

魔盾安全分析报告

分析类型	开始时间	结束时间	持续时间	分析引擎版本
FILE	2016-10-30 20:21:28	2016-10-30 20:24:40	192 秒	1.4-Maldun

虚拟机器名	标签	虚拟机管理	开机时间	关机时间
win7-sp1-x64-1	win7-sp1-x64-1	KVM	2016-10-30 20:21:28	2016-10-30 20:24:40

魔盾分数
10.0
恶意的

文件详细信息

文件名	waiting.exe
文件大小	110080 字节
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
CRC32	94B40ABC
MD5	936a0af1dc7ef417dbd6d26ba59adb35
SHA1	4839f3231e0a9243435e474fa31618f8e0e19a07
SHA256	19b5c8fe244ae2d7b1a530d5e3ca503a18a46927ea7944a6d4687a5cd702cf0f
SHA512	36f5d49e9a432d764c8ed960d67153592d1197cdf35a92599b03483f233f7901808438dbbde0ce29a5447915b94b2d259dc70f78e0008fe60b564b99dc211d29
Ssdeep	1536:6w/Hut1n1LqRSh3YEMmHN/mtvgh+ThWMCBV/qrnouy8XJroEmRrbOV:B/H6sgMmtWgh+cMqkoutX1oECr+
PEiD	无匹配
Yara	<ul style="list-style-type: none"><li>UPXv20MarkusLaszloReiser ()</li><li>UPXV200V290MarkusOberhumerLaszloMolnarJohnReiser ()</li><li>UPX293300LZMAMarkusOberhumerLaszloMolnarJohnReiser ()</li><li>UPX20030XMarkusOberhumerLaszloMolnarJohnReiser ()</li></ul>
VirusTotal	无此文件扫描结果

特征

创建RWX内存
开始系统监听0.0.0.0:4361
对一些具体的运行中的进程呈现出兴趣
process: csrss.exe process: svchost.exe
对一个无法找到的进程进行重复搜索，可能希望以startbrowser=1选项运行
从文件自身的二进制镜像中读取数据
self_read: process: runhome.exe, pid: 2540, offset: 0x00000000, length: 0x000e5400
一个进程创建了一个隐藏窗口
Process: waiting.exe -> C:\Windows\sysnative\cmd Process: export.exe -> C:\Users\test\AppData\Local\Temp\ihgzvzum.bat Process: runhome.exe -> C:\Users\test\AppData\Local\Temp\cugfjlnk.bat Process: svchost.exe -> cmd.exe
投放出一个二进制文件并执行它
binary: C:\Users\test\AppData\Local\Temp\export.exe binary: C:\Users\test\AppData\Roaming\hgpylpin\runhome.exe binary: C:\Users\test\AppData\Roaming\hgpylpin\AdMain.exe
魔盾wping.org 域名信誉系统
灰名单: wj.center.oldlist.info 灰名单: pack.1e5.com 灰名单: very.icafedh.com 未知: c.cotton.netease.com
魔盾wping.org IP地址信誉系统
灰名单: 150.138.170.115
HTTP数据流中包含可疑的恶意软件数据
get_no_useragent: HTTP traffic contains a GET request with no user-agent header suspicious_request: http://very.icafedh.com/new_net/key_lq_new.zip suspicious_request: http://very.icafedh.com/wy/wy.ini suspicious_request: http://flow.app100714692.twsapp.com/v19/page/get.php?mac=52-54-00-C6-F5-C2&qqnum=&ver=2.0.2.5&type=0 suspicious_request: http://pack.1e5.com/ico/119.ico suspicious_request: http://int.dpool.sina.com.cn/iplookup/iplookup.php

**suspicious\_request:** http://b2c.nb.163.com/b2c/channel/get\_channel\_client/?channel\_id=1  
**suspicious\_request:** http://pack.1e5.com/ico/123.ico  
**suspicious\_request:** http://c.cotton.netease.com/buckets/3XrHkq/files/5dDFTA9Dln0  
**suspicious\_request:** http://very.icafedh.com/new\_net/game\_bc2\_new.zip  
**suspicious\_request:** http://pack.1e5.com/down/new5.zip.crc  
**suspicious\_request:** http://very.icafedh.com/new\_net/game3\_new.zip  
**suspicious\_request:** http://very.icafedh.com/new\_net/key2\_new.zip

发起了一些HTTP请求

**url:** http://pack.1e5.com/down/new5.zip.crc?id=2574986  
**url:** http://pack.1e5.com/down/new5.zip?id=2576780  
**url:** http://very.icafedh.com/new\_net/key\_lq\_new.zip  
**url:** http://very.icafedh.com/wy/wy.ini  
**url:** http://flow.app100714692.twsapp.com/v19/page/get.php?mac=52-54-00-C6-F5-C2&qqnum=&ver=2.0.2.5&type=0  
**url:** http://pack.1e5.com/ico/119.ico  
**url:** http://int.dpool.sina.com.cn/iplookup/iplookup.php  
**url:** http://b2c.nb.163.com/b2c/channel/get\_channel\_client/?channel\_id=1  
**url:** http://pack.1e5.com/ico/123.ico  
**url:** http://c.cotton.netease.com/buckets/3XrHkq/files/5dDFTA9Dln0  
**url:** http://very.icafedh.com/new\_net/game\_bc2\_new.zip  
**url:** http://pack.1e5.com/down/new5.zip.crc  
**url:** http://very.icafedh.com/new\_net/game3\_new.zip  
**url:** http://very.icafedh.com/new\_net/key2\_new.zip

二进制文件可能包含加密或压缩数据

**section:** name: UPX1, entropy: 7.98, characteristics: IMAGE\_SCN\_CNT\_INITIALIZED\_DATA|IMAGE\_SCN\_MEM\_EXECUTE|IMAGE\_SCN\_MEM\_READ|IMAGE\_SCN\_MEM\_WRITE, raw\_size: 0x0000de00, virtual\_size: 0x0000e000

可执行文件被使用UPX压缩

**section:** name: UPX0, entropy: 0.00, characteristics: IMAGE\_SCN\_CNT\_UNINITIALIZED\_DATA|IMAGE\_SCN\_MEM\_EXECUTE|IMAGE\_SCN\_MEM\_READ|IMAGE\_SCN\_MEM\_WRITE, raw\_size: 0x00000000, virtual\_size: 0x00025000

强制将一个创建的进程加载为另一个不相关进程的子进程

可能进行了时间有效期检查，检查本地时间后过早退出

**process:** timeout.exe, PID 3020

执行了一个进程并在其中注入代码（可能是在解包过程中）

通过进程尝试长时间延迟分析任务

**Process:** rundll32.exe tried to sleep 1027 seconds, actually delayed analysis time by 0 seconds

网络活动包含了一个以上的不重复的用户代理

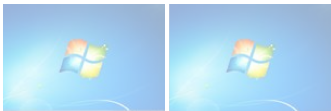
**Process:** export.exe  
**User-Agent:** iexplore.exe  
**Process:** rundll32.exe  
**User-Agent:**  
**Process:** rundll32.exe  
**User-Agent:** flowdatadll

尝试修改代理设置

投放了一个或多个恶意文件

**file:** c:\users\test\appdata\roaming\hgpylpin\popad.dll  
**file:** c:\users\test\appdata\roaming\hgpylpin\adkernel.dll  
**malicious:** c:\users\test\appdata\roaming\hgpylpin\yun.exe  
**suspicious:** c:\users\test\appdata\roaming\hgpylpin\desktop.dll  
**malicious:** c:\users\test\appdata\roaming\hgpylpin\admin.exe

运行截图



网络分析

访问主机记录

直接访问	IP地址	国家名
否	223.252.200.144	China
否	183.60.118.216	China
否	180.149.136.219	China
否	150.138.170.115	China
否	117.21.217.18	China
否	116.28.63.219	China
否	116.28.63.214	China
否	116.28.63.213	China

域名解析

域名	响应
wj.center.oldlist.info	A 116.28.63.214
pack.1e5.com	A 120.39.245.9 CNAME pack.1e5.com.xgslb.cn CNAME azure.xgslb.cn

	A 117.21.217.18
wj.hk.pk2012.info	
hk.pk2012.info	A 116.28.63.213
very.icafedh.com	CNAME azure.xgslb.net CNAME very.icafedh.com.xgslb.net
39222777.com	A 116.28.63.219
flow.app100714692.twsapp.com	A 183.60.118.216
int.dpool.sina.com.cn	A 180.149.136.219
b2c.nb.163.com	A 223.252.200.144
c.cotton.netease.com	CNAME c.cotton.netease.com.wscdns.com CNAME 1st.dtwscachev702.ourwebhttps.com A 150.138.170.115

TCP连接

IP地址	端口
116.28.63.219	20010
116.28.63.219	20010
116.28.63.219	20010
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
117.21.217.18	80
150.138.170.115	80
180.149.136.219	80
183.60.118.216	80
223.252.200.144	80

UDP连接

IP地址	端口
192.168.122.70	57797
116.28.63.213	6000
116.28.63.214	6000
116.28.63.214	5000
116.28.63.214	6655
116.28.63.214	5000
116.28.63.214	6655
116.28.63.219	8998
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
192.168.122.1	53
255.255.255.255	4361
255.255.255.255	4361


HTTP请求

URL	HTTP数据
-----	--------

http://pack.1e5.com/down/new5.zip.crc?id=2574986	GET /down/new5.zip.crc?id=2574986 HTTP/1.1 User-Agent: iexplore.exe Host: pack.1e5.com
http://pack.1e5.com/down/new5.zip?id=2576780	GET /down/new5.zip?id=2576780 HTTP/1.1 User-Agent: iexplore.exe Host: pack.1e5.com
http://very.icafedh.com/new_net/key_lq_new.zip	GET /new_net/key_lq_new.zip HTTP/1.1 Host: very.icafedh.com Cache-Control: no-cache
http://very.icafedh.com/wy/wy.ini	GET /wy/wy.ini HTTP/1.1 User-Agent: iexplore.exe Host: very.icafedh.com
http://flow.app100714692.twsapp.com/v19/page/get.php?mac=52-54-00-C6-F5-C2&qqnum=&ver=2.0.2.5&type=0	GET /v19/page/get.php?mac=52-54-00-C6-F5-C2&qqnum=&ver=2.0.2.5&type=0 HTTP/1.1 User-Agent: flowdatadll Host: flow.app100714692.twsapp.com Cache-Control: no-cache
http://pack.1e5.com/ico/119.ico	GET /ico/119.ico HTTP/1.1 User-Agent: iexplore.exe Host: pack.1e5.com
http://int.dpool.sina.com.cn/iplookup/iplookup.php	GET /iplookup/iplookup.php HTTP/1.1 User-Agent: iexplore.exe Host: int.dpool.sina.com.cn
http://b2c.nb.163.com/b2c/channel/get_channel_client/?channel_id=1	GET /b2c/channel/get_channel_client/?channel_id=1 HTTP/1.1 User-Agent: iexplore.exe Host: b2c.nb.163.com
http://pack.1e5.com/ico/123.ico	GET /ico/123.ico HTTP/1.1 User-Agent: iexplore.exe Host: pack.1e5.com
http://c.cotton.netease.com/buckets/3XrHkq/files/5dDFTA9DIn0	GET /buckets/3XrHkq/files/5dDFTA9DIn0 HTTP/1.1 User-Agent: iexplore.exe Host: c.cotton.netease.com Connection: Keep-Alive
http://very.icafedh.com/new_net/game_bc2_new.zip	GET /new_net/game_bc2_new.zip HTTP/1.1 Host: very.icafedh.com Cache-Control: no-cache
http://pack.1e5.com/down/new5.zip.crc	GET /down/new5.zip.crc HTTP/1.1 User-Agent: iexplore.exe Host: pack.1e5.com
http://very.icafedh.com/new_net/game3_new.zip	GET /new_net/game3_new.zip HTTP/1.1 Host: very.icafedh.com Cache-Control: no-cache
http://very.icafedh.com/new_net/key2_new.zip	GET /new_net/key2_new.zip HTTP/1.1 Host: very.icafedh.com Cache-Control: no-cache

静态分析

PE 信息

初始地址	0x00400000
入口地址	0x00433130
声明校验值	0x00000000
实际校验值	0x00021890
最低操作系统版本要求	4.0
编译时间	2016-05-27 22:05:04
图标	
图标精确哈希值	538a7c83150367577956690b0589e400
图标相似性哈希值	611bb965ab29e8abdf33aeeca22d5263

版本信息

LegalCopyright:	\x53bb\x5e7f\x544a
FileVersion:	1,0,0,0
ProductVersion:	1.0.0.0
Translation:	0x0000 0x04e4

PE数据组成

名称	虚拟地址	虚拟大小	原始数据大小	特征	熵(Entropy)
UPX0	0x00001000	0x00025000	0x00000000	IMAGE_SCN_CNT_UNINITIALIZED_DATA IMAGE_SCN_MEM_EXECUTE IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE	0.00
UPX1	0x00026000	0x0000e000	0x0000de00	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_EXECUTE IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE	7.98
.rsrc	0x00034000	0x0000d000	0x0000ce00	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE	3.63

资源

名称	偏移量	大小	语言	子语言	熵(Entropy)	文件类型
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_ICON	0x000402f4	0x00000468	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.92	GLS_BINARY_LSB_FIRST
RT_RCDATA	0x000318b0	0x0000001c	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.81	data
RT_RCDATA	0x000318b0	0x0000001c	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.81	data
RT_RCDATA	0x000318b0	0x0000001c	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.81	data
RT_RCDATA	0x000318b0	0x0000001c	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.81	data
RT_RCDATA	0x000318b0	0x0000001c	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.81	data
RT_GROUP_ICON	0x00040760	0x00000076	LANG_NEUTRAL	SUBLANG_NEUTRAL	2.94	MS Windows icon resource - 8 icons, 256-colors
RT_VERSION	0x000407dc	0x0000016c	LANG_NEUTRAL	SUBLANG_NEUTRAL	3.17	data
RT_MANIFEST	0x0004094c	0x00000263	LANG_NEUTRAL	SUBLANG_NEUTRAL	4.92	XML document text

导入

库 **KERNEL32.DLL**:

- 0x440c78 - LoadLibraryA
- 0x440c7c - GetProcAddress
- 0x440c80 - VirtualProtect
- 0x440c84 - VirtualAlloc
- 0x440c88 - VirtualFree
- 0x440c8c - ExitProcess

库 **COMCTL32.DLL**:

- 0x440c94 - InitCommonControlsEx

库 **GDI32.DLL**:

- 0x440c9c - BitBlt

库 **MSVCRT.dll:**

- 0x440ca4 - fabs

库 **OLE32.DLL:**

- 0x440cac - CoInitialize

库 **SHELL32.DLL:**

- 0x440cb4 - ShellExecuteExA

库 **SHLWAPI.DLL:**

- 0x440cbc - PathGetArgsA

库 **USER32.DLL:**

- 0x440cc4 - GetDC

库 **WINMM.DLL:**

- 0x440ccc - timeBeginPeriod

投放文件

ProtocolFilters.dll

文件名	ProtocolFilters.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\ProtocolFilters.dll</li></ul>
文件大小	1421312 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	fdaf390c22fadd69dfbf7c1738736b3b
SHA1	f7a9bed16b54bf339ecc72f7d621b6398fda783f
SHA256	ae3b1746b593c1bde89306756d8d108237612346f11f5bebefda0d26cc0cf119
SHA512	35dc7d7e4d56a4ca612e8a63e5d02143e1e285a0ac23b421bf89099c3cd061eca60dc99740a93d8d061787096ab85c1f9e4f58af5d75ea60eddb94afe857303e
Ssdeep	24576:Uv3Cx7gvdVLFih/81I9NkObhbPH7Bm6+KpPWoOxMj3OlG Czbp/X+TBCxeqNgaZ: +CxkVM/8unkOl bPH7Bu5qMzbp/OTBQeu
Yara	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li><li>DebuggerException__SetConsoleCtrl ()</li><li>MD5_Constants (Look for MD5 constants)</li><li>RIPEMD160_Constants (Look for RIPEMD-160 constants)</li><li>SHA1_Constants (Look for SHA1 constants)</li><li>SHA512_Constants (Look for SHA384/SHA512 constants)</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

home.xml

文件名	home.xml
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\home.xml</li></ul>
文件大小	4108 bytes
文件类型	data
MD5	13ee33525273346eedd182e44e0046d9
SHA1	b7ed388af080c22fb7d3f8f102429debbfca5149
SHA256	1f320ac61af709e5a7b2efce2ff5b381d8723a1c84cea9e6d197bc49dea38651
SHA512	d9f61f03341bc8d7093fed34ba7b591e6cae11b14c68b33dda9b0837b8b2b7d1f46dc693a09f119a623b9304de268ea90d120498a040ca7220c0e2fdae98a5b9
Ssdeep	96:rWCY9cShR1or6NJSzi6+Ujsev0TnImUVcdq56iGyQ2/S9l8W:qjiShRUYjqb+UoSMe6Ty0OW
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

PopAd.dll

文件名	PopAd.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\PopAd.dll</li></ul>
文件大小	147456 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	1a36f21ad47b2495ccb28ac56912908b

SHA1	1b1132b1f8f1451c6f1cd76c9c0de5a342893dcd
SHA256	b7131f56d0f072cae4701e56a6701f32c1909c2d283899181d9fd49a2b5bdcc2
SHA512	83891a9220c76814d28abd5a4f7cca50b715d9e58236809aba0aecd1af6cfd1c06931b4a2a4fef5b04d8cb459e2e05dcf2ad13c6145ffc74f56589419b325c8
Ssdeep	3072:DrnDWtw2BojN7gxzki38xH+LsTzPRvx+SoFI8Epbll:DDKtw2BoxL+SoFI8O
Yara	<ul style="list-style-type: none"><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

NewPhone.dll

文件名	NewPhone.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\NewPhone.dll</li></ul>
文件大小	565248 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	09af2ba254f56c3ac2538647890fdf90
SHA1	65cc1faab75e0118ab4bb18ef7974bc752be90b3
SHA256	c164a5e9da39b48cf235ceaa5c1fb881742da8a53c65fb0c134e511638c05453
SHA512	3ece13b6a5a78302e368e2c115b3eeb6368acb208ded485b334e5018ce4fd14ebe3bb6ec55959efc2489c205f232936579b1949ca3f947022838e14066ca4f48
Ssdeep	12288:kdP+yZKh8lG4iB+rEo4lWYNjJbYtdnpWh5C:kdWyZKh8lG4iNblFNjjiH8lC
Yara	<ul style="list-style-type: none"><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

SFU\_Recode\_Dll.dll

文件名	SFU_Recode_Dll.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\SFU_Recode_Dll.dll</li></ul>
文件大小	331776 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	b7878d09372af179272e5a42402f10f1
SHA1	b177384d3d5e1eaae06a330149283ee328b90407
SHA256	158217d69dc1e627fa2f044c5476f01c3c6dc4ce0f98b9848580bd10eb928d82
SHA512	5ece91e62214713747954d250caad1cf66f5bc2a0224ca36ba0f33203dbdace27ebd10eb2eb1895cfb9f9edfdf959a2215f4d94f4a4ab095d52b0e8e63f0a8dc
Ssdeep	3072:M0ZigJ8CixeR/qCX5kdje0t4Hoq2Q3j0uWu/IFerpu+ldFx:M1lcEVqCX5lJe0bu/7Vbp
Yara	<ul style="list-style-type: none"><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

key.dat

文件名	key.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\omuibisy\key.dat</li></ul>
文件大小	80920 bytes
文件类型	data
MD5	8ec6e61406bfcca3dcee85ab6636192b
SHA1	4017216b07af1025e0486b94d62eb5e72835c543
SHA256	7b5b581b2afd5633699ba21490a342b8d758cfa354b06adc037323c5a0e6c389
SHA512	c0a60795aff551432129c2ffd8b5b4a22286febe4947b57d3d90f7ff19eec75045a02e6ea9a7539eaaba9bad3f85cdc58615401e83e8f06694da3dfe3cfbd63d
Ssdeep	1536:etrmwgUBi0wFxdlroyKaEj7tamCUp9cGXltj6yUftoaKlEi01uT:eIC0j8yKZEmh7j6yUFMi00T
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

LoadHook.dll

文件名	LoadHook.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\LoadHook.dll</li></ul>
文件大小	712815 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	3956e5547ad36240e71a346cde5c597

SHA1	163e2d21641a75d7c37142c6f637c143c1d9c3ee
SHA256	50d953d9f32aa14b9d0fde381c3b0f2e679e6e3dde6a259368e54999faef7427
SHA512	89c483c566e0aec96955e0efff855e406ed5d4c1fbe1b2c579cdbbeaae3c1ae236c9243f1b2ae2545a1728b74ffdc7cecf3eec55b8dbdfed12af7d74c1806158
Ssdeep	12288:DuAb6Zlvi2+heL+h4SyDxSog4gkTPxAVhnbKL:DuAb6Zlvakqh4/xSohgMxAVhOL
Yara	<ul style="list-style-type: none"><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

WyAd.dll

文件名	WyAd.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\WyAd.dll</li></ul>
文件大小	188416 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	e11de3f332e05632ea53f45ddb91d119
SHA1	399736eb067714985c4efad4de2332ba25253944
SHA256	9a366fcd0a36c025401e92ce39615faad1449c980fb3b5f59cb9862b8abc836
SHA512	69b2c13c5cfd45c166e260027aa800f99663b61e958cf0e1bb41565cd1e85df1453f80d76307926082c545152591e2d3e14ab002f5270f517f076dca20814fbb
Ssdeep	3072:oc3LCSdQ9+axanLcuNOV0jTn/SoFIE749DRYQy+H49iz5svPRI5A0CE0:j7CuQ9+axa3T/SoFIEMRRYQyM49izGvG
Yara	<ul style="list-style-type: none"><li>DebuggerCheck__API ()</li><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

devdata.ini

文件名	devdata.ini
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\devdata.ini</li></ul>
文件大小	21 bytes
文件类型	ASCII text, with CRLF line terminators
MD5	956230fb0a4ad46db83cfb118a21de2c
SHA1	e055897aacb97ee9b86f942440980fd375b247b8
SHA256	925d1d6c64332901bca702a4bb4431528812c8072c7df6e681094fdc5e41ec0f
SHA512	1038ef0fe51b9a25bf8d2add6559cd2469de7145cdf25a5ce89f48bb853324ea551d10e331bae6b48691456d490d7fedc4e595facc4a96b4b0377c039ec51b95
Ssdeep	3:LqS:T
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

AdKernel.dll

文件名	AdKernel.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll</li></ul>
文件大小	294912 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	fab6ef45debd0781a96d255d7c6ffc0c
SHA1	5b4f52da1c1dad9898a36aabcd025b0ec428384
SHA256	28f0fed7d0650456635726303847ec7580e91fdfae509b6a1bd9afd75e52018a
SHA512	dfd284bdc3f3da416ed1c630f4a32e728e93511d664cb6a1ee19e112b936be40264bfad6411b2364edf809d93a63a8e8fc434b7897d9a675b944cd36ed4311f7
Ssdeep	6144:EX11qBzEjYx6Z457/IG46bhfU7cSoFlpS7FYMQL1gk9y4QOzoijsOfIUeh/:81UZ6Ze7/IG46V7qPZLb2h
Yara	<ul style="list-style-type: none"><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

desk6925031.ico

文件名	desk6925031.ico
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6925031.ico</li></ul>
文件大小	16958 bytes
文件类型	MS Windows icon resource - 1 icon



MD5	422c831ad4ba00d9b5c6134e38291103
SHA1	58cde18837dbd5b6b0f9c4494028f385230b8f80
SHA256	ed439501a9f6bda5281a5c9695260487edbae27b35734c85295fe20a82f0361f
SHA512	36afbdafd8f16f4f9d14d4bb65691bf86cd71442a907fe3256770fe6684a84511492e0902f5ed2dc1ddd10cfc5bfaee9614d763fd56e8cff71fcc863fe1d6725
Ssdeep	384:wiRiM:xWXqpPtZiyfpN5UGEFMx
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

run.ini

文件名	run.ini
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\run.ini</li></ul>
文件大小	78 bytes
文件类型	ASCII text, with CRLF line terminators
MD5	49b765000e7b85be1c1056205fb7c435
SHA1	fdc592f1e49d8cc21b59dcd7c8d9a36384835e98
SHA256	2ca0d6040e28d751422e9ee1c1b8f7650d8b48ab93d9ee10ecb01a33b16afb12
SHA512	195d48805820adb8db32648787abe1feec52049c8fe99028239882c6625331ce45861bda46fe66119d670a17eb2626e88b62db1d5f7677736ed7ec2bbb485cbf
Ssdeep	3:se6AvVKwfBlmWfkiE2J5xAIlsORy:T6CfCm+kn23fiY
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

CIBSTATIST.dll

文件名	CIBSTATIST.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\CIBSTATIST.dll</li></ul>
文件大小	71168 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	368f4d0754d671fad3d9eac6b1790b78
SHA1	e6b7f359839ee96b5f8245246dc61e5b796b22f3
SHA256	30709429ced2866b193c5ffe2d2001040d6ea5708f4c712e7bd06f1cc8d83fc8
SHA512	e39974654803f50d3091cd954f6dc1c2d88b6bc65390b0cbace15c654364b466331613387cf043ff308857c23126072b8c22798af7e17531e9882e6cf3fcd40c
Ssdeep	768:S07u5ymE2fqSdYY6DNNwEIrtpZYIEIf2bBtQBtjb4yJMXLoyhvnYPpvN2lED0QT/:SqYycqSdCcElpqzFBpb4oMEOSsQpMca
Yara	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

inject.dll

文件名	inject.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\inject.dll</li></ul>
文件大小	311296 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	8acfbcb44e27a9595e8f6891f93329f59
SHA1	defbebb21ab66286c291a218943f9ad795501415
SHA256	ce7a88a05da9980f920aba03c10b8e2e50b7ab988b974949caa1ae19185929f6
SHA512	e18fdee5ef8f0b32771f2124e4249874195552dac914ee693a24a8dd18b8f0879ea809369c13b1add67b4779a7a19e29aa149dd6af388a0540fa24b6616ecdae
Ssdeep	6144:wwP1zCHZ2NmhpXQoJq3qfXhSsAnGfrkkkkkkkkkkkkkkokkkok0kkkkokkkkX:wGCXpXxqYnGfrkkkkkkkkkkkkkkokf
Yara	<ul style="list-style-type: none"><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

yfudjsrq.dat

文件名	yfudjsrq.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\yfudjsrq.dat</li></ul>
文件大小	80390 bytes
文件类型	Zip archive data, at least v2.0 to extract

MD5	e15439d34cc181088fd0b7ad9b69e447
SHA1	16830901407ab29bc105078461d407ab2c0c5abb
SHA256	912e913be3f44e09f3bb7339e1305624d1b42dc72ba0573b79edeaf4ca2bb9e4
SHA512	91e6457f2ce045da370946ba9b0a8a541f0eea6c76c57880f9158558556ec0e837d14c88541fc572e100fb459564035d30958689b5d225fee6204f689aab5e
Ssdeep	1536:NCu9zsj8h2hPJOFwC9KThLDo8AOovILSjFJOJTSvfz4/LVgfn97txORDhZS:NzsjKoFwzhLMW0jFOjsfz4TWNFORBS
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

nfapi.dll

文件名	nfapi.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\nfapi.dll</li></ul>
文件大小	126976 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	e9563b56e4c5c190b003eb5bd3b42d5d
SHA1	4d2af7f323835946ecc4369ff9f95fedc59be0b
SHA256	51c673655efa9949e6f30e99e3cbf73b2472d92b6e0443cb852add0047f6526c
SHA512	11c5711448397f8a7961e60d7cc27f96b37e7a78cee86726f21ed206c650a2e9392d1ee2b832016c2e96a723fa8397534fa813b45f5e75faf7a294f302fdc55a
Ssdeep	1536:qgsjVf2oWZ8UrCdXXP7g6QaC1zxXPqRY1fNP0E1nCGBWYmwUtUluaFLT77mwg:qV34OUrC5MnL6wWYm9tWF0
Yara	<ul style="list-style-type: none"><li>DebuggerCheck__API ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

zbgqtqbl.dat

文件名	zbgqtqbl.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\zbgqtqbl.dat</li></ul>
文件大小	23 bytes
文件类型	ASCII text, with CRLF line terminators
MD5	2d93dc5cb1f0d6431f57c8464adf9302
SHA1	36caac532a5cc18c5ac58ee58db103d58493839e
SHA256	9332621b1409a53e285a3d9592098542079a3506f25b54b7355b6866184c4d79
SHA512	5c13352189cf1c746bcf3263cc02500424da377e4ac14e646b1be968f2c1a581259091a52d6d169e1dea059abeb9949a91b7e4d4b6ec9b4e80bb41c9f76a170
Ssdeep	3:ThhhpL:t3pL
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

yun.exe

文件名	yun.exe
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\yun.exe</li></ul>
文件大小	56320 bytes
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	fb24e1bd570f14b16f2787668a37f5a9
SHA1	76a31eb2a7b79952b498ae5b69d082c7f98069e2
SHA256	083c0542c2781a2e255ce06bee40a6509e32ce8e8afe0084e9de762d57abfa9b
SHA512	cbc535eee6ca55082cadd90195d54f6e1bedbee15541cd2274d215045451617a2277b03e3a1bb1fc03412504524780edd1824a5a1cc887df4e5574e246fb00cc
Ssdeep	1536:Fpyt2p3meEZKlcs3q7n2eWPwlBhUiY82jfQ46bMwluyWNV3:F4t2gQLcn7nxBhUiYfjfQ4+lubF
Yara	<ul style="list-style-type: none"><li>ASPackv212AlexeySolodovnikov ()</li><li>ASProtectV2XDLLAlexeySolodovnikov ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

fimxgoep.dat.crc

文件名	fimxgoep.dat.crc
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\fimxgoep.dat.crc</li></ul>
文件大小	24 bytes
文件类型	ASCII text, with CRLF line terminators

MD5	cf07938c2d548fe80168689f822d75c8
SHA1	d4ae68ea51dd7971f46fe90961e62caa9af50bc7
SHA256	09ecbbc77ca28aec12a2f54ad5763325f2db9d3b9b061fb86e0904d29331bfde
SHA512	822d4641818cc25bd197e50096d5a9bf2d517c1b877f0b05b2f08eefa7819905b2b564a3c8a5258cef281bc542b951d0a4c788391588bdc6b287cd93e1d3d76e
Ssdeep	3:TRJF:R
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

DeskTop.dll

文件名	DeskTop.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\DeskTop.dll</li></ul>
文件大小	499712 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	6547b79438efa6af2e1f91ef3a741806
SHA1	3478574ea4a8f381903f555bcec96d7649fa233c
SHA256	d9f6913e1b31db1c941258057cd8513c6e690cadeab03c372780e1ef11c7bf82
SHA512	d7c57a16dea72a5cdf4d2ddfa1146848a6acd243b37e20ee98a4870a72baea2474af4c64cc40e14351fe1476ba25737e0acb1cfba7995668b26614d4d4b33c9
Ssdeep	6144:/xjmermBtsxeO9ifLFSofI0td6zpQhtpVT5ZTJAlwKlrETpd5h5ZSenZX4jQCTcX:/8W0O0udQz55IYb534jfq/
Yara	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

api32.dat

文件名	api32.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\api32.dat</li></ul>
文件大小	53248 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	7ff288ddcb25228421fbe92bc281848c
SHA1	3c0a552b5ce1c0db0cff4cf29802e0a76167644
SHA256	7af53d0d722fe06117fe1080bff5ebc8b2fc8b9226fcee5b13e7d650e7af54c
SHA512	7bdc00e2648ba2756a9e8b09c7ca9b9a99c3435ca9c4411d99f9bb70b652e404c04455558fb3306c4ca56bab2d61802e689b44d75af39e46dd42ba3b70169604
Ssdeep	1536:ew/Hcjnf+sKwidky+c0NUcNYAutQBMBVRhK5:eC8jWJwidZG NUeutQBMBVRhK
Yara	<ul style="list-style-type: none"><li>Check_OutputDebugStringA_iat ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

fimxgoep.dat

文件名	fimxgoep.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\fimxgoep.dat</li></ul>
文件大小	1965056 bytes
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	a7f404acadd9224c8d744d87b4d774bb
SHA1	d0ef9bdfd31c8dd03a196e8d89ea7d2f14849910
SHA256	ab344b7a0fcbddcd922c00a74f0bc272e4e02bd691577809d8829e76910d4619
SHA512	8246a94b4213e1161ce1885c8498f5ad8d4c177eab0831ee73de2dc1d54d6bda304794da2ef7071e69758813103623f9391eb9da7a116a64653a4f6302a0e7ce
Ssdeep	49152:iGmcfKXI0Lkb5H8cyFwCae8lr3gv21Qq2sev:TqkNrySCaebQvw8v
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

pop.dat

文件名	pop.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\pop.dat</li></ul>
文件大小	16937 bytes
文件类型	data

<b>MD5</b>	4752435376a58d8886b8764082e0c60c
<b>SHA1</b>	bdfcaf6415e8e55bb5017e0275c78d7e386f6f2e
<b>SHA256</b>	f3e74dea1e3a52abde2589e6dd266a21172a14f1fc4fd81a4312987ce2701f13
<b>SHA512</b>	a78b26edbbdbc233256c5a9767d6982c42291103e81b4c3b421ae2d2f59aa7eb1adf29d08362f6d5c7deb bc4dd21cf236a01b0a0645ed8244a41d62916b8c734
<b>Ssdeep</b>	384:wpmRnZKDnLcT2DIC5aKcJsBA3WMsdxrKfax+RvWJc8u8:zRoDnL0ms5FcGMEdxrKfaYvWJcJ8
<b>Yara</b>	无匹配
<b>VirusTotal</b>	<a href="#">搜索相关分析</a>

export.exe

文件名	export.exe
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\export.exe</li></ul>
文件大小	69632 bytes
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	d38d8ab692d9819f152941e4806de7fc
<b>SHA1</b>	363cf945904a59ae09f9ef1b39596dc9addf6264
<b>SHA256</b>	cc71854fca7bfe952be2a1d655505925b16651f04c09cf8fb7206d82a5048923
<b>SHA512</b>	8d37bec046439212ace631b2b3c0d9f5c3573ca04ae6252cc3bc05c295a0f5103330b17e7130a3f2a5e0db594356e834fbe192848fbcefb d45d890ade2c c56c7
<b>Ssdeep</b>	1536:gdGQdLR+uOycfmjAcj9cmlG4tQ4KZSZAN+myN5kPgh5io:7QVR+uAmjAcj9XIG4tQqqN+mY5Vh5io
<b>Yara</b>	无匹配
<b>VirusTotal</b>	<a href="#">搜索相关分析</a>

tips.ini

文件名	tips.ini
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\tips.ini</li></ul>
文件大小	40 bytes
文件类型	ASCII text, with CRLF line terminators
<b>MD5</b>	319e308d0da13a2372f943c765ed193f
<b>SHA1</b>	14a72d3468b7a8fd555170f8dd3eb073ff9fab95
<b>SHA256</b>	2f46bea89309090e3a8e86d63193bc13ae1b84108e5d1a0f293f1620cccd e5b4
<b>SHA512</b>	7f3048fcb6c12b80230a8e97cc6f3811b886408ed5cab40fe613a469fe394916ef07b32c0ed58a785ad12faa475853cc21159ba9e6b3a1c3c923a9c23e85fafa
<b>Ssdeep</b>	3:K30ciOjcc:E0YJh
<b>Yara</b>	无匹配
<b>VirusTotal</b>	<a href="#">搜索相关分析</a>

NetData.dll

文件名	NetData.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\NetData.dll</li></ul>
文件大小	585728 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	ba5bceef3f1a2c3d44f444674c51c9d5
<b>SHA1</b>	f45130c99bd1e97f8cfea7b54d325b999fc6272b
<b>SHA256</b>	93b69dbc6e6aa6a976cd94014e72a07c930103dc8bfb9127b4311c0a83bc3134
<b>SHA512</b>	9803961fbd687eb1338d0881e06b1e28c8b1f9f10cdca5f7f535631980c865509648e5b1074efcb b789be1f4220cfa12648a43d37c04369a144c70b9cc1c 7b29
<b>Ssdeep</b>	12288:iqJZh8ydmqyzql6XuWpRECsAj d76umuV3al5:i6Zh/LXuW7bfjd2umuV3al5
<b>Yara</b>	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li><li>ThreadControl_Context ()</li><li>Armadillov1xxv2xx ()</li></ul>
<b>VirusTotal</b>	<a href="#">搜索相关分析</a>

ihgjzvum.bat

文件名	ihgjzvum.bat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\ihgjzvum.bat</li></ul>
文件大小	135 bytes

文件类型	ASCII text, with CRLF line terminators
MD5	19e45f19f35ad427e7ea09a112af973e
SHA1	7f9d1b439ac69490bb28a23a1f9403a545c80a74
SHA256	777615c1862489f68ff02cd5f80c5e1afc99f6256678272a3c1dd8a6721ec6a6
SHA512	5b3c9ef4f9cc13cb58ca0a42585bb744df90db29b5261c8815886cf02da2cf18e467ef3afdb197f7f39c3e8f29dc6ba64463d6ee3dba2571498fa48395df3eac
Ssdeep	3:mRoiZOmWfkiE2J5xAlcVK+bMD2UmWfkiE2J5xAlcVK+1KRewWiwF:mRoiom+kn23fkRMD2Um+kn23fk70WiwF
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

AdMain.exe

文件名	AdMain.exe
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\AdMain.exe</li></ul>
文件大小	40960 bytes
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	1959b6546fbcd0f9da2f32182ceea73
SHA1	6018b5463ddfd3f22799f37d51f4905e0dbbbe45
SHA256	cedd29088e17bbce0e5e6136c32e466d3b9fce4a1e7b6a21c8703ae0db2afbd8
SHA512	3518d45f0f5cd2701409961b3db2cabce6641190000798676d5b5b8dce76e7461b3163e9b3a0f5e20830944bb150fa6afb460515182871304f26eee5e37be4308
Ssdeep	384:EDisoYDHE8XvFaG9topkdUkXCmeuOyUu/CFMtBKCC5I3q:MNEcFlfxSJJMtq5I
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

weifileconfig.ini

文件名	weifileconfig.ini
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\weifileconfig.ini</li></ul>
文件大小	117 bytes
文件类型	ISO-8859 text, with CRLF line terminators
MD5	69400af0f6ef19cecbf36a57440a8466
SHA1	cb104bc1b711dc5ec1dda53794f450a2d6abf883
SHA256	fbe939a8e012d2131d69a7d8934fc55600f8855bd868426609ca8e95f348261a
SHA512	274768fcb22c779a4edd66e85befb9e15ffa04d903950cd347e9d5baec909ca20593fa49d18be9316f4086282dc027591725a35fb4da6856cdef8bbbbbcdbe99
Ssdeep	3:1WtAOEOGqZJl1p08MLWi4HlvYKkmTnsUIULACSXnlvDLV:1WiOvOq2Jlp08MLWi4HSj/n7lUY4vF
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

desk6423780.ico

文件名	desk6423780.ico
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6423780.ico</li></ul>
文件大小	15086 bytes
文件类型	MS Windows icon resource - 3 icons, 16x16, 256-colors
MD5	e3bcb5274abdba3a562bb4ce5d00eac2
SHA1	64cbf1a1f11af318f1fd158e4358a89a8f708ee8
SHA256	250344a6a8b6bf40a87312512b2ea4e120f4475778a09a756f5e766ec171baed
SHA512	b4e09a71c6203884443c0ae9d75b8040dfdb5b06cbf8c26eee93fba628996ab19b9274b20cc5163d0d74af0ab9aad8400de45eed2e323b5321104a74c5eade2c
Ssdeep	192:7rj7P5OXJFYMITmTK75+ZZ8G17Gnd5qsBKxXY4e2JvNi+s92lJjG+xs4zv4Fol3:PSISE5u8G17WjBKCSJ5/s1ST4LFurT
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

flowdatadll.dll

文件名	flowdatadll.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\flowdatadll.dll</li></ul>
文件大小	1241088 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

MD5	2ee6f179314d01a0c97522bbb1c836cc
SHA1	2fa2ee2f4dad09213da0ebd5f90c5ce83f099522
SHA256	1a81160a9b33d5680b837c0b4216b23872e4e65b736df7f766bd87dd5b573cb8
SHA512	1c6abf055245737b205d3a8e9562e8718d37d41d72442174ecdc84b9295bb39afe718656ff3984a7df0b5db3fb7820793cca60766bd74181382fb6a8a50effda
Ssdeep	24576:Fy8TraFljZwWXPDycEBVbjdw1R56rfA75Mc6gA164AxrRoqo:zraFRZVXJ1nc+4xq
Yara	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li><li>MD5_Constants (Look for MD5 constants)</li><li>NET ()</li><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

422E.bat

文件名	422E.bat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\422D.tmp\422E.bat</li></ul>
文件大小	400 bytes
文件类型	ISO-8859 text, with CRLF line terminators
MD5	e0ce189cc540f05eb8bd7baf40a39970
SHA1	b262b179be81774b5d89822258095bece9f59123
SHA256	da7e11c197c06fb71052403d4684cbb6d8523edb492db7a44e7e429960f91f0c
SHA512	72e3023debdde049b3cfa509735c7d74a68bc35679b1c9dcc6724197ee46df5b08a85b650fea14f58c85a961b1b47ecd696e339a20c8e5e21167c87d7ae9b68b
Ssdeep	6:NAD9RXE29CcF95btFiezH1fKvDzwAJAOsF954Owe/btiRtiD5IhDojGkbW+9ReAG:NALFXaSK7zwAvk9weDkCDWk8UJRW
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

cdd.dll

文件名	cdd.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\cdd.dll</li></ul>
文件大小	139264 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	87c21dd678fb7cc2bc4381831ee0f4dd
SHA1	169f4c037442baa70a86e80a10cc20bff635819d
SHA256	e5ef21a415606afdbe7400280393860f8b6811666a9259dac84e8e0482f4a7aa
SHA512	c0614d08bce28bea31c1c0ee9c7957ccc9350e189361a6ccb61344e6e11401ea023d55a70810e0b36aee8be11cf85a36d3bdb2ff97b6dbd1f71119ad3016b41
Ssdeep	3072:dNiruylo7A9PJrNlKgC8jWJwidZGNUeutQBMBVRhKMU:dQNoaMmjwdBVRh3
Yara	<ul style="list-style-type: none"><li>Armadillov1xxv2xx ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

Hijack.dll

文件名	Hijack.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\Hijack.dll</li></ul>
文件大小	421888 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	12c2be55967eec5a8f6c2f884768dda7
SHA1	80e9b0f1005f121a241527f93510cd7ad9cf4b3a
SHA256	603208a00ae5f21a970603bb9b11ca928bcab43c7a6cd3de56ee31dd40d26a5d
SHA512	1fc8c0dc770e38f6c402f388bc67c5709370a6bfd55e5fea778c049f5dfb85501ccf5a92e9458cca5a7300b73f84cffd3a17cc37efc21e89f1e5f7a705eb649
Ssdeep	6144:iFw0sTxnhkhuZfQxSQjVT3F/dD/yIFo4FdnH3i83/luxdVwT23tc:is8uZlXSQ5TRdD9H3Nvlfwt
Yara	<ul style="list-style-type: none"><li>DebuggerCheck_API ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

trjqhbuq.dat

文件名	trjqhbuq.dat
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Local\Temp\trjqhbuq.dat</li></ul>
文件大小	3989226 bytes

文件类型	Zip archive data, at least v2.0 to extract
MD5	7915eb907a92dd372a600396211129cd
SHA1	e279cd8f4dbc46c0a2f14cac7b66252d463e8a64
SHA256	8abebe2f9796d922aee2a9cfcdd36c80bfaca2fdbf977e516598f641c6d4bc
SHA512	016f47e5a7b2afd2b9d2de42c58b4c455a4ff7c0fa46885c758e59e60c39d7ca809c16db457215c117f4a45501b7695466875d4e752682ff2ab9f4db705c7f31
Ssdeep	98304:cnCF6ay7lccrMwH0/3qD23EWF3AiQAAQlhkfj:cCF69lrHlqD23inAQlhC
Yara	无匹配
VirusTotal	<a href="#">搜索相关分析</a>

devdata.dll

文件名	devdata.dll
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\devdata.dll</li></ul>
文件大小	1190400 bytes
文件类型	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	6411e0b6eaefbbd970036c55417f55d6
SHA1	f64cd6079c6f3c85f5349a9eb401136956e0e561
SHA256	f3234969284aae1830b3087529bc9acb0f7191de7ffc3dee041e49b1543e4e4d
SHA512	4fac5da6d84692bf3d812d66d1350d242cd56b092157ae5d913b0de6c8316afa59ef4f72d9a6c102bd9aad044c35f31f5186b1fe4a0428cce2953676ce12673b
Ssdeep	24576:k/moTwi4pD7ltdeBpNcmzE81yBmWjloqYDdVSTlZjGylG4cb:keoTwi4pD8tdeBLF1yBsYDdVI7IG4cb
Yara	<ul style="list-style-type: none"><li>DebuggerCheck__API ()</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

runhome.exe

文件名	runhome.exe
相关文件	<ul style="list-style-type: none"><li>C:\Users\test\AppData\Roaming\hgpylpin\runhome.exe</li></ul>
文件大小	939008 bytes
文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	ead6e7242c936aa5edf862fce56cbaec
SHA1	ddc8e27855d92c013f47f7eb46f7817d7716977f
SHA256	33b7c137cfe969f6c5f93f3b8ad40c4bf57640c4984da89ce7c977096fade154
SHA512	7901193f2e672dc054129adc8e8a18698bd9b65b570d9703065714a17e3de8053a000b8e2b2970f793aca7929f1b40189c4566ba391c79808d4388efe03b1062
Ssdeep	24576:V7ocjCVFfqZrLoINgcfnN+xq4OJh4XFgT4n0r08u:V7G4HT2nN+xq4acCTc02
Yara	<ul style="list-style-type: none"><li>DebuggerCheck__API ()</li><li>DebuggerCheck__QueryInfo ()</li><li>DebuggerException__SetConsoleCtrl ()</li><li>Check_OutputDebugStringA_iat ()</li><li>MD5_Constants (Look for MD5 constants)</li></ul>
VirusTotal	<a href="#">搜索相关分析</a>

行为分析

<p><b>互斥量(Mutexes)</b></p> <ul style="list-style-type: none"><li>Local\ZoneAttributeCacheCounterMutex</li><li>Local\ZonesCacheCounterMutex</li><li>Local\ZonesLockedCacheCounterMutex</li><li>IESQMMUTEX_0_208</li><li>Local\ZonesCounterMutex</li><li>Local\!IETId!Mutex</li><li>DBWinMutex</li><li>112EQAD</li></ul>
<p><b>执行的命令</b></p> <ul style="list-style-type: none"><li>"C:\Windows\sysnative\cmd.exe" /c "C:\Users\test\AppData\Local\Temp\422D.tmp\422E.bat C:\Users\test\AppData\Local\Temp\waiting.exe"</li><li>C:\Windows\sysnative\cmd /c "C:\Users\test\AppData\Local\Temp\422D.tmp\422E.bat C:\Users\test\AppData\Local\Temp\waiting.exe"</li><li>timeout /t 3</li><li>.\export.exe</li><li>timeout /t 0</li><li>"C:\Users\test\AppData\Roaming\hgpylpin\Admain.exe" export</li><li>"C:\Users\test\AppData\Local\Temp\ihgjzvum.bat"</li><li>C:\Users\test\AppData\Local\Temp\ihgjzvum.bat</li><li>C:\Windows\system32\rundll32.exe "C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll" MyStart</li><li>C:\Users\test\AppData\Roaming\hgpylpin\RunHome.exe</li><li>C:\Windows\SysWOW64\svchost.exe -k netsvcs</li><li>"C:\Users\test\AppData\Local\Temp\cugfljnk.bat"</li><li>C:\Users\test\AppData\Local\Temp\cugfljnk.bat</li></ul>

- "C:\Windows\SysWOW64\cmd.exe" /c netsh winsock reset
- cmd.exe /c netsh winsock reset

创建的服务 无信息

启动的服务 无信息

进程

**waiting.exe** PID: 2620, 上一级进程 PID: 2992

**cmd.exe** PID: 2744, 上一级进程 PID: 2620

**timeout.exe** PID: 3020, 上一级进程 PID: 2744

**export.exe** PID: 2836, 上一级进程 PID: 2744

**timeout.exe** PID: 1992, 上一级进程 PID: 2744

**timeout.exe** PID: 460, 上一级进程 PID: 2744

**timeout.exe** PID: 3012, 上一级进程 PID: 2744

**timeout.exe** PID: 1948, 上一级进程 PID: 2744

**timeout.exe** PID: 1204, 上一级进程 PID: 2744

**timeout.exe** PID: 1968, 上一级进程 PID: 2744

**timeout.exe** PID: 2052, 上一级进程 PID: 2744

**timeout.exe** PID: 2204, 上一级进程 PID: 2744

**timeout.exe** PID: 3060, 上一级进程 PID: 2744

**timeout.exe** PID: 1140, 上一级进程 PID: 2744

**timeout.exe** PID: 1664, 上一级进程 PID: 2744

**timeout.exe** PID: 2812, 上一级进程 PID: 2744

**timeout.exe** PID: 2912, 上一级进程 PID: 2744

**timeout.exe** PID: 1304, 上一级进程 PID: 2744

**timeout.exe** PID: 544, 上一级进程 PID: 2744

**timeout.exe** PID: 548, 上一级进程 PID: 2744

**timeout.exe** PID: 976, 上一级进程 PID: 2744

**timeout.exe** PID: 1360, 上一级进程 PID: 2744

**timeout.exe** PID: 2100, 上一级进程 PID: 2744

**timeout.exe** PID: 2104, 上一级进程 PID: 2744

**timeout.exe** PID: 2688, 上一级进程 PID: 2744

**timeout.exe** PID: 2764, 上一级进程 PID: 2744

**timeout.exe** PID: 2868, 上一级进程 PID: 2744

**timeout.exe** PID: 1820, 上一级进程 PID: 2744

**timeout.exe** PID: 2036, 上一级进程 PID: 2744

**timeout.exe** PID: 752, 上一级进程 PID: 2744

**timeout.exe** PID: 2292, 上一级进程 PID: 2744

**timeout.exe** PID: 2588, 上一级进程 PID: 2744

**timeout.exe** PID: 1708, 上一级进程 PID: 2744

**timeout.exe** PID: 2948, 上一级进程 PID: 2744

**timeout.exe** PID: 2896, 上一级进程 PID: 2744

**timeout.exe** PID: 1364, 上一级进程 PID: 2744

**timeout.exe** PID: 2428, 上一级进程 PID: 2744

**timeout.exe** PID: 816, 上一级进程 PID: 2744

**timeout.exe** PID: 2524, 上一级进程 PID: 2744

**timeout.exe** PID: 2476, 上一级进程 PID: 2744

**timeout.exe** PID: 792, 上一级进程 PID: 2744

**timeout.exe** PID: 1180, 上一级进程 PID: 2744

**timeout.exe** PID: 2016, 上一级进程 PID: 2744

**timeout.exe** PID: 1568, 上一级进程 PID: 2744

**timeout.exe** PID: 2288, 上一级进程 PID: 2744

**timeout.exe** PID: 2864, 上一级进程 PID: 2744

**timeout.exe** PID: 2168, 上一级进程 PID: 2744

**timeout.exe** PID: 2832, 上一级进程 PID: 2744

**AdMain.exe** PID: 2900, 上一级进程 PID: 2836

**cmd.exe** PID: 1436, 上一级进程 PID: 2836

**rundll32.exe** PID: 1268, 上一级进程 PID: 2900

**timeout.exe** PID: 2664, 上一级进程 PID: 2744

**timeout.exe** PID: 2556, 上一级进程 PID: 2744

**runhome.exe** PID: 2540, 上一级进程 PID: 1268

**timeout.exe** PID: 2080, 上一级进程 PID: 2744

**svchost.exe** PID: 3224, 上一级进程 PID: 580



#### 访问的文件

- \\Device\\KsecDD
- C:\\Users\\test\\AppData\\Local\\Temp\\
- C:\\Users
- C:\\Users\\test
- C:\\Users\\test\\AppData
- C:\\Users\\test\\AppData\\Local
- C:\\Users\\test\\AppData\\Local\\Temp
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp\\422E.tmp
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp\\422E.bat
- C:\\Users\\test\\AppData\\Local\\Temp\\export.exe
- C:\\Users\\test\\AppData\\Local\\Temp\\423F.tmp
- C:\\Users\\test\\AppData\\Local\\Temp\\waiting.exe
- C:\\Windows\\sysnative\\cmd.\*
- C:\\Windows\\SysWOW64\\shell32.dll
- C:\\Users\\test\\AppData\\Local\\Microsoft\\Windows\\Caches
- C:\\Users\\test\\AppData\\Local\\Microsoft\\Windows\\Caches\\cversions.1.db
- C:\\Users\\test\\AppData\\Local\\Microsoft\\Windows\\Caches\\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db
- C:\\Users\\test\\Desktop\\desktop.ini
- C:\\Windows\\SysWOW64\\propsys.dll
- C:\\Windows\\sysnative\\propsys.dll
- C:\\Windows\\sysnative\\cmd.exe
- C:\\Windows
- C:\\Windows\\sysnative\\cmd.exe:Zone.Identifier
- \\??\\MountPointManager
- C:\\Windows\\sysnative\\cmd
- C:\\
- C:\\Users\\
- C:\\Users\\test\\
- C:\\Users\\test\\AppData\\
- C:\\Users\\test\\AppData\\Local\\
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp\\422E.bat C:\\Users\\test\\AppData\\Local\\Temp\\waiting.exe
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp\\422E.bat\\
- C:\\Users\\test\\AppData\\Local\\Temp\\422D.tmp\\
- C:\\
- C:\\Users\\test\\AppData\\Local\\Temp\\timeout.\*
- C:\\Users\\test\\AppData\\Local\\Temp\\timeout
- C:\\ProgramData\\Oracle\\Java\\javapath\\timeout.\*
- C:\\ProgramData\\Oracle\\Java\\javapath\\timeout
- C:\\Windows\\sysnative\\timeout.\*
- C:\\Windows\\sysnative\\timeout.COM
- C:\\Windows\\sysnative\\timeout.exe
- C:\\Windows\\Globalization\\Sorting\\sortdefault.nls
- C:\\Users\\test\\AppData\\Local\\Temp\\1.txt
- C:\\Users\\Administrator\\Desktop
- C:\\Users\\Administrator
- C:\\Windows\\sysnative\\zh-CN\\KERNELBASE.dll.mui
- C:\\Users\\test\\AppData\\Local\\Temp\\2.txt
- \\Device\\NamedPipe\\
- C:\\Users\\test\\AppData\\Local\\Temp\\3.txt
- C:\\Users\\test\\AppData\\Local\\Temp\\config.ini
- C:\\Users\\test\\AppData\\Local\\Temp\\data.ini
- C:\\Users\\test\\AppData\\Local\\Temp\\trjghbuq.dat
- C:\\stop.txt
- \\??\\Nsi
- \\DEVICE\\NETBT\_TCPIP\_{33E35B0A-D1F6-4AB1-A1AE-56B8A256B787}
- \\Device\\Afd\\Endpoint
- \\Device\\RasAcd
- C:\\Users\\test\\AppData\\Local\\Temp\\zbgqtqbl.dat
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdKernel.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdMain.exe
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\WyAd.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\DeskTop.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\NewPhone.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\devdata.ini
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\devdata.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\yun.exe
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\runhome.exe
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\home.xml
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\Hijack.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\NetData.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\CIBSTATIST.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\weifileconfig.ini
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\inject.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\tips.ini
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\LoadHook.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\SFU\_Recode\_Dll.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\cdd.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\PopAd.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\pop.dat
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\flowdatadll.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\nfapi.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\ProtocolFilters.dll
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\run.ini
- C:\\Users\\test\\AppData\\Local\\Temp\\ihgjzvum.bat
- C:\\Users\\test\\AppData\\Local\\Temp\\"C:\\Users\\test\\AppData\\Local\\Temp\\ihgjzvum.bat"
- C:\\Users\\test\\AppData\\Local\\Temp\\ihgjzvum.bat\\
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdKernel.dll.manifest
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdKernel.dll.123.Manifest
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdKernel.dll.124.Manifest
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\AdKernel.dll.2.Manifest
- C:\\Windows\\SysWOW64\\rundll32.exe
- C:\\Users\\test\\AppData\\Roaming\\hgpylpin\\MFC42.DLL

- C:\Windows\System32\mfcd42.dll
- C:\Users\test\AppData\Roaming\hgpylpin\ODBC32.dll
- C:\Windows\System32\odbc32.dll
- C:\Users\test\AppData\Roaming\hgpylpin\MSVCP60.dll
- C:\Windows\System32\msvc60.dll
- C:\Users\test\AppData\Roaming\hgpylpin\iphlpapi.dll
- C:\Windows\System32\IPHLPAPI.DLL
- C:\Users\test\AppData\Roaming\hgpylpin\WINNSI.DLL
- C:\Windows\System32\winnsi.dll
- C:\Windows\System32\tzres.dll
- C:\Users\test\AppData\Roaming\hgpylpin\home.dat
- C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
- C:\ProgramData\Microsoft\Network\Connections\Pbk\\*.pbk
- C:\Windows\System32\ras\\*.pbk
- C:\Users\test\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
- C:\Users\test\AppData\Roaming\Microsoft\Network\Connections\Pbk\\*.pbk
- C:\Users\test\AppData\Roaming\hgpylpin\dbghelp.dll
- C:\Windows\System32\dbghelp.dll
- C:\Users\test\AppData\Local\Temp\yfudjsrq.dat
- C:\Windows\SysWOW64\runDll32.exe.Local\
- C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af
- C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af\comctl32.dll
- C:\Users\test\AppData\Roaming\hgpylpin\WINMM.dll
- C:\Windows\System32\winmm.dll
- C:\Users\test\AppData\Roaming\hgpylpin\config.ini
- C:\Users\test\AppData\Local\Temp\omuibisy
- C:\Users\test\AppData\Local\Temp\omuibisy\
- C:\Users\test\AppData\Local\Temp\omuibisy\key.dat
- C:\Users\test\AppData\Roaming\hgpylpin\CommLogOpt.ini
- C:\Users\test\AppData\Roaming\hgpylpin\phone.ini
- C:\Users\test\AppData\Local\Temp\api32.dat
- C:\Users\test\AppData\Roaming\hgpylpin\business.ini
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat.crc
- C:\Users\test\AppData\Roaming\hgpylpin\ico\\*.\*
- C:\Users\test\AppData\Roaming\hgpylpin\ico
- C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6423780.ico
- C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6925031.ico
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat
- C:\2015.ini
- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Users\Public\Desktop\|xeffxbe\xb1|xeffxbfxa4|xeffxbfx8c|xeffxbe\xac|xeffxbe\xb4|xeffxbe\xab|xeffxbfx86|xeffxbfxa6.Ink
- C:\Users\test\AppData\Local\Temp\tfkbzyys.dat
- C:\Users\test\AppData\Local\Temp\mdvitfd.dat
- C:\Users\test\AppData\Local\Temp\vuqqkkqf
- C:\Users\Public\Desktop\|xeffxbfx88|xeffxbfx88|xeffxbfx91|xeffxbe\xaa|xeffxbe\xbd|xeffxbe\xad|xeffxbe\xba|xeffxbfxbe.Ink
- C:\Users\test\Desktop\|xeffxbe\xb1|xeffxbfxa4|xeffxbfx8c|xeffxbe\xac|xeffxbe\xb4|xeffxbe\xab|xeffxbfx86|xeffxbfxa6.Ink
- C:\Users\test\Desktop\|xeffxbfx88|xeffxbfx88|xeffxbfx91|xeffxbe\xaa|xeffxbe\xbd|xeffxbe\xad|xeffxbe\xba|xeffxbfxbe.Ink
- C:\ico.ini
- C:\Users\test\AppData\Roaming\hgpylpin\fast.exe
- C:\Users\desktop.ini
- C:\Users\test\AppData\Roaming
- C:\Users\test\AppData\Local\Temp\vuqqkkqf\game.dat
- C:\Users\test\Searches
- C:\Users\test\Searches\desktop.ini
- C:\Users\test\Videos
- C:\Users\test\Videos\desktop.ini
- C:\Users\test\Pictures
- C:\Users\test\Pictures\desktop.ini
- C:\Users\test\Desktop
- C:\Users\test\Contacts
- C:\Users\test\Contacts\desktop.ini
- C:\Users\test\Favorites
- C:\Users\test\Favorites\desktop.ini
- C:\Users\test\Music
- C:\Users\test\Music\desktop.ini
- C:\Users\test\Downloads
- C:\Users\test\Downloads\desktop.ini
- C:\Users\test\Documents
- C:\Users\test\Documents\desktop.ini
- C:\Users\test\Links
- C:\Users\test\Links\desktop.ini
- C:\Users\test\Saved Games
- C:\Users\test\Saved Games\desktop.ini
- C:\Windows\System32\shdocvw.dll
- C:\Windows\AppPatch\sysmain.sdb
- C:\Windows\System32\
- C:\Windows\SysWOW64\shdocvw.dll
- C:\Windows\System32
- C:\Windows\System32\\*.\*
- C:\Users\test\AppData\Local\Temp\qomurqcf.dat
- C:\Users\test\AppData\Local\Temp\nwftrebx
- C:\Users\test\AppData\Local\Temp\nwftrebx\game.dat
- C:\Users\test\AppData\Local\Temp\cugfljnk.bat
- C:\Windows\SysWOW64\CommLogOpt.ini
- C:\Windows\system\drivers\wdouNoNY.dat

#### 读取的文件

- \Device\KsecDD
- C:\Users\test\AppData\Local\Temp\422D.tmp
- C:\Users\test\AppData\Local\Temp\422D.tmp\422E.tmp
- C:\Users\test\AppData\Local\Temp\422D.tmp\422E.bat
- C:\Users\test\AppData\Local\Temp\export.exe
- C:\Users\test\AppData\Local\Temp\423F.tmp
- C:\Windows\SysWOW64\shell32.dll
- C:\Users\test\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

- C:\Users\test\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db
- C:\Users\test\Desktop\desktop.ini
- C:\
- C:\Users\
- C:\Users\test\
- C:\Users\test\AppData\
- C:\Users\test\AppData\Local\
- C:\Users\test\AppData\Local\Temp\
- C:\Users\test\AppData\Local\Temp\422D.tmp\
- C:\Windows\Globalization\Sorting\sortdefault.nls
- C:\Windows\systemnative\zh-CN\KERNELBASE.dll.mui
- \Device\NamedPipe\
- C:\Users\test\AppData\Local\Temp\3.txt
- C:\Users\test\AppData\Local\Temp\config.ini
- C:\Users\test\AppData\Local\Temp\trjqhbuq.dat
- \DEVICE\NETBT\_TCPIP\_{33E35B0A-D1F6-4AB1-A1AE-56B8A256B787}
- \Device\Afd\Endpoint
- \Device\RasAcid
- C:\Users\test\AppData\Local\Temp\zbqqtbl.dat
- C:\Users\test\AppData\Roaming\hgpylpin\run.ini
- C:\Users\test\AppData\Local\Temp\hgjzvm.bat
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll.123.Manifest
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll.124.Manifest
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll.2.Manifest
- C:\Windows\SysWOW64\rundll32.exe
- C:\Windows\System32\mf42.dll
- C:\Windows\System32\odbc32.dll
- C:\Windows\System32\msvc60.dll
- C:\Windows\System32\IPHLPAPI.DLL
- C:\Windows\System32\winnsi.dll
- C:\Windows\System32\tzres.dll
- C:\Users\test\AppData\Roaming\hgpylpin\Hijack.dll
- C:\Users\test\AppData\Roaming\hgpylpin\ProtocolFilters.dll
- C:\Users\test\AppData\Roaming\hgpylpin\nfapi.dll
- C:\Users\test\AppData\Roaming\hgpylpin\home.dat
- C:\Users\test\AppData\Roaming\hgpylpin\WyAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\DeskTop.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NewPhone.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NetData.dll
- C:\Users\test\AppData\Roaming\hgpylpin\devdata.dll
- C:\Users\test\AppData\Roaming\hgpylpin\CIBSTATIST.dll
- C:\Users\test\AppData\Roaming\hgpylpin\inject.dll
- C:\Windows\System32\dbghelp.dll
- C:\Users\test\AppData\Local\Temp\yfudjsrq.dat
- C:\Users\test\AppData\Roaming\hgpylpin\PopAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\flowdatadll.dll
- C:\Windows\winsxs\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af\comctl32.dll
- C:\Users\test\AppData\Roaming\hgpylpin\LoadHook.dll
- C:\Windows\System32\winmm.dll
- C:\Users\test\AppData\Roaming\hgpylpin\config.ini
- C:\Users\test\AppData\Roaming\hgpylpin\cdd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\CommLogOpt.ini
- C:\Users\test\AppData\Roaming\hgpylpin\phone.ini
- C:\Users\test\AppData\Roaming\hgpylpin\pop.dat
- C:\Users\test\AppData\Roaming\hgpylpin\tips.ini
- C:\Users\test\AppData\Roaming\hgpylpin\business.ini
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat.crc
- C:\Users\test\AppData\Local\Temp\omuibisy\key.dat
- C:\2015.ini
- C:\Users\test\AppData\Local\Temp\tfkbzyys.dat
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat
- C:\Users\test\AppData\Local\Temp\mdvitfd.dat
- C:\ico.ini
- C:\Users\desktop.ini
- C:\Users
- C:\Users\test
- C:\Users\test\AppData
- C:\Users\test\AppData\Roaming
- C:\Users\test\AppData\Roaming\hgpylpin
- C:\Users\test\Searches\desktop.ini
- C:\Users\test\Videos\desktop.ini
- C:\Users\test\Pictures\desktop.ini
- C:\Users\test\Contacts\desktop.ini
- C:\Users\test\Favorites\desktop.ini
- C:\Users\test\Music\desktop.ini
- C:\Users\test\Downloads\desktop.ini
- C:\Users\test\Documents\desktop.ini
- C:\Users\test\Links\desktop.ini
- C:\Users\test\Saved Games\desktop.ini
- C:\Windows\System32\shdocvw.dll
- C:\Windows\AppPatch\sysmain.sdb
- C:\Windows\System32\
- C:\Users\test\AppData\Local\Temp\qomurqcf.dat
- C:\Users\test\AppData\Roaming\hgpylpin\runhome.exe
- C:\Windows\SysWOW64\CommLogOpt.ini
- C:\Users\test\AppData\Roaming\hgpylpin\home.xml

#### 修改的文件

- C:\Users\test\AppData\Local\Temp\422D.tmp\422E.bat
- C:\Users\test\AppData\Local\Temp\export.exe
- C:\Users\test\AppData\Local\Temp\1.txt
- C:\Users\test\AppData\Local\Temp\2.txt
- \Device\Afd\Endpoint
- \Device\RasAcid

- C:\Users\test\AppData\Local\Temp\zbqgtqbl.dat
- C:\Users\test\AppData\Local\Temp\trjqhbuq.dat
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll
- C:\Users\test\AppData\Roaming\hgpylpin\AdMain.exe
- C:\Users\test\AppData\Roaming\hgpylpin\WyAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\DeskTop.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NewPhone.dll
- C:\Users\test\AppData\Roaming\hgpylpin\devdata.ini
- C:\Users\test\AppData\Roaming\hgpylpin\devdata.dll
- C:\Users\test\AppData\Roaming\hgpylpin\yun.exe
- C:\Users\test\AppData\Roaming\hgpylpin\runhome.exe
- C:\Users\test\AppData\Roaming\hgpylpin\home.xml
- C:\Users\test\AppData\Roaming\hgpylpin\Hijack.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NetData.dll
- C:\Users\test\AppData\Roaming\hgpylpin\CIBSTATIST.dll
- C:\Users\test\AppData\Roaming\hgpylpin\weifileconfig.ini
- C:\Users\test\AppData\Roaming\hgpylpin\inject.dll
- C:\Users\test\AppData\Roaming\hgpylpin\tips.ini
- C:\Users\test\AppData\Roaming\hgpylpin\LoadHook.dll
- C:\Users\test\AppData\Roaming\hgpylpin\SFU\_Recode\_Dll.dll
- C:\Users\test\AppData\Roaming\hgpylpin\cdd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\PopAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\pop.dat
- C:\Users\test\AppData\Roaming\hgpylpin\flowdatadll.dll
- C:\Users\test\AppData\Roaming\hgpylpin\nfapi.dll
- C:\Users\test\AppData\Roaming\hgpylpin\ProtocolFilters.dll
- C:\Users\test\AppData\Roaming\hgpylpin\run.ini
- C:\Users\test\AppData\Local\Temp\lhgzvum.bat
- C:\Users\test\AppData\Local\Temp\yfudjsrq.dat
- C:\Users\test\AppData\Local\Temp\omuibisy\key.dat
- C:\Users\test\AppData\Local\Temp\api32.dat
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat.crc
- C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6423780.ico
- C:\Users\test\AppData\Roaming\hgpylpin\ico\desk6925031.ico
- C:\Users\test\AppData\Local\Temp\fimxgoep.dat
- C:\Users\test\AppData\Local\Temp\tfkbzyys.dat
- C:\Users\test\AppData\Local\Temp\mdvitfjd.dat
- C:\Users\test\AppData\Roaming\hgpylpin\fast.exe
- C:\Users\test\AppData\Local\Temp\qomurqcf.dat
- C:\Users\test\AppData\Local\Temp\cugfljnk.bat
- C:\Windows\system32\drivers\wdouNoNY.dat

#### 删除的文件

- C:\Users\test\AppData\Local\Temp\422D.tmp
- C:\Users\test\AppData\Local\Temp\422D.tmp\422E.tmp
- C:\Users\test\AppData\Local\Temp\zbqgtqbl.dat
- C:\Users\test\AppData\Local\Temp\export.exe
- C:\Users\test\AppData\Local\Temp\lhgzvum.bat
- C:\Users\test\AppData\Roaming\hgpylpin\phone.ini
- C:\Users\test\AppData\Local\Temp\yfudjsrq.dat
- C:\Users\test\AppData\Local\Temp\omuibisy\key.dat
- C:\Users\test\AppData\Local\Temp\omuibisy
- C:\Users\test\AppData\Roaming\hgpylpin\AdKernel.dll
- C:\Users\Public\Desktop\{\xef\xbe\xb1\xef\xbf\xa4\xef\xbf\x8c\xef\xbe\xac\xef\xbe\xb4\xef\xbe\xab\xef\xbf\x86\xef\xbf\xa6}.lnk
- C:\Users\test\AppData\Roaming\hgpylpin\AdMain.exe
- C:\Users\test\AppData\Roaming\hgpylpin\run.ini
- C:\Users\Public\Desktop\{\xef\xbf\x88\xef\xbf\x88\xef\xbf\x91\xef\xbe\xaa\xef\xbe\xbd\xef\xbe\xad\xef\xbe\xba\xef\xbf\xbe}.lnk
- C:\Users\test\AppData\Roaming\hgpylpin\Hijack.dll
- C:\Users\test\AppData\Local\Temp\mdvitfjd.dat
- C:\Users\test\Desktop\{\xef\xbe\xb1\xef\xbf\xa4\xef\xbf\x8c\xef\xbe\xac\xef\xbe\xb4\xef\xbe\xab\xef\xbf\x86\xef\xbf\xa6}.lnk
- C:\Users\test\Desktop\{\xef\xbf\x88\xef\xbf\x88\xef\xbf\x91\xef\xbe\xaa\xef\xbe\xbd\xef\xbe\xad\xef\xbe\xba\xef\xbf\xbe}.lnk
- C:\Users\test\AppData\Roaming\hgpylpin\runhome.exe
- C:\Users\test\AppData\Roaming\hgpylpin\WyAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\DeskTop.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NewPhone.dll
- C:\Users\test\AppData\Roaming\hgpylpin\NetData.dll
- C:\Users\test\AppData\Roaming\hgpylpin\devdata.dll
- C:\Users\test\AppData\Roaming\hgpylpin\CIBSTATIST.dll
- C:\Users\test\AppData\Roaming\hgpylpin\inject.dll
- C:\Users\test\AppData\Roaming\hgpylpin\PopAd.dll
- C:\Users\test\AppData\Roaming\hgpylpin\flowdatadll.dll
- C:\Users\test\AppData\Roaming\hgpylpin\LoadHook.dll
- C:\Users\test\AppData\Roaming\hgpylpin\cdd.dll
- C:\Users\test\AppData\Local\Temp\tfkbzyys.dat
- C:\Users\test\AppData\Local\Temp\vuuqqkqf\game.dat
- C:\Users\test\AppData\Local\Temp\vuuqqkqf
- C:\Users\test\AppData\Local\Temp\qomurqcf.dat
- C:\Users\test\AppData\Local\Temp\nwftrebx\game.dat
- C:\Users\test\AppData\Local\Temp\nwftrebx
- C:\Users\test\AppData\Roaming\hgpylpin\home.xml

#### 注册表键

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetCon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\waiting.exe
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
- HKEY\_CLASSES\_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
- HKEY\_CLASSES\_ROOT\Drive\shell\FolderExtensions
- HKEY\_CLASSES\_ROOT\Drive\shell\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Drive\shell\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
- HKEY\_CLASSES\_ROOT\exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exe(Default)
- HKEY\_CLASSES\_ROOT\exe\OpenWithProgids
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\exe\OpenWithProgids
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\exe
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\exe\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\exe\UserChoice
- HKEY\_CLASSES\_ROOT\exefile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\CurVer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\ShellEx\IconHandler
- HKEY\_CLASSES\_ROOT\SystemFileAssociations\exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\ShellEx\IconHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exe\Content Type
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\AlwaysShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\AlwaysShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\exe\NeverShowExt
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\Category
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\Name
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\ParentFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\Description
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\RelativePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-7FE99A87C641}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4FCC3A-DB2C-424C-B029-

[illegible]

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PropertyBag
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2280033686-3172497658-3481507381-1000
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2280033686-3172497658-3481507381-1000\ProfileImagePath
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\Directory
- HKEY\_CLASSES\_ROOT\Directory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\CurVer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\ShellEx\IconHandler
- HKEY\_CLASSES\_ROOT\Folder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\ShellEx\IconHandler
- HKEY\_CLASSES\_ROOT\AllFilesystemObjects
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\ShellEx\IconHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\AlwaysShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\NeverShowExt
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\exe
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open
- HKEY\_CURRENT\_USER\Software\Classes\exefile\shell\open
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\DelegateExecute
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\DropTarget
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- HKEY\_CLASSES\_ROOT\ade
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\ade\(\Default)
- HKEY\_CLASSES\_ROOT\adp
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\adp\(\Default)
- HKEY\_CLASSES\_ROOT\app
- HKEY\_CLASSES\_ROOT\asp
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\asp\(\Default)
- HKEY\_CLASSES\_ROOT\bas
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\bas\(\Default)
- HKEY\_CLASSES\_ROOT\bat
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\bat\(\Default)
- HKEY\_CLASSES\_ROOT\cer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cer\(\Default)
- HKEY\_CLASSES\_ROOT\chm
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\chm\(\Default)
- HKEY\_CLASSES\_ROOT\cmd
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cmd\(\Default)
- HKEY\_CLASSES\_ROOT\com
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\com\(\Default)
- HKEY\_CLASSES\_ROOT\cpl
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cpl\(\Default)
- HKEY\_CLASSES\_ROOT\crt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\crt\(\Default)
- HKEY\_CLASSES\_ROOT\csh
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_INITIALIZE\_URLACTION\_SHELLEXECUTE\_TO\_ALLOW\_KB936610
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_INITIALIZE\_URLACTION\_SHELLEXECUTE\_TO\_ALLOW\_KB936610
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\*
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ALLOW\_REVERSE\_SOLIDUS\_IN\_USERINFO\_KB932562
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_ALLOW\_REVERSE\_SOLIDUS\_IN\_USERINFO\_KB932562
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Internet Explorer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY\_LOCAL\_MACHINE\System\Setup
- HKEY\_LOCAL\_MACHINE\SYSTEM\Setup\SystemSetupInProgress
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\Flags
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\Flags
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\Flags
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\waiting.exe
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\*
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\*
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONES\_DEFAULT\_DRIVE\_INTRANET\_KB941000
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_ZONES\_DEFAULT\_DRIVE\_INTRANET\_KB941000
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN\*
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1806
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1806
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodelfIdentifiers
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safertoolbox\codeidentifiers\TransparentEnabled
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\command
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\Default
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\ProgId
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellCompatibility\ProgIDs\exefile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\InheritConsoleHandles
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\ddeexec
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\RestrictRun
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\cmd.exe
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\cmd.exe



- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\SetWorkingDirectoryFromTarget
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\NoWorkingDirectory
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a4-1bd9-11e5-9838-806e6f6e6963}\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a4-1bd9-11e5-9838-806e6f6e6963}\Data
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a4-1bd9-11e5-9838-806e6f6e6963}\Generation
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a3-1bd9-11e5-9838-806e6f6e6963}\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a3-1bd9-11e5-9838-806e6f6e6963}\Data
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a3-1bd9-11e5-9838-806e6f6e6963}\Generation
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\BFA91AA3
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\AppCompat
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\AppCompat
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\LogIgnoreMonitorReason
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\System
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\EnableExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DelayedExpansion
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DefaultColor
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\AutoRun
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\EnableExtensions
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DelayedExpansion
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DefaultColor
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\CompletionChar
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\PathCompletionChar
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\AutoRun
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Nls\Locale
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000804
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\LevelObjects
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\Levels
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\UrlZones
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Paths
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Hashes
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\UrlZones
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Paths
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Hashes
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\UrlZones
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Paths
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Hashes
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\UrlZones
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\UrlZones
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\UrlZones
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Paths
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Hashes
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\UrlZones
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Paths
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Hashes
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\UrlZones
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Paths
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Hashes
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\UrlZones
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\UrlZones
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\DefaultLevel
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\SaferFlags
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Srp\GP\
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Srp\GP\RuleCount
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\PolicyScope
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\LogFileName
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE\_Initialize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE\_Initialize\DisableMetaFiles
- HKEY\_CURRENT\_USER\SOFTWARE\1e5
- HKEY\_CURRENT\_USER\Software\1e5\ie\_path
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{33e35b0a-d1f6-4ab1-a1ae-56b8a256b787}
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{33E35B0A-D1F6-4AB1-A1AE-56B8A256B787}\EnableDhcp
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Linkage\Bind
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\export\_RASMANCS
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\MaxFileSize

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileDirectory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\FileDirectory
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\DnsCache\Parameters
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows NT\DnsClient
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\export.exe
- HKEY\_CURRENT\_USER\Software\Classes\Directory
- HKEY\_LOCAL\_MACHINE\Software\Classes\Directory
- HKEY\_CURRENT\_USER\Software\Classes\Directory\ShellEx\IconHandler
- HKEY\_CURRENT\_USER\Software\Classes\Folder
- HKEY\_LOCAL\_MACHINE\Software\Classes\Folder
- HKEY\_CURRENT\_USER\Software\Classes\Folder\ShellEx\IconHandler
- HKEY\_CURRENT\_USER\Software\Classes\AllFilesystemObjects
- HKEY\_LOCAL\_MACHINE\Software\Classes\AllFilesystemObjects
- HKEY\_CURRENT\_USER\Software\Classes\AllFilesystemObjects\ShellEx\IconHandler
- HKEY\_CURRENT\_USER\Software\Classes\Directory\DocObject
- HKEY\_CURRENT\_USER\Software\Classes\Folder\DocObject
- HKEY\_CURRENT\_USER\Software\Classes\AllFilesystemObjects\DocObject
- HKEY\_CURRENT\_USER\Software\Classes\Directory\BrowseInPlace
- HKEY\_CURRENT\_USER\Software\Classes\Folder\BrowseInPlace
- HKEY\_CURRENT\_USER\Software\Classes\AllFilesystemObjects\BrowseInPlace
- HKEY\_CURRENT\_USER\Software\Classes\Directory\Clsid
- HKEY\_CURRENT\_USER\Software\Classes\Folder\Clsid
- HKEY\_CURRENT\_USER\Software\Classes\AllFilesystemObjects\Clsid
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\UseFilter
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\AdKernel.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\ProtocolFilters.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\mfapi.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\hijack.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\rundll32\_RASAPI32
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileDirectory
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\A66E19E6
- HKEY\_USERS\S-1-5-21-2280033686-3172497658-3481507381-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\rundll32\_RASMANCS
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileDirectory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxySettingsPerUser
- HKEY\_USERS\S-1-5-21-2280033686-3172497658-3481507381-1000
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigCustomUA
- HKEY\_CURRENT\_USER\Software\Classes
- HKEY\_CURRENT\_USER\Software\Classes\AutoProxyTypes
- HKEY\_LOCAL\_MACHINE\Software\Classes\AutoProxyTypes
- HKEY\_CURRENT\_USER\Software\Classes\AutoProxyTypes\Application/x-internet-signup
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-internet-signup
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-internet-signup\DllFile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-internet-signup\FileExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-internet-signup\Default
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-internet-signup\Flags
- HKEY\_CURRENT\_USER\Software\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig\DllFile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig\FileExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig\Default
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application/x-ns-proxy-autoconfig\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_INCLUDE\_PORT\_IN\_SPN\_KB908209
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_INCLUDE\_PORT\_IN\_SPN\_KB908209
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_MIME\_HANDLING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_MIME\_HANDLING\rundll32.exe

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_MIME\_HANDLING\*
- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security\_HKLM\_only
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_IGNORE\_POLICIES\_ZONEMAP\_IF\_ESC\_ENABLED\_KB918915
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_IGNORE\_POLICIES\_ZONEMAP\_IF\_ESC\_ENABLED\_KB918915
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges\
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges\
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK\*
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONES\_CHECK\_ZONEMAP\_POLICY\_KB941001
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_ZONES\_CHECK\_ZONEMAP\_POLICY\_KB941001
- HKEY\_LOCAL\_MACHINE\Software\Policies
- HKEY\_CURRENT\_USER\Software\Policies
- HKEY\_CURRENT\_USER\Software
- HKEY\_LOCAL\_MACHINE\Software
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\alipay.com
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\alisoft.com
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\taobao.com
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_USE\_IETLDLIST\_FOR\_DOMAIN\_DETERMINATION
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_USE\_IETLDLIST\_FOR\_DOMAIN\_DETERMINATION
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdDllVersionLow
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdDllVersionHigh
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionLow
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionHigh
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\rundll32.exe
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1A10
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\wyad.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\DeskTop.dll
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\SourcePath
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DevicePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\NewPhone.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\NetData.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\inject.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\PopAd.dll
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\flowdatadll.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\LoadHook.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\cdd.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\rundll32.exe
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\Explorer
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Explorer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Category
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Name
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\ParentFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Description
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\RelativePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\StreamResourceType
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\LocalRedirectOnly
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Roamable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\FolderTypeId
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\UnitFolderHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\PropertyBag
- HKEY\_CLASSES\_ROOT\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\CallForAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\RestrictedAttributes

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]



[illegible]

[illegible]

[illegible]

- [illegible]

[illegible]

- [illegible]

[illegible]



[illegible]



[illegible]

[illegible]

[illegible]

- [illegible]

[illegible]

[illegible]

[illegible]



[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]



[illegible]

- [illegible]

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\InitFolderHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}\PropertyBag
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Category
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Name
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\ParentFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Description
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\RelativePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\StreamResourceType
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\LocalRedirectOnly
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Roamable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\InitFolderHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\PropertyBag
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\SuppressionPolicy
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{Default}
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace\DelegateFolders
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\SuppressionPolicy
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace\DelegateFolders
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\UsersFiles\NameSpace
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\UsersFiles\NameSpace\DelegateFolders
- HKEY\_CLASSES\_ROOT\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\CallForAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\RestrictedAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsFORDISPLAY
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideFolderVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\UseDropHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsFORPARSING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsParseDisplayName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\QueryForOverlay
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\MapNetDriveVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\QueryForInfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideInWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideOnDesktopPerUser
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsAliasedNotifications
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsUniversalDelegate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\NoFileFolderJunction
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\PinToNameSpaceTree
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HasNavigationEnum
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
- HKEY\_CLASSES\_ROOT\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\{Default}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\LoadWithoutCOM
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Blocked
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Blocked
- HKEY\_LOCAL\_MACHINE\Software\Classes\CLSID\{dffc5-679f-4156-8947-c5c76bc0b67f}\InProcServer32
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\shdcovw.dll
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{DFFACDC5-679F-4156-8947-C5C76BC0B67F} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF
- HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\SQMClient\Windows
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\SQMClient\Windows
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\RunHome.exe
- HKEY\_USERS\DEFAULT\Control Panel\International
- HKEY\_USERS\DEFAULT\Control Panel\International\LocaleName
- HKEY\_USERS\DEFAULT\Control Panel\International\sCountry
- HKEY\_USERS\DEFAULT\Control Panel\International\sList
- HKEY\_USERS\DEFAULT\Control Panel\International\sDecimal
- HKEY\_USERS\DEFAULT\Control Panel\International\sThousand
- HKEY\_USERS\DEFAULT\Control Panel\International\sGrouping
- HKEY\_USERS\DEFAULT\Control Panel\International\sNativeDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\sCurrency
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonDecimalSep
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonThousandSep
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonGrouping
- HKEY\_USERS\DEFAULT\Control Panel\International\sPositiveSign
- HKEY\_USERS\DEFAULT\Control Panel\International\sNegativeSign
- HKEY\_USERS\DEFAULT\Control Panel\International\sTimeFormat
- HKEY\_USERS\DEFAULT\Control Panel\International\sShortTime
- HKEY\_USERS\DEFAULT\Control Panel\International\s1159
- HKEY\_USERS\DEFAULT\Control Panel\International\s2359
- HKEY\_USERS\DEFAULT\Control Panel\International\sShortDate
- HKEY\_USERS\DEFAULT\Control Panel\International\sYearMonth
- HKEY\_USERS\DEFAULT\Control Panel\International\sLongDate
- HKEY\_USERS\DEFAULT\Control Panel\International\iCountry
- HKEY\_USERS\DEFAULT\Control Panel\International\iMeasure
- HKEY\_USERS\DEFAULT\Control Panel\International\iPaperSize
- HKEY\_USERS\DEFAULT\Control Panel\International\iDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\iLZero
- HKEY\_USERS\DEFAULT\Control Panel\International\iNegNumber
- HKEY\_USERS\DEFAULT\Control Panel\International\iNumShape
- HKEY\_USERS\DEFAULT\Control Panel\International\iCurrDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\iCurrency
- HKEY\_USERS\DEFAULT\Control Panel\International\iNegCurr
- HKEY\_USERS\DEFAULT\Control Panel\International\iCalendarType
- HKEY\_USERS\DEFAULT\Control Panel\International\iFirstDayOfWeek
- HKEY\_USERS\DEFAULT\Control Panel\International\iFirstWeekOfYear
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\svchost.exe
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\puzlzMi
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\puzlzMi\name

#### 读取的注册表键

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetCon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Drive\shell\ex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowCompColor
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowInfoTip
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidelcons
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowSuperHidden
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowTypeOverlay
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\\*.exe\{Default}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\\*.exe\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\SystemFileAssociations\\*.exe\BrowseInPlace

[illegible]

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InitFolderHandler
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2280033686-3172497658-3481507381-1000\ProfileImagePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\BrowseInPlace
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\IsShortcut
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\AlwaysShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\NeverShowExt
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\WMM\Error Reporting\WMM\Disable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\DelegateExecute
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\ade\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\adp\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\asp\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\bas\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\bat\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cer\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\chm\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cmd\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\com\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\cpl\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\crt\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\*
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY\_LOCAL\_MACHINE\SYSTEM\Setup\SystemSetupInProgress
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\Flags
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\waiting.exe
- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\*
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\*
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\SpecialFoldersCacheSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN\waiting.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN\*
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1806
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1806
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\command
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\(\Default)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\InheritConsoleHandles
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\SetWorkingDirectoryFromTarget
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\exefile\shell\open\NoWorkingDirectory

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a4-1bd9-11e5-9838-806e6f6e6963}\Data
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a4-1bd9-11e5-9838-806e6f6e6963}\Generation
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a3-1bd9-11e5-9838-806e6f6e6963}\Data
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{372941a3-1bd9-11e5-9838-806e6f6e6963}\Generation
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\BFA91AA3
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\LogIgnoreMonitorReason
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\EnableExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DelayedExpansion
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\DefaultColor
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\AutoRun
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\EnableExtensions
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DelayedExpansion
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DefaultColor
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\CompletionChar
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\PathCompletionChar
- HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\AutoRun
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000804
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\Levels
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\DefaultLevel
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\SaferFlags
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Srp\GP\RuleCount
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\PolicyScope
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\LogFileName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE\_Initialize\DisableMetaFiles
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{33E35B0A-D1F6-4AB1-A1AE-56B8A256B787}\EnableDhcp
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Linkage\Bind
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileDirectory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASAPI32\FileDirectory
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\UseFilter
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\AdKernel.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\ProtocolFilters.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\mfapi.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\hijack.dll
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileDirectory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\A66E19E6
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileDirectory
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxySettingsPerUser
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigCustomUA
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-internet-signup\DllFile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-internet-signup\FileExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-internet-signup\Default
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-internet-signup\Flags
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-ns-proxy-autoconfig\DllFile
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-ns-proxy-autoconfig\FileExtensions
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-ns-proxy-autoconfig\Default
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\AutoProxyTypes\Application\x-ns-proxy-autoconfig\Flags
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_MIME\_HANDLING\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_MIME\_HANDLING\*
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security\_HKLM\_only
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK\rundll32.exe
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK\*



- HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionLow

• HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionHigh

• HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionLow

• HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IETId\IETIdVersionHigh

• HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\rundll32.exe

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN\rundll32.exe

• HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

• HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1A10

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\wydad.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\DeskTop.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\SourcePath

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\DevicePath

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\NewPhone.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\NetData.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\inject.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\PopAd.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\flowdata.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\LoadHook.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllINXOptions\scdd.dll

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Category

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Name

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\ParentFolder

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Description

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\RelativePath

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\ParsingName

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\InfoTip

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\LocalizedName

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Icon

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Security

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\StreamResource

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\StreamResourceType

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\LocalRedirectOnly

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Roamable

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\PreCreate

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Stream

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\PublishExpandedPath

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\Attributes

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\FolderTypeID

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F3CE0F7C-4901-4ACC-8648-D5D44B04EF8F}\UnitFolderHandler

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\Attributes

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\CallForAttributes

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\RestrictedAttributes

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\WantsFORDISPLAY

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\HideFolderVerbs

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\UseDropHandler

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\WantsFORPARSING

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\WantsParseDisplayName

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\QueryForOverlay

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\MapNetDriveVerbs

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\QueryForInfoTip

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\HideInWebView

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\HideOnDesktopPerUser

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\WantsAliasedNotifications

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\WantsUniversalDelegate

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\NoFileFolderJunction

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\PinToNameSpaceTree

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\ShellFolder\HasNavigationEnum

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{59031A47-3F72-44A7-89C5-5595FE6B30EE}

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Category

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Name

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParentFolder

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Description

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\RelativePath

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParsingName

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\InfoTip

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\LocalizedName

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Icon

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Security

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResource

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResourceType

• HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\F



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]



[illegible]

[illegible]

[illegible]











79D08E667CA7}\ParsingName



[illegible]

[illegible]

- [illegible]

- [illegible]

[illegible]

- [illegible]

- [illegible]



- [illegible]



[illegible]

[illegible]

[illegible]

[illegible]

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\ParentFolder
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Description
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\RelativePath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\ParsingName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\InfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\LocalizedName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Icon
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Security
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\StreamResource
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\StreamResourceType
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\LocalRedirectOnly
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Roamable
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\PreCreate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Stream
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\PublishExpandedPath
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\FolderTypeID
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}\InitFolderHandler
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\SuppressionPolicy
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{Default}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\SuppressionPolicy
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\Attributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\CallForAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\RestrictedAttributes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsFORDISPLAY
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideFolderVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\UseDropHandler
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsFORPARSING
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsParseDisplayName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\QueryForOverlay
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\MapNetDriveVerbs
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\QueryForInfoTip
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideInWebView
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HideOnDesktopPerUser
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsAliasedNotifications
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\WantsUniversalDelegate
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\NoFileFolderJunction
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\PinToNameSpaceTree
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\ShellFolder\HasNavigationEnum
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\{Default}
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\LoadWithoutCOM
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{DFFACDC5-679F-4156-8947-C5C76BC0B67F} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
- HKEY\_USERS\DEFAULT\Control Panel\International\LocaleName
- HKEY\_USERS\DEFAULT\Control Panel\International\sCountry
- HKEY\_USERS\DEFAULT\Control Panel\International\sList
- HKEY\_USERS\DEFAULT\Control Panel\International\sDecimal
- HKEY\_USERS\DEFAULT\Control Panel\International\sThousand
- HKEY\_USERS\DEFAULT\Control Panel\International\sGrouping
- HKEY\_USERS\DEFAULT\Control Panel\International\sNativeDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\sCurrency
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonDecimalSep
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonThousandSep
- HKEY\_USERS\DEFAULT\Control Panel\International\sMonGrouping
- HKEY\_USERS\DEFAULT\Control Panel\International\sPositiveSign
- HKEY\_USERS\DEFAULT\Control Panel\International\sNegativeSign
- HKEY\_USERS\DEFAULT\Control Panel\International\sTimeFormat
- HKEY\_USERS\DEFAULT\Control Panel\International\sShortTime
- HKEY\_USERS\DEFAULT\Control Panel\International\s1159
- HKEY\_USERS\DEFAULT\Control Panel\International\s2359
- HKEY\_USERS\DEFAULT\Control Panel\International\sShortDate
- HKEY\_USERS\DEFAULT\Control Panel\International\sYearMonth
- HKEY\_USERS\DEFAULT\Control Panel\International\sLongDate
- HKEY\_USERS\DEFAULT\Control Panel\International\iCountry
- HKEY\_USERS\DEFAULT\Control Panel\International\iMeasure
- HKEY\_USERS\DEFAULT\Control Panel\International\iPaperSize
- HKEY\_USERS\DEFAULT\Control Panel\International\iDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\iLZero
- HKEY\_USERS\DEFAULT\Control Panel\International\iNegNumber
- HKEY\_USERS\DEFAULT\Control Panel\International\iNumShape
- HKEY\_USERS\DEFAULT\Control Panel\International\iCurrDigits
- HKEY\_USERS\DEFAULT\Control Panel\International\iCurrency
- HKEY\_USERS\DEFAULT\Control Panel\International\iNegCurr
- HKEY\_USERS\DEFAULT\Control Panel\International\iCalendarType
- HKEY\_USERS\DEFAULT\Control Panel\International\iFirstDayOfWeek
- HKEY\_USERS\DEFAULT\Control Panel\International\iFirstWeekOfYear

#### 修改的注册表键

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

- HKEY\_CURRENT\_USER\SOFTWARE\1e5
- HKEY\_CURRENT\_USER\Software\1e5\ie\_path
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\export\_RASMANCS
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\export\_RASMANCS\FileDirectory
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\rundll32\_RASAPI32
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASAPI32\FileDirectory
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\rundll32\_RASMANCS
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableFileTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\EnableConsoleTracing
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\ConsoleTracingMask
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\MaxFileSize
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32\_RASMANCS\FileDirectory
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\puzlzMi
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\puzlzMi\name

#### 删除的注册表键

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

#### API解析

- kernel32.dll.GetModuleHandleA
- kernel32.dll.HeapCreate
- kernel32.dll.GetCommandLineA
- kernel32.dll.RemoveDirectoryA
- kernel32.dll.GetTempFileNameA
- kernel32.dll.GetShortPathNameA
- kernel32.dll.GetWindowsDirectoryA
- kernel32.dll.GetSystemDirectoryA
- kernel32.dll.HeapDestroy
- kernel32.dll.ExitProcess
- kernel32.dll.GetExitCodeProcess
- kernel32.dll.GetNativeSystemInfo
- kernel32.dll.FindResourceA
- kernel32.dll.LoadResource
- kernel32.dll.SizeofResource
- kernel32.dll.HeapAlloc
- kernel32.dll.HeapFree
- kernel32.dll.Sleep
- kernel32.dll.LoadLibraryA
- kernel32.dll.GetProcAddress
- kernel32.dll.FreeLibrary
- kernel32.dll.GetCurrentThreadId
- kernel32.dll.GetCurrentProcessId
- kernel32.dll.CloseHandle
- kernel32.dll.InitializeCriticalSection
- kernel32.dll.GetModuleFileNameA
- kernel32.dll.GetEnvironmentVariableA
- kernel32.dll.SetEnvironmentVariableA
- kernel32.dll.CreateFileA
- kernel32.dll.ReadFile
- kernel32.dll.WriteFile
- kernel32.dll.SetFilePointer
- kernel32.dll.DeleteFileA
- kernel32.dll.GetFileSize
- kernel32.dll.HeapReAlloc
- kernel32.dll.GetCurrentProcess
- kernel32.dll.TerminateProcess
- kernel32.dll.SetUnhandledExceptionFilter
- kernel32.dll.EnterCriticalSection
- kernel32.dll.LeaveCriticalSection
- kernel32.dll.GetVersionExA
- kernel32.dll.SetLastError
- kernel32.dll.HeapSize
- kernel32.dll.TlsAlloc
- kernel32.dll.GetCurrentDirectoryA
- kernel32.dll.SetCurrentDirectoryA
- kernel32.dll.GetTempPathA
- kernel32.dll.SetFileAttributesA
- kernel32.dll.CreateDirectoryA
- kernel32.dll.DeleteCriticalSection
- kernel32.dll.MultiByteToWideChar
- kernel32.dll.WideCharToMultiByte
- comctl32.dll.InitCommonControlsEx
- gdi32.dll.GetStockObject
- gdi32.dll.SelectObject
- gdi32.dll.SetBkColor

- gdi32.dll.SetTextColor
- gdi32.dll.GetTextExtentPoint32A
- gdi32.dll.CreateSolidBrush
- gdi32.dll.DeleteObject
- gdi32.dll.GetObjectA
- gdi32.dll.CreateCompatibleDC
- gdi32.dll.GetDIBits
- gdi32.dll.DeleteDC
- gdi32.dll.GetObjectType
- gdi32.dll.CreateDIBSection
- gdi32.dll.BitBlt
- gdi32.dll.CreateBitmap
- gdi32.dll.SetPixel
- msvcrt.dll.memset
- msvcrt.dll.strncmp
- msvcrt.dll.memmove
- msvcrt.dll.strncpy
- msvcrt.dll.strstr
- msvcrt.dll.\_strnicmp
- msvcrt.dll.\_stricmp
- msvcrt.dll.strlen
- msvcrt.dll.strcmp
- msvcrt.dll.memcpy
- msvcrt.dll.sprintf
- msvcrt.dll.fabs
- msvcrt.dll.ceil
- msvcrt.dll.malloc
- msvcrt.dll.floor
- msvcrt.dll.free
- msvcrt.dll.fclose
- msvcrt.dll.strcpy
- msvcrt.dll.tolower
- ole32.dll.CoInitialize
- ole32.dll.CoTaskMemFree
- ole32.dll.RevokeDragDrop
- shell32.dll.ShellExecuteExA
- shlwapi.dll.PathQuoteSpacesA
- shlwapi.dll.PathGetArgsA
- shlwapi.dll.PathAddBackslashA
- shlwapi.dll.PathRenameExtensionA
- shlwapi.dll.PathUnquoteSpacesA
- user32.dll.CharUpperA
- user32.dll.CharLowerA
- user32.dll.MessageBoxA
- user32.dll.SendMessageA
- user32.dll.PostMessageA
- user32.dll.GetWindowThreadProcessId
- user32.dll.IsWindowVisible
- user32.dll.GetWindowLongA
- user32.dll.GetForegroundWindow
- user32.dll.IsWindowEnabled
- user32.dll.EnableWindow
- user32.dll.EnumWindows
- user32.dll.SetWindowPos
- user32.dll.DestroyWindow
- user32.dll.GetDC
- user32.dll.GetWindowTextLengthA
- user32.dll.GetWindowTextA
- user32.dll.SetRect
- user32.dll.DrawTextA
- user32.dll.GetSystemMetrics
- user32.dll.ReleaseDC
- user32.dll.GetSysColor
- user32.dll.GetSysColorBrush
- user32.dll.CreateWindowExA
- user32.dll.CallWindowProcA
- user32.dll.SetWindowLongA
- user32.dll.SetFocus
- user32.dll.RedrawWindow
- user32.dll.RemovePropA
- user32.dll.DefWindowProcA
- user32.dll.SetPropA
- user32.dll.GetParent
- user32.dll.GetPropA
- user32.dll.GetWindow
- user32.dll.SetActiveWindow
- user32.dll.UnregisterClassA
- user32.dll.DestroyAcceleratorTable
- user32.dll.LoadIconA
- user32.dll.LoadCursorA
- user32.dll.RegisterClassA
- user32.dll.AdjustWindowRectEx
- user32.dll.ShowWindow
- user32.dll.CreateAcceleratorTableA
- user32.dll.PeekMessageA
- user32.dll.MsgWaitForMultipleObjects
- user32.dll.GetMessageA
- user32.dll.GetActiveWindow
- user32.dll.TranslateAcceleratorA
- user32.dll.TranslateMessage
- user32.dll.DispatchMessageA
- user32.dll.GetFocus
- user32.dll.GetClientRect
- user32.dll.FillRect
- user32.dll.EnumChildWindows
- user32.dll.DefFrameProcA
- user32.dll.GetWindowRect

- user32.dll.IsChild
- user32.dll.GetClassNameA
- user32.dll.GetKeyState
- user32.dll.DestroyIcon
- user32.dll.RegisterWindowMessageA
- winmm.dll.timeBeginPeriod
- uxtheme.dll.ThemeInitApiHook
- user32.dll.IsProcessDPIAware
- dwmapi.dll.DwmIsCompositionEnabled
- kernel32.dll.InitOnceExecuteOnce
- msimg32.dll.AlphaBlend
- comctl32.dll.DllGetVersion
- uxtheme.dll.IsAppThemed
- cryptbase.dll.SystemFunction036
- kernel32.dll.GetLongPathNameA
- ole32.dll.OleInitialize
- ole32.dll.CreateBindCtx
- ole32.dll.CoTaskMemAlloc
- propsys.dll.PSCreateMemoryPropertyStore
- propsys.dll.PSPropertyBag\_WriteDWORD
- ole32.dll.CoGetApartmentType
- ole32.dll.CoRegisterInitializeSpy
- comctl32.dll.#236
- oleaut32.dll.#6
- ole32.dll.CoGetMalloc
- propsys.dll.PSPropertyBag\_ReadDWORD
- comctl32.dll.#320
- ole32.dll.StringFromGUID2
- comctl32.dll.#324
- comctl32.dll.#323
- advapi32.dll.RegEnumKeyW
- oleaut32.dll.#2
- propsys.dll.PSPropertyBag\_ReadBSTR
- propsys.dll.PSPropertyBag\_ReadStrAlloc
- shell32.dll.#102
- advapi32.dll.OpenThreadToken
- ole32.dll.CoInitializeEx
- ole32.dll.CoCreateInstance
- advapi32.dll.InitializeSecurityDescriptor
- advapi32.dll.SetEntriesInAclW
- ntmarta.dll.GetMartaExtensionInterface
- advapi32.dll.SetSecurityDescriptorDacl
- advapi32.dll.IsTextUnicode
- comctl32.dll.#328
- comctl32.dll.#334
- comctl32.dll.#332
- comctl32.dll.#338
- comctl32.dll.#339
- ole32.dll.CoUninitialize
- sechost.dll.ConvertSidToStringSidW
- profapi.dll.#104
- propsys.dll.#430
- advapi32.dll.RegOpenKeyExW
- advapi32.dll.RegGetValueW
- advapi32.dll.RegCloseKey
- ole32.dll.CoTaskMemRealloc
- propsys.dll.InitPropVariantFromStringAsVector
- propsys.dll.PSCoerceToCanonicalValue
- propsys.dll.PropVariantToStringAlloc
- ole32.dll.PropVariantClear
- ole32.dll.CoAllowSetForegroundWindow
- kernel32.dll.InitializeSRWLock
- kernel32.dll.AcquireSRWLockExclusive
- kernel32.dll.AcquireSRWLockShared
- kernel32.dll.ReleaseSRWLockExclusive
- kernel32.dll.ReleaseSRWLockShared
- shell32.dll.SHGetFolderPathW
- advapi32.dll.SaferGetPolicyInformation
- setupapi.dll.CM\_Get\_Device\_Interface\_List\_Size\_ExW
- setupapi.dll.CM\_Get\_Device\_Interface\_List\_ExW
- comctl32.dll.#386
- ntdll.dll.RtlDllShutdownInProgress
- comctl32.dll.#329
- ole32.dll.OleUninitialize
- ole32.dll.CoRevokeInitializeSpy
- comctl32.dll.#388
- oleaut32.dll.#500
- kernel32.dll.SetThreadUILanguage
- kernel32.dll.CopyFileExW
- kernel32.dll.IsDebuggerPresent
- kernel32.dll.SetConsoleInputExeNameW
- advapi32.dll.SaferIdentifyLevel
- advapi32.dll.SaferComputeTokenFromLevel
- advapi32.dll.SaferCloseLevel
- kernel32.dll.SortGetHandle
- kernel32.dll.SortCloseHandle
- dnsapi.dll.DnsApiFree
- wininet.dll.InternetOpenA
- dhcpcsvc.dll.DhcplIsEnabled
- iphlapi.dll.ConvertInterfaceNameToLuidW
- wininet.dll.InternetSetOptionExA
- wininet.dll.InternetConnectA
- wininet.dll.HttpOpenRequestA
- wininet.dll.HttpSendRequestA
- rasapi32.dll.RasConnectionNotificationW
- rasman.dll.RasPortClearStatistics
- rasman.dll.RasBundleClearStatistics



- rasman.dll.RasBundleClearStatisticsEx
- rasman.dll.RasDeviceEnum
- rasman.dll.RasDeviceGetInfo
- rasman.dll.RasFreeBuffer
- rasman.dll.RasGetBuffer
- rasman.dll.RasGetInfo
- rasman.dll.RasGetDialMachineEventContext
- rasman.dll.RasSetDialMachineEventHandle
- rasman.dll.RasGetNdiswanDriverCaps
- rasman.dll.RasInitialize
- rasman.dll.RasInitializeNoWait
- rasman.dll.RasPortCancelReceive
- rasman.dll.RasPortEnum
- rasman.dll.RasPortGetInfo
- rasman.dll.RasPortGetFramingEx
- rasman.dll.RasPortGetStatistics
- rasman.dll.RasBundleGetStatistics
- rasman.dll.RasPortGetStatisticsEx
- rasman.dll.RasBundleGetStatisticsEx
- rasman.dll.RasPortReceive
- rasman.dll.RasPortReceiveEx
- rasman.dll.RasPortSend
- rasman.dll.RasPortGetBundle
- rasman.dll.RasGetDevConfig
- rasman.dll.RasGetDevConfigEx
- rasman.dll.RasSetDevConfig
- rasman.dll.RasPortClose
- rasman.dll.RasPortListen
- rasman.dll.RasPortConnectComplete
- rasman.dll.RasPortDisconnect
- rasman.dll.RasRequestNotification
- rasman.dll.RasPortEnumProtocols
- rasman.dll.RasPortSetFraming
- rasman.dll.RasPortSetFramingEx
- rasman.dll.RasSetCachedCredentials
- rasman.dll.RasGetDialParams
- rasman.dll.RasSetDialParams
- rasman.dll.RasCreateConnection
- rasman.dll.RasDestroyConnection
- rasman.dll.RasConnectionEnum
- rasman.dll.RasAddConnectionPort
- rasman.dll.RasEnumConnectionPorts
- rasman.dll.RasGetConnectionParams
- rasman.dll.RasSetConnectionParams
- rasman.dll.RasGetConnectionUserData
- rasman.dll.RasSetConnectionUserData
- rasman.dll.RasGetPortUserData
- rasman.dll.RasSetPortUserData
- rasman.dll.RasAddNotification
- rasman.dll.RasSignalNewConnection
- rasman.dll.RasApplyPostConnectActions
- rasman.dll.RasProtocolStop
- rasman.dll.RasProtocolCallback
- rasman.dll.RasProtocolChangePassword
- rasman.dll.RasProtocolGetInfo
- rasman.dll.RasProtocolRetry
- rasman.dll.RasProtocolStart
- rasman.dll.RasPortOpen
- rasman.dll.RasAllocateRoute
- rasman.dll.RasActivateRoute
- rasman.dll.RasActivateRouteEx
- rasman.dll.RasDeviceSetInfo
- rasman.dll.RasDeviceSetInfoSafe
- rasman.dll.RasDeviceConnect
- rasman.dll.RasPortSetInfo
- rasman.dll.RasSendProtocolResultToRasman
- rasman.dll.RasSetEapInfo
- rasman.dll.RasRpcConnect
- rasman.dll.RasRpcDisconnect
- rasman.dll.RasGetNumPortOpen
- rasman.dll.RasRefConnection
- rasman.dll.RasSetEapUIData
- rasman.dll.RasGetEapUIData
- rasman.dll.RasFindPrerequisiteEntry
- rasman.dll.RasPortOpenEx
- rasman.dll.RasLinkGetStatistics
- rasman.dll.RasConnectionGetStatistics
- rasman.dll.RasGetHportFromConnection
- rasman.dll.RasRPCBind
- rasman.dll.RasReferenceCustomCount
- rasman.dll.RasGetHConnFromEntry
- rasman.dll.RasGetDeviceName
- rasman.dll.RasEnableIpSec
- rasman.dll.RasSetTunnelEndPoints
- rasman.dll.RasStartRasAutoIfRequired
- rasman.dll.RasStartProtocolRenegotiation
- rasman.dll.RasSendNotification
- rasman.dll.RasGetDeviceNameW
- rasman.dll.RasGetUnicodeDeviceName
- rasman.dll.RasRpcGetVersion
- rasman.dll.RasRpcPortEnum
- rasman.dll.RasRpcDeviceEnum
- rasman.dll.RasRpcGetDevConfig
- rasman.dll.RasRpcPortGetInfo
- rasman.dll.RasRpcGetInstalledProtocols
- rasman.dll.RasRpcGetInstalledProtocolsEx
- rasman.dll.RasRpcGetSystemDirectory

- rasman.dll.RasRpcGetUserPreferences
- rasman.dll.RasRpcDeleteEntry
- rasman.dll.RasRpcEnumConnections
- rasman.dll.RasRpcGetCountryInfo
- rasman.dll.RasRpcGetErrorString
- rasman.dll.RasRpcSetUserPreferences
- rasman.dll.RasProtocolUpdateConnection
- rasman.dll.RasAddNotificationEx
- rasman.dll.RasRemoveNotificationEx
- rasman.dll.RasGetNotificationEntry
- rasman.dll.RasSignalMonitorThreadExit
- rasman.dll.RasmanUninitialize
- rtutils.dll.TraceRegisterExA
- rtutils.dll.TracePrintfExA
- sechost.dll.OpenSCManagerA
- sechost.dll.OpenServiceA
- sechost.dll.QueryServiceStatus
- sechost.dll.CloseServiceHandle
- sechost.dll.NotifyServiceStatusChangeA
- advapi32.dll.RegDeleteTreeA
- advapi32.dll.RegDeleteTreeW
- wininet.dll.HttpQueryInfoA
- wininet.dll.InternetReadFile
- wininet.dll.InternetCloseHandle
- advapi32.dll.UnregisterTraceGuids
- rpcrt4.dll.RpcBindingFree
- comctl32.dll.#321
- kernel32.dll.IsWow64Process
- adkernel.dll.MyStart
- kernel32.dll.FlsAlloc
- kernel32.dll.FlsGetValue
- kernel32.dll.FlsSetValue
- kernel32.dll.FlsFree
- kernel32.dll.InitializeCriticalSectionAndSpinCount
- kernel32.dll.IsProcessorFeaturePresent
- kernel32.dll.QueryFullProcessImageNameW
- kernel32.dll.QueryFullProcessImageNameA
- ntdll.dll.NtQuerySymbolicLinkObject
- ntdll.dll.NtOpenSymbolicLinkObject
- rasapi32.dll.RasEnumEntriesW
- shlwapi.dll.PathCanonicalizeW
- shlwapi.dll.PathRemoveFileSpecW
- shlwapi.dll.PathFindFileNameW
- sensapi.dll.IsNetworkAlive
- rpcrt4.dll.RpcBindingFromStringBindingW
- rpcrt4.dll.RpcBindingSetAuthInfoExW
- rpcrt4.dll.NdrClientCall2
- iphlpapi.dll.GetAdapterIndex
- urlmon.dll.CoInternetCreateSecurityManager
- urlmon.dll.CoInternetCreateZoneManager
- urlmon.dll.CoInternetIsFeatureEnabledForUrl
- version.dll.GetFileVersionInfoSizeW
- version.dll.GetFileVersionInfoW
- version.dll.VerQueryValueW
- kernel32.dll.RegQueryValueExW
- netdata.dll.GetVer
- kernelbase.dll.InitializeCriticalSectionAndSpinCount
- kernel32.dll.ProcessIdToSessionId
- imm32.dll.ImmCreateContext
- imm32.dll.ImmDestroyContext
- imm32.dll.ImmNotifyIME
- imm32.dll.ImmAssociateContext
- imm32.dll.ImmReleaseContext
- imm32.dll.ImmGetContext
- imm32.dll.ImmGetCompositionStringA
- imm32.dll.ImmSetCompositionStringA
- imm32.dll.ImmGetCompositionStringW
- imm32.dll.ImmSetCompositionStringW
- imm32.dll.ImmSetCandidateWindow
- icmp.dll.IcmpCreateFile
- icmp.dll.IcmpCloseHandle
- icmp.dll.IcmpSendEcho
- wintrust.dll.WinVerifyTrust
- kernel32.dll.OpenFileMappingA
- kernel32.dll.GetLocalTime
- kernel32.dll.GetLastError
- kernel32.dll.CreateEventA
- kernel32.dll.DeviceIoControl
- kernel32.dll.GlobalAlloc
- kernel32.dll.Process32Next
- kernel32.dll.MapViewOfFile
- kernel32.dll.CreateToolhelp32Snapshot
- kernel32.dll.GetACP
- kernel32.dll.FormatMessageA
- kernel32.dll.GetTickCount
- kernel32.dll.UnmapViewOfFile
- kernel32.dll.Process32First
- kernel32.dll.CreateThread
- kernel32.dll.SetStdHandle
- kernel32.dll.GetStringTypeW
- kernel32.dll.GetStringTypeA
- kernel32.dll.LCMapStringW
- kernel32.dll.LCMapStringA
- kernel32.dll.IsBadCodePtr
- kernel32.dll.IsBadReadPtr
- kernel32.dll.GetEnvironmentStringsW
- kernel32.dll.GetEnvironmentStrings

- kernel32.dll.FreeEnvironmentStringsW
- kernel32.dll.FreeEnvironmentStringsA
- kernel32.dll.IsBadWritePtr
- kernel32.dll.VirtualAlloc
- kernel32.dll.VirtualFree
- kernel32.dll.InterlockedExchange
- kernel32.dll.RtlUnwind
- kernel32.dll.GetVersion
- kernel32.dll.RaiseException
- kernel32.dll.TlsSetValue
- kernel32.dll.TlsFree
- kernel32.dll.TlsGetValue
- kernel32.dll.InterlockedDecrement
- kernel32.dll.InterlockedIncrement
- kernel32.dll.GetCPInfo
- kernel32.dll.GetOEMCP
- kernel32.dll.SetHandleCount
- kernel32.dll.GetStdHandle
- kernel32.dll.GetFileType
- kernel32.dll.GetStartupInfoA
- kernel32.dll.FlushFileBuffers
- user32.dll.wsprintfA
- iphlapi.dll.GetAdaptersInfo
- ws2\_32.dll.#151
- ws2\_32.dll.#17
- ws2\_32.dll.#5
- ws2\_32.dll.#51
- ws2\_32.dll.#57
- ws2\_32.dll.#16
- ws2\_32.dll.#19
- ws2\_32.dll.#1
- ws2\_32.dll.#13
- ws2\_32.dll.#21
- ws2\_32.dll.#2
- ws2\_32.dll.#20
- ws2\_32.dll.#18
- ws2\_32.dll.#9
- ws2\_32.dll.#4
- ws2\_32.dll.#52
- ws2\_32.dll.#3
- ws2\_32.dll.#23
- ws2\_32.dll.#116
- ws2\_32.dll.#115
- ws2\_32.dll.#8
- ws2\_32.dll.#14
- ws2\_32.dll.#11
- ws2\_32.dll.#12
- ws2\_32.dll.#10
- psapi.dll.GetModuleFileNameExA
- psapi.dll.GetProcessImageFileNameA
- oleaut32.dll.#9
- advapi32.dll.RegQueryValueW
- apphelp.dll.ApphelpCheckShellObject
- ntdll.dll.NtQueryInformationProcess
- kernel32.dll.InitializeProcThreadAttributeList
- kernel32.dll.UpdateProcThreadAttribute
- kernel32.dll.DeleteProcThreadAttributeList
- kernel32.dll.Wow64DisableWow64FsRedirection
- kernel32.dll.Wow64RevertWow64FsRedirection