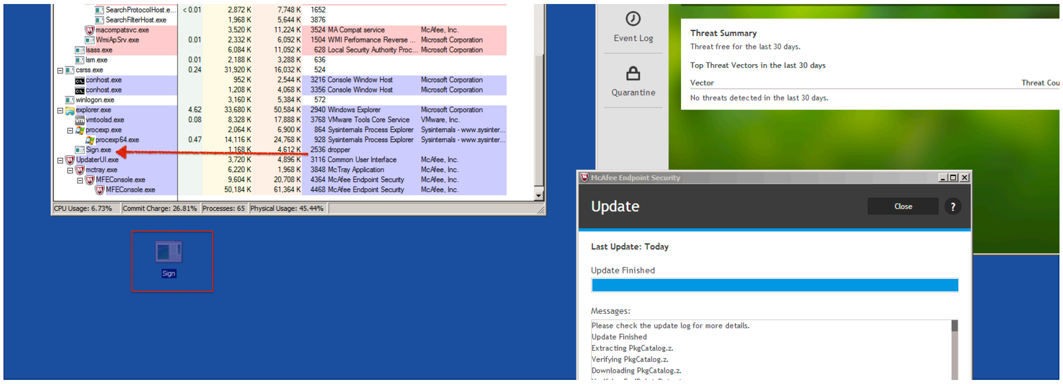
```
Derived Types
Connected : bool
ConnectedDomain : string
ConnectedUser : string
HighestVersion : uint
TargetServer : string
Connect(object, object, object, object) : void
GetFolder(string) : ITaskFolder
GetRunningTasks(int) : IRunningTaskCollection
NewTask(uint) : ITaskDefinition
```

Other Payloads:

3CD5FA46507657F723719B7809D2D1F9
4ED42233962A89DEAA89FD7B989DB081

Prevention:

I tested the payload i.e. WORD document and then the standalone binary. Most of the good AV's were not able to prevent it. They had no clue about the payload at all. I started with McAfee.



```
SearchProtocolHost.e...  < 0.01   2,872 K   7,748 K  1652
SearchFilterHost.exe              1,968 K   5,644 K  3876
macompatsvc.exe                   3,520 K  11,224 K  3524 MA Compat service                McAfee, Inc.
WmiApSrv.exe               0.01   2,332 K   6,092 K  1504 WMI Performance Reverse ...     Microsoft Corporation
lsass.exe                         6,084 K  11,092 K   628 Local Security Authority Proc... Microsoft Corporation
lsm.exe                    0.01   2,188 K   3,288 K   636
csrss.exe                  0.24  31,920 K  16,032 K   524
conhost.exe                         952 K   2,544 K  3216 Console Window Host              Microsoft Corporation
conhost.exe                       1,208 K   4,068 K  3356 Console Window Host              Microsoft Corporation
winlogon.exe                      3,160 K   5,384 K   572
explorer.exe               4.62  33,680 K  50,584 K  2940 Windows Explorer                 Microsoft Corporation
vmtoolsd.exe               0.08   8,328 K  17,888 K  3768 VMware Tools Core Service        VMware, Inc.
procexp.exe                       2,064 K   6,900 K   864 Sysinternals Process Explorer    Sysinternals - www.sysinter...
procexp64.exe              0.47  14,116 K  24,768 K   928 Sysinternals Process Explorer    Sysinternals - www.sysinter...
Sign.exe                          1,168 K   4,612 K  2536 dropper
UpdaterUI.exe                     3,720 K   4,896 K  3116 Common User Interface            McAfee, Inc.
mctray.exe                        6,220 K   1,968 K  3848 McTray Application               McAfee, Inc.
MFEConsole.exe                    9,604 K  20,708 K  4364 McAfee Endpoint Security         McAfee, Inc.
MFEConsole.exe                   50,184 K  61,364 K  4468 McAfee Endpoint Security         McAfee, Inc.
CPU Usage: 6.73%  Commit Charge: 26.81%  Processes: 65  Physical Usage: 45.44%
```

Threat Summary
Threat free for the last 30 days.

Top Threat Vectors in the last 30 days

Vector — Threat Cou
No threats detected in the last 30 days.

McAfee Endpoint Security

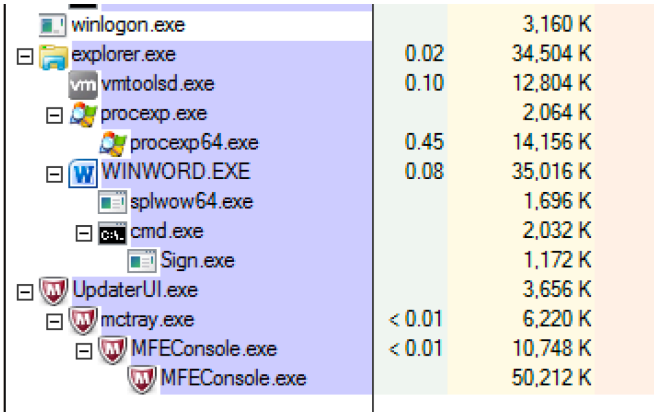
Update

Last Update: Today

Update Finished

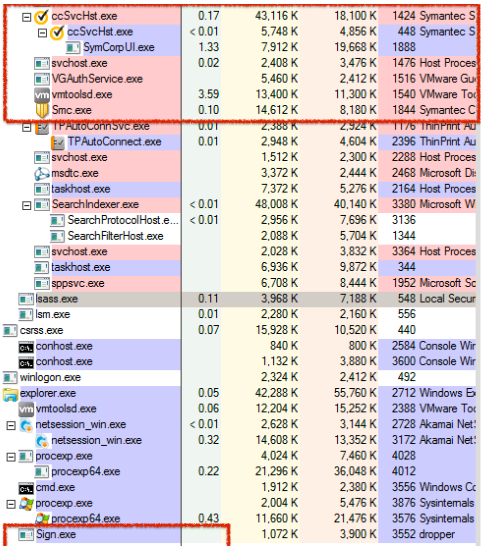
Messages:

```
Please check the update log for more details.
Update Finished
Extracting PkgCatalog.z.
Verifying PkgCatalog.z.
Downloading PkgCatalog.z.
```



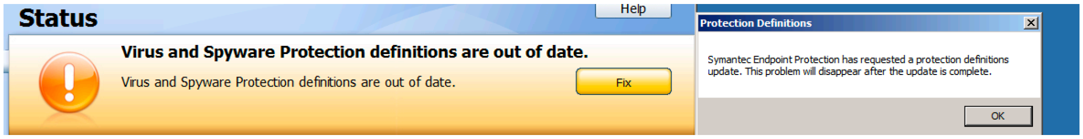
```
winlogon.exe                   3,160 K
explorer.exe           0.02   34,504 K
  vmtoolsd.exe         0.10   12,804 K
  procexp.exe                  2,064 K
    procexp64.exe      0.45   14,156 K
  WINWORD.EXE          0.08   35,016 K
    splwow64.exe               1,696 K
    cmd.exe                    2,032 K
      Sign.exe                 1,172 K
UpdaterUI.exe                  3,656 K
  mctray.exe         < 0.01    6,220 K
    MFEConsole.exe   < 0.01   10,748 K
      MFEConsole.exe          50,212 K
```

Then I tried against Symantec and there was no prevention.



```
ccSvcHst.exe                 0.17   43,116 K   18,100 K  1424 Symantec S
  ccSvcHst.exe             < 0.01    5,748 K    4,856 K   448 Symantec S
    SymCorpUI.exe            1.33    7,912 K   19,668 K  1888
svchost.exe                  0.02    2,408 K    3,476 K  1476 Host Proces
VGAuthService.exe                    5,460 K    2,412 K  1516 VMware Gu
vmtoolsd.exe                 3.59   13,400 K   11,300 K  1540 VMware To
Smc.exe                      0.10   14,612 K    8,180 K  1844 Symantec C
TPAutoConnSvc.exe            0.01    2,388 K    2,924 K  1176 ThinPrint Au
  TPAutoConnect.exe          0.01    2,948 K    4,604 K  2396 ThinPrint Au
svchost.exe                          1,512 K    2,300 K  2288 Host Proces
msdtc.exe                            3,372 K    2,444 K  2468 Microsoft Di
taskhost.exe                         7,372 K    5,276 K  2164 Host Proces
SearchIndexer.exe          < 0.01   48,008 K   40,140 K  3380 Microsoft W
  SearchProtocolHost.e...  < 0.01    2,956 K    7,696 K  3136
  SearchFilterHost.exe               2,088 K    5,704 K  1344
svchost.exe                          2,028 K    3,832 K  3364 Host Proces
taskhost.exe                         6,936 K    9,872 K   344
sppsvc.exe                           6,708 K    8,444 K  1952 Microsoft Sc
lsass.exe                    0.11    3,968 K    7,188 K   548 Local Secur
lsm.exe                      0.01    2,280 K    2,160 K   556
csrss.exe                    0.07   15,928 K   10,520 K   440
  conhost.exe                          840 K      800 K  2584 Console Wir
  conhost.exe                        1,132 K    3,880 K  3600 Console Wir
winlogon.exe                         2,324 K    2,412 K   492
explorer.exe                 0.05   42,288 K   55,760 K  2712 Windows Ex
  vmtoolsd.exe               0.06   12,204 K   15,252 K  2388 VMware Too
  netsession_win.exe       < 0.01    2,628 K    3,144 K  2728 Akamai Net!
    netsession_win.exe       0.32   14,608 K   13,352 K  3172 Akamai Net!
  procexp.exe                        4,024 K    7,460 K  4028
    procexp64.exe            0.22   21,296 K   36,048 K  4012
  cmd.exe                            1,912 K    2,380 K  3556 Windows Co
  procexp.exe                        2,004 K    5,476 K  3876 Sysinternals
    procexp64.exe            0.43   11,660 K   21,476 K  3576 Sysinternals
  Sign.exe                           1,072 K    3,900 K  3552 dropper
```

But Symantec AV was not updated. Last update was done 11 days ago. So I started the update and waited for like an hour or so and kept on getting the following message.



Virus and Spyware Protection definitions are out of date.

Virus and Spyware Protection definitions are out of date.

Symantec Endpoint Protection has requested a protection definitions update. This problem will disappear after the update is complete.

Eventually I gave up!