cape

Detection(s): **SmokeLoader**

Sandbox Info

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2023-12-02 00:12:37	2023-12-02 00:18:14	337 seconds	2.4-CAPE

Machine	Label	Manager	Started On	Shutdown On
win7	win7	KVM	2023-12-02 00:12:37	2023-12-02 00:18:14

Malware config(s)

Type	SmokeLoader Config
C2s	http://go-piratia.ru/tmp/index.php http://humydrole.com/tmp/index.php http://pirateking.online/tmp/index.php http://piratia.pw/tmp/index.php http://trunk-co.ru/tmp/index.php http://weareelight.com/tmp/index.php

File Details

Filename	**3928.exe**
File Type	**PE32 executable (GUI) Intel 80386, for MS Windows**
File Size	**311808 bytes**
MD5	e0e783bba2f8e3f0d2da2bded27eceed
SHA1	a723dea176c400de9bdd169b703eb283032ed2cb
SHA256	076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239 [VT] [MWDB] [Bazaar]
SHA3-384	47e1eea30594c469186f60ea30931c83c81d927936354ffe3e6e6e810ebea85eb97f82b9b59fb53228fdaf50ea80cc87
CRC32	1D33105F
TLSH	T112641A1392A17C55E9164B328E1FC6E8761EFB518F7D77AA1218AB2F04731B2C263F11
Ssdeep	6144:f3JXcSiTU5/67tt575Wh5oLzrFV2qIp69a:f3/5/67ttD8Czr+5Il
PE	Strings

Signatures

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

type: call
pid: 1988

cid: 882
IP: 190.218.32.77:80 (unknown)

A file was accessed within the Public folder.

file: C:\Users\Public\Desktop\Acrobat Reader DC.lnk

SetUnhandledExceptionFilter detected (possible anti-debug)

type: call
pid: 3496
cid: 14

Checks adapter addresses which can be used to detect virtual network interfaces

type: call
pid: 1988
cid: 780

Dynamic (imported) function loading detected

DynamicLoader: ntdll.dll/RtlExitUserThread
type: call
pid: 1988
cid: 8
DynamicLoader: CRYPTSP.dll/CryptHashData
type: call
pid: 1988
cid: 684
DynamicLoader: CRYPTSP.dll/CryptGetHashParam
type: call
pid: 1988
cid: 686
DynamicLoader: CRYPTSP.dll/CryptDestroyHash
type: call
pid: 1988
cid: 687
DynamicLoader: CRYPTSP.dll/CryptReleaseContext
type: call
pid: 1988
cid: 688
DynamicLoader: ADVAPI32.dll/LookupAccountNameW
type: call
pid: 1988
cid: 751
DynamicLoader: XmlLite.dll/CreateXmlWriter
type: call
pid: 1988
cid: 754
DynamicLoader: XmlLite.dll/CreateXmlWriterOutputWithEncodingName
type: call
pid: 1988
cid: 755
DynamicLoader: ole32.dll/CoInitializeEx
type: call
pid: 1988
cid: 773
DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
type: call
pid: 1988
cid: 775
DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
type: call
pid: 1988
cid: 776
DynamicLoader: ole32.dll/CoTaskMemAlloc
type: call
pid: 1988

cid: 777
DynamicLoader: ole32.dll/StringFromIID
type: call
pid: 1988
cid: 778
DynamicLoader: NSI.dll/NsiAllocateAndGetTable
type: call
pid: 1988
cid: 783
DynamicLoader: CFGMGR32.dll/CM_Open_Class_Key_ExW
type: call
pid: 1988
cid: 789
DynamicLoader: IPHLPAPI.DLL/ConvertInterfaceGuidToLuid
type: call
pid: 1988
cid: 793
DynamicLoader: IPHLPAPI.DLL/GetIfEntry2
type: call
pid: 1988
cid: 798
DynamicLoader: IPHLPAPI.DLL/GetIpForwardTable2
type: call
pid: 1988
cid: 803
DynamicLoader: IPHLPAPI.DLL/GetIpNetEntry2
type: call
pid: 1988
cid: 814
DynamicLoader: IPHLPAPI.DLL/FreeMibTable
type: call
pid: 1988
cid: 823
DynamicLoader: ole32.dll/CoTaskMemFree
type: call
pid: 1988
cid: 824
DynamicLoader: NSI.dll/NsiFreeTable
type: call
pid: 1988
cid: 825
DynamicLoader: ole32.dll/CoUninitialize
type: call
pid: 1988
cid: 833
DynamicLoader: SHLWAPI.dll/StrCmpNW
type: call
pid: 1988
cid: 841
DynamicLoader: WS2_32.dll/GetAddrInfoW
type: call
pid: 1988
cid: 853
DynamicLoader: WS2_32.dll/WSASocketW
type: call
pid: 1988
cid: 873
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 875
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 877
DynamicLoader: WS2_32.dll/
type: call

pid: 1988
cid: 880
DynamicLoader: WS2_32.dll/WSAIoctl
type: call
pid: 1988
cid: 881
DynamicLoader: WS2_32.dll/FreeAddrInfoW
type: call
pid: 1988
cid: 883
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 890
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 892
DynamicLoader: WS2_32.dll/WSARecv
type: call
pid: 1988
cid: 893
DynamicLoader: WS2_32.dll/WSASend
type: call
pid: 1988
cid: 896
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 927
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 939
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 1578
DynamicLoader: WS2_32.dll/
type: call
pid: 1988
cid: 1587
DynamicLoader: comctl32.dll/
type: call
pid: 1988
cid: 1690
DynamicLoader: comctl32.dll/
type: call
pid: 1988
cid: 1691
DynamicLoader: kernel32.dll/FlsFree
type: call
pid: 1988
cid: 1702
DynamicLoader: comctl32.dll/
type: call
pid: 1988
cid: 1707

Enumerates running processes

process: System with pid 4
type: call
pid: 1988
cid: 36
process: smss.exe with pid 264
type: call
pid: 1988

cid: 37
process: csrss.exe with pid 352
type: call
pid: 1988
cid: 38
process: wininit.exe with pid 388
type: call
pid: 1988
cid: 39
process: csrss.exe with pid 400
type: call
pid: 1988
cid: 40
process: winlogon.exe with pid 436
type: call
pid: 1988
cid: 41
process: services.exe with pid 484
type: call
pid: 1988
cid: 42
process: lsass.exe with pid 492
type: call
pid: 1988
cid: 43
process: lsm.exe with pid 500
type: call
pid: 1988
cid: 44
process: svchost.exe with pid 592
type: call
pid: 1988
cid: 45
process: svchost.exe with pid 656
type: call
pid: 1988
cid: 46
process: svchost.exe with pid 760
type: call
pid: 1988
cid: 47
process: svchost.exe with pid 824
type: call
pid: 1988
cid: 48
process: svchost.exe with pid 848
type: call
pid: 1988
cid: 49
process: svchost.exe with pid 976
type: call
pid: 1988
cid: 50
process: svchost.exe with pid 112
type: call
pid: 1988
cid: 51
process: spoolsv.exe with pid 1012
type: call
pid: 1988
cid: 52
process: svchost.exe with pid 1116
type: call
pid: 1988
cid: 53
process: armsvc.exe with pid 1268
type: call

pid: 1988
cid: 54
process: svchost.exe with pid 1296
type: call
pid: 1988
cid: 55
process: svchost.exe with pid 1712
type: call
pid: 1988
cid: 56
process: taskhost.exe with pid 1896
type: call
pid: 1988
cid: 57
process: dwm.exe with pid 1964
type: call
pid: 1988
cid: 58
process: explorer.exe with pid 1988
type: call
pid: 1988
cid: 59
process: OSPPSVC.EXE with pid 620
type: call
pid: 1988
cid: 60
process: sppsvc.exe with pid 1088
type: call
pid: 1988
cid: 61
process: SearchIndexer.exe with pid 2080
type: call
pid: 1988
cid: 62
process: wmpnetwk.exe with pid 2292
type: call
pid: 1988
cid: 63
process: mscorsvw.exe with pid 2564
type: call
pid: 1988
cid: 64
process: mscorsvw.exe with pid 2652
type: call
pid: 1988
cid: 65
process: svchost.exe with pid 2696
type: call
pid: 1988
cid: 66
process: taskeng.exe with pid 4052
type: call
pid: 1988
cid: 67
process: audiodg.exe with pid 2708
type: call
pid: 1988
cid: 68
process: cmd.exe with pid 1792
type: call
pid: 1988
cid: 69
process: conhost.exe with pid 1612
type: call
pid: 1988
cid: 70
process: cmd.exe with pid 1812

type: call
pid: 1988
cid: 71
process: conhost.exe with pid 812
type: call
pid: 1988
cid: 72
process: taskhost.exe with pid 2184
type: call
pid: 1988
cid: 73
process: svchost.exe with pid 3840
type: call
pid: 1988
cid: 74

Expresses interest in specific running processes

type: call
pid: 1988
cid: 36
type: call
pid: 1988
cid: 37
type: call
pid: 1988
cid: 38
type: call
pid: 1988
cid: 39
type: call
pid: 1988
cid: 40
type: call
pid: 1988
cid: 41
type: call
pid: 1988
cid: 42
type: call
pid: 1988
cid: 43
type: call
pid: 1988
cid: 44
type: call
pid: 1988
cid: 45
type: call
pid: 1988
cid: 46
type: call
pid: 1988
cid: 47
type: call
pid: 1988
cid: 48
type: call
pid: 1988
cid: 49
type: call
pid: 1988
cid: 50
type: call
pid: 1988
cid: 51
type: call
pid: 1988

cid: 52
type: call
pid: 1988
cid: 53
type: call
pid: 1988
cid: 54
type: call
pid: 1988
cid: 55
type: call
pid: 1988
cid: 56
type: call
pid: 1988
cid: 57
type: call
pid: 1988
cid: 58
type: call
pid: 1988
cid: 59
type: call
pid: 1988
cid: 60
type: call
pid: 1988
cid: 61
type: call
pid: 1988
cid: 62
type: call
pid: 1988
cid: 63
type: call
pid: 1988
cid: 64
type: call
pid: 1988
cid: 65
type: call
pid: 1988
cid: 66
type: call
pid: 1988
cid: 67
type: call
pid: 1988
cid: 68
type: call
pid: 1988
cid: 69
type: call
pid: 1988
cid: 70
type: call
pid: 1988
cid: 71
type: call
pid: 1988
cid: 72
type: call
pid: 1988
cid: 73
type: call
pid: 1988
cid: 74

type: call
pid: 1988
cid: 82
type: call
pid: 1988
cid: 83
type: call
pid: 1988
cid: 84
type: call
pid: 1988
cid: 85
type: call
pid: 1988
cid: 86
type: call
pid: 1988
cid: 87
type: call
pid: 1988
cid: 88
type: call
pid: 1988
cid: 89
type: call
pid: 1988
cid: 90
type: call
pid: 1988
cid: 91
type: call
pid: 1988
cid: 92
type: call
pid: 1988
cid: 93
type: call
pid: 1988
cid: 94
type: call
pid: 1988
cid: 95
type: call
pid: 1988
cid: 96
type: call
pid: 1988
cid: 97
type: call
pid: 1988
cid: 98
type: call
pid: 1988
cid: 99
type: call
pid: 1988
cid: 100
type: call
pid: 1988
cid: 101
type: call
pid: 1988
cid: 102
type: call
pid: 1988
cid: 103
type: call

pid: 1988
cid: 104
type: call
pid: 1988
cid: 105
type: call
pid: 1988
cid: 106
type: call
pid: 1988
cid: 107
type: call
pid: 1988
cid: 108
type: call
pid: 1988
cid: 109
type: call
pid: 1988
cid: 110
type: call
pid: 1988
cid: 111
type: call
pid: 1988
cid: 112
type: call
pid: 1988
cid: 113
type: call
pid: 1988
cid: 114
type: call
pid: 1988
cid: 115
type: call
pid: 1988
cid: 116
type: call
pid: 1988
cid: 117
type: call
pid: 1988
cid: 118
type: call
pid: 1988
cid: 119
type: call
pid: 1988
cid: 120
type: call
pid: 1988
cid: 129
type: call
pid: 1988
cid: 130
type: call
pid: 1988
cid: 131
type: call
pid: 1988
cid: 132
type: call
pid: 1988
cid: 133
type: call
pid: 1988

cid: 134
type: call
pid: 1988
cid: 135
type: call
pid: 1988
cid: 136
type: call
pid: 1988
cid: 137
type: call
pid: 1988
cid: 138
type: call
pid: 1988
cid: 139
type: call
pid: 1988
cid: 140
type: call
pid: 1988
cid: 141
type: call
pid: 1988
cid: 142
type: call
pid: 1988
cid: 143
type: call
pid: 1988
cid: 144
type: call
pid: 1988
cid: 145
type: call
pid: 1988
cid: 146
type: call
pid: 1988
cid: 147
type: call
pid: 1988
cid: 148
type: call
pid: 1988
cid: 149
type: call
pid: 1988
cid: 150
type: call
pid: 1988
cid: 151
type: call
pid: 1988
cid: 152
type: call
pid: 1988
cid: 153
type: call
pid: 1988
cid: 154
type: call
pid: 1988
cid: 155
type: call
pid: 1988
cid: 156

type: call
pid: 1988
cid: 157
type: call
pid: 1988
cid: 158
type: call
pid: 1988
cid: 159
type: call
pid: 1988
cid: 160
type: call
pid: 1988
cid: 161
type: call
pid: 1988
cid: 162
type: call
pid: 1988
cid: 163
type: call
pid: 1988
cid: 164
type: call
pid: 1988
cid: 165
type: call
pid: 1988
cid: 166
type: call
pid: 1988
cid: 167
type: call
pid: 1988
cid: 183
type: call
pid: 1988
cid: 184
type: call
pid: 1988
cid: 185
type: call
pid: 1988
cid: 186
type: call
pid: 1988
cid: 187
type: call
pid: 1988
cid: 188
type: call
pid: 1988
cid: 189
type: call
pid: 1988
cid: 190
type: call
pid: 1988
cid: 191
type: call
pid: 1988
cid: 192
type: call
pid: 1988
cid: 193
type: call

pid: 1988
cid: 194
type: call
pid: 1988
cid: 195
type: call
pid: 1988
cid: 196
type: call
pid: 1988
cid: 197
type: call
pid: 1988
cid: 198
type: call
pid: 1988
cid: 199
type: call
pid: 1988
cid: 200
type: call
pid: 1988
cid: 201
type: call
pid: 1988
cid: 202
type: call
pid: 1988
cid: 203
type: call
pid: 1988
cid: 204
type: call
pid: 1988
cid: 205
type: call
pid: 1988
cid: 206
type: call
pid: 1988
cid: 207
type: call
pid: 1988
cid: 208
type: call
pid: 1988
cid: 209
type: call
pid: 1988
cid: 210
type: call
pid: 1988
cid: 211
type: call
pid: 1988
cid: 212
type: call
pid: 1988
cid: 213
type: call
pid: 1988
cid: 214
type: call
pid: 1988
cid: 215
type: call
pid: 1988

cid: 216
type: call
pid: 1988
cid: 217
type: call
pid: 1988
cid: 218
type: call
pid: 1988
cid: 219
type: call
pid: 1988
cid: 220
type: call
pid: 1988
cid: 221
type: call
pid: 1988
cid: 227
type: call
pid: 1988
cid: 228
type: call
pid: 1988
cid: 229
type: call
pid: 1988
cid: 230
type: call
pid: 1988
cid: 231
type: call
pid: 1988
cid: 232
type: call
pid: 1988
cid: 233
type: call
pid: 1988
cid: 234
type: call
pid: 1988
cid: 235
type: call
pid: 1988
cid: 236
type: call
pid: 1988
cid: 237
type: call
pid: 1988
cid: 238
type: call
pid: 1988
cid: 239
type: call
pid: 1988
cid: 240
type: call
pid: 1988
cid: 241
type: call
pid: 1988
cid: 242
type: call
pid: 1988
cid: 243

type: call
pid: 1988
cid: 244
type: call
pid: 1988
cid: 245
type: call
pid: 1988
cid: 246
type: call
pid: 1988
cid: 247
type: call
pid: 1988
cid: 248
type: call
pid: 1988
cid: 249
type: call
pid: 1988
cid: 250
type: call
pid: 1988
cid: 251
type: call
pid: 1988
cid: 252
type: call
pid: 1988
cid: 253
type: call
pid: 1988
cid: 254
type: call
pid: 1988
cid: 255
type: call
pid: 1988
cid: 256
type: call
pid: 1988
cid: 257
type: call
pid: 1988
cid: 258
type: call
pid: 1988
cid: 259
type: call
pid: 1988
cid: 260
type: call
pid: 1988
cid: 261
type: call
pid: 1988
cid: 262
type: call
pid: 1988
cid: 263
type: call
pid: 1988
cid: 264
type: call
pid: 1988
cid: 265
type: call

pid: 1988
cid: 274
type: call
pid: 1988
cid: 275
type: call
pid: 1988
cid: 276
type: call
pid: 1988
cid: 277
type: call
pid: 1988
cid: 278
type: call
pid: 1988
cid: 279
type: call
pid: 1988
cid: 280
type: call
pid: 1988
cid: 281
type: call
pid: 1988
cid: 282
type: call
pid: 1988
cid: 283
type: call
pid: 1988
cid: 284
type: call
pid: 1988
cid: 285
type: call
pid: 1988
cid: 286
type: call
pid: 1988
cid: 287
type: call
pid: 1988
cid: 288
type: call
pid: 1988
cid: 289
type: call
pid: 1988
cid: 290
type: call
pid: 1988
cid: 291
type: call
pid: 1988
cid: 292
type: call
pid: 1988
cid: 293
type: call
pid: 1988
cid: 294
type: call
pid: 1988
cid: 295
type: call
pid: 1988

cid: 296
type: call
pid: 1988
cid: 297
type: call
pid: 1988
cid: 298
type: call
pid: 1988
cid: 299
type: call
pid: 1988
cid: 300
type: call
pid: 1988
cid: 301
type: call
pid: 1988
cid: 302
type: call
pid: 1988
cid: 303
type: call
pid: 1988
cid: 304
type: call
pid: 1988
cid: 305
type: call
pid: 1988
cid: 306
type: call
pid: 1988
cid: 307
type: call
pid: 1988
cid: 308
type: call
pid: 1988
cid: 309
type: call
pid: 1988
cid: 310
type: call
pid: 1988
cid: 311
type: call
pid: 1988
cid: 312
type: call
pid: 1988
cid: 343
type: call
pid: 1988
cid: 344
type: call
pid: 1988
cid: 345
type: call
pid: 1988
cid: 346
type: call
pid: 1988
cid: 347
type: call
pid: 1988
cid: 348

type: call
pid: 1988
cid: 349
type: call
pid: 1988
cid: 350
type: call
pid: 1988
cid: 351
type: call
pid: 1988
cid: 352
type: call
pid: 1988
cid: 353
type: call
pid: 1988
cid: 354
type: call
pid: 1988
cid: 355
type: call
pid: 1988
cid: 356
type: call
pid: 1988
cid: 357
type: call
pid: 1988
cid: 358
type: call
pid: 1988
cid: 359
type: call
pid: 1988
cid: 360
type: call
pid: 1988
cid: 361
type: call
pid: 1988
cid: 362
type: call
pid: 1988
cid: 363
type: call
pid: 1988
cid: 364
type: call
pid: 1988
cid: 365
type: call
pid: 1988
cid: 366
type: call
pid: 1988
cid: 367
type: call
pid: 1988
cid: 368
type: call
pid: 1988
cid: 369
type: call
pid: 1988
cid: 370
type: call

pid: 1988
cid: 371
type: call
pid: 1988
cid: 372
type: call
pid: 1988
cid: 373
type: call
pid: 1988
cid: 374
type: call
pid: 1988
cid: 375
type: call
pid: 1988
cid: 376
type: call
pid: 1988
cid: 377
type: call
pid: 1988
cid: 378
type: call
pid: 1988
cid: 379
type: call
pid: 1988
cid: 380
type: call
pid: 1988
cid: 381
type: call
pid: 1988
cid: 399
type: call
pid: 1988
cid: 400
type: call
pid: 1988
cid: 401
type: call
pid: 1988
cid: 402
type: call
pid: 1988
cid: 403
type: call
pid: 1988
cid: 404
type: call
pid: 1988
cid: 405
type: call
pid: 1988
cid: 406
type: call
pid: 1988
cid: 407
type: call
pid: 1988
cid: 408
type: call
pid: 1988
cid: 409
type: call
pid: 1988

cid: 410
type: call
pid: 1988
cid: 411
type: call
pid: 1988
cid: 412
type: call
pid: 1988
cid: 413
type: call
pid: 1988
cid: 414
type: call
pid: 1988
cid: 415
type: call
pid: 1988
cid: 416
type: call
pid: 1988
cid: 417
type: call
pid: 1988
cid: 418
type: call
pid: 1988
cid: 419
type: call
pid: 1988
cid: 420
type: call
pid: 1988
cid: 421
type: call
pid: 1988
cid: 422
type: call
pid: 1988
cid: 423
type: call
pid: 1988
cid: 424
type: call
pid: 1988
cid: 425
type: call
pid: 1988
cid: 426
type: call
pid: 1988
cid: 427
type: call
pid: 1988
cid: 428
type: call
pid: 1988
cid: 429
type: call
pid: 1988
cid: 430
type: call
pid: 1988
cid: 431
type: call
pid: 1988
cid: 432

type: call
pid: 1988
cid: 433
type: call
pid: 1988
cid: 434
type: call
pid: 1988
cid: 435
type: call
pid: 1988
cid: 436
type: call
pid: 1988
cid: 437
type: call
pid: 1988
cid: 523
type: call
pid: 1988
cid: 524
type: call
pid: 1988
cid: 525
type: call
pid: 1988
cid: 526
type: call
pid: 1988
cid: 527
type: call
pid: 1988
cid: 528
type: call
pid: 1988
cid: 529
type: call
pid: 1988
cid: 530
type: call
pid: 1988
cid: 531
type: call
pid: 1988
cid: 532
type: call
pid: 1988
cid: 533
type: call
pid: 1988
cid: 534
type: call
pid: 1988
cid: 535
type: call
pid: 1988
cid: 536
type: call
pid: 1988
cid: 537
type: call
pid: 1988
cid: 538
type: call
pid: 1988
cid: 539
type: call

pid: 1988
cid: 540
type: call
pid: 1988
cid: 541
type: call
pid: 1988
cid: 542
type: call
pid: 1988
cid: 543
type: call
pid: 1988
cid: 544
type: call
pid: 1988
cid: 545
type: call
pid: 1988
cid: 546
type: call
pid: 1988
cid: 547
type: call
pid: 1988
cid: 548
type: call
pid: 1988
cid: 549
type: call
pid: 1988
cid: 550
type: call
pid: 1988
cid: 551
type: call
pid: 1988
cid: 552
type: call
pid: 1988
cid: 553
type: call
pid: 1988
cid: 554
type: call
pid: 1988
cid: 555
type: call
pid: 1988
cid: 556
type: call
pid: 1988
cid: 557
type: call
pid: 1988
cid: 558
type: call
pid: 1988
cid: 559
type: call
pid: 1988
cid: 560
type: call
pid: 1988
cid: 561
type: call
pid: 1988

cid: 573
type: call
pid: 1988
cid: 574
type: call
pid: 1988
cid: 575
type: call
pid: 1988
cid: 576
type: call
pid: 1988
cid: 577
type: call
pid: 1988
cid: 578
type: call
pid: 1988
cid: 579
type: call
pid: 1988
cid: 580
type: call
pid: 1988
cid: 581
type: call
pid: 1988
cid: 582
type: call
pid: 1988
cid: 583
type: call
pid: 1988
cid: 584
type: call
pid: 1988
cid: 585
type: call
pid: 1988
cid: 586
type: call
pid: 1988
cid: 587
type: call
pid: 1988
cid: 588
type: call
pid: 1988
cid: 589
type: call
pid: 1988
cid: 590
type: call
pid: 1988
cid: 591
type: call
pid: 1988
cid: 592
type: call
pid: 1988
cid: 593
type: call
pid: 1988
cid: 594
type: call
pid: 1988
cid: 595

type: call
pid: 1988
cid: 596
type: call
pid: 1988
cid: 597
type: call
pid: 1988
cid: 598
type: call
pid: 1988
cid: 599
type: call
pid: 1988
cid: 600
type: call
pid: 1988
cid: 601
type: call
pid: 1988
cid: 602
type: call
pid: 1988
cid: 603
type: call
pid: 1988
cid: 604
type: call
pid: 1988
cid: 605
type: call
pid: 1988
cid: 606
type: call
pid: 1988
cid: 607
type: call
pid: 1988
cid: 608
type: call
pid: 1988
cid: 609
type: call
pid: 1988
cid: 610
type: call
pid: 1988
cid: 611
type: call
pid: 1988
cid: 617
type: call
pid: 1988
cid: 618
type: call
pid: 1988
cid: 619
type: call
pid: 1988
cid: 620
type: call
pid: 1988
cid: 621
type: call
pid: 1988
cid: 622
type: call

pid: 1988
cid: 623
type: call
pid: 1988
cid: 624
type: call
pid: 1988
cid: 625
type: call
pid: 1988
cid: 626
type: call
pid: 1988
cid: 627
type: call
pid: 1988
cid: 628
type: call
pid: 1988
cid: 629
type: call
pid: 1988
cid: 630
type: call
pid: 1988
cid: 631
type: call
pid: 1988
cid: 632
type: call
pid: 1988
cid: 633
type: call
pid: 1988
cid: 634
type: call
pid: 1988
cid: 635
type: call
pid: 1988
cid: 636
type: call
pid: 1988
cid: 637
type: call
pid: 1988
cid: 638
type: call
pid: 1988
cid: 639
type: call
pid: 1988
cid: 640
type: call
pid: 1988
cid: 641
type: call
pid: 1988
cid: 642
type: call
pid: 1988
cid: 643
type: call
pid: 1988
cid: 644
type: call
pid: 1988

cid: 645
type: call
pid: 1988
cid: 646
type: call
pid: 1988
cid: 647
type: call
pid: 1988
cid: 648
type: call
pid: 1988
cid: 649
type: call
pid: 1988
cid: 650
type: call
pid: 1988
cid: 651
type: call
pid: 1988
cid: 652
type: call
pid: 1988
cid: 653
type: call
pid: 1988
cid: 654
type: call
pid: 1988
cid: 655
type: call
pid: 1988
cid: 661
type: call
pid: 1988
cid: 700
type: call
pid: 1988
cid: 716
type: call
pid: 1988
cid: 722
type: call
pid: 1988
cid: 735
type: call
pid: 1988
cid: 757
type: call
pid: 1988
cid: 767
type: call
pid: 1988
cid: 838
type: call
pid: 1988
cid: 856
type: call
pid: 1988
cid: 864
type: call
pid: 1988
cid: 885
type: call
pid: 1988
cid: 922

type: call
pid: 1988
cid: 946
type: call
pid: 1988
cid: 961
type: call
pid: 1988
cid: 996
type: call
pid: 1988
cid: 1005
type: call
pid: 1988
cid: 1012
type: call
pid: 1988
cid: 1112
type: call
pid: 1988
cid: 1133
type: call
pid: 1988
cid: 1159
type: call
pid: 1988
cid: 1352
type: call
pid: 1988
cid: 1467
type: call
pid: 1988
cid: 1547
type: call
pid: 1988
cid: 1572
type: call
pid: 1988
cid: 1580
type: call
pid: 1988
cid: 1601
type: call
pid: 1988
cid: 1683
type: call
pid: 1988
cid: 1687
type: call
pid: 1988
cid: 1696
type: call
pid: 1988
cid: 1700
type: call
pid: 1988
cid: 1713
type: call
pid: 1988
cid: 1921
type: call
pid: 1988
cid: 1940
type: call
pid: 1988
cid: 1950
type: call

pid: 1988
cid: 2144
type: call
pid: 1988
cid: 2149
type: call
pid: 1988
cid: 2191
type: call
pid: 1988
cid: 2344
type: call
pid: 1988
cid: 2429
type: call
pid: 1988
cid: 2552
type: call
pid: 1988
cid: 2598
type: call
pid: 1988
cid: 2638
process: svchost.exe

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

type: call
pid: 3496
cid: 89
type: call
pid: 1988
cid: 121
type: call
pid: 1988
cid: 168
type: call
pid: 1988
cid: 222
type: call
pid: 1988
cid: 266
type: call
pid: 1988
cid: 313
type: call
pid: 1988
cid: 382
type: call
pid: 1988
cid: 438
type: call
pid: 1988
cid: 562
type: call
pid: 1988
cid: 612
type: call
pid: 1988
cid: 1339
type: call
pid: 1988
cid: 1536

CAPE extracted potentially suspicious content

explorer_exe: SmokeLoader

Creates RWX memory

type: call
pid: 3496
cid: 18

Performs some HTTP requests

url: http://humydrole.com/tmp/index.php

A system process is generating network traffic likely as a result of process injection

network_connection: explorer.exe_WSASend_post /tmp/index.php http/1.1 connection: keep-alive content-type: application/x-www-form-urlencoded accept: */* referer: http://vbknthgegfteqy.org/ user-agent: mozilla/4.0 (compatible; msie 8.0; windows nt 6.1; win64; x64; trident/4.0; .net clr 2.0.50727; slcc2; .net clr 3.5.30729; .net clr 3.0.30729; .net4.0c; .net4.0e) content-length: 217 host: humydrole.com
type: call
pid: 1988
cid: 897
network_connection: explorer.exe_WSASend_;nr\x18\x86\xc3h/\xd6\xa2\xc2qs ~\xbc}x\xcb\xedj\x00\xe5\x17}zs\x93h\xb1\xcf\x1e\xeex\xc6)\x01j#i\xec\x9c?\xc2"6\xbc\xf3l\xfa\x1at\xef \x0f\xf7m@\x17\x7fn\xe2\x1b\x1d\xc7\x80 \xff.[k,\x90\xf4v\x0buk \xc1\xe4y>\xe3\xd6\xe8q\x00\xd6\xd1\xc0\xc8\xe3 \x7f\xd7\xce\xf7\xd4\xaej\xdc\x9e\xea(\x83\x16\x07y\x06\x16c\x85v\x82\x1fi\xe8\xda\x9f\xed\xaa\x9b\x02\\xee\xc2\xc6\x18\xc5 \xa5\x14\xe69\xb3)u7\xaa\x08l\xbdfa"&\xf4p\x90\xa4\xd1\xf2\xff\x9a\xa0\xfd\x86m\xd4\xd6\xcc(a\xfe\x0e:\xa6\x90\x06\x81i[)\xfe\xe9\x b7\xf4\xc6\xb0\x88\xe5\x8f\xc0\x05d\xe2\xde\xf8d\xbe\xf6\xd5"\xb86\xc2\x91\x86\xd2\xbb\xff\xa1\x80)`\xee\xef\xd1\x15\x06\xd2\xc8\x cd#"
type: call
pid: 1988
cid: 898

Detects Avast Antivirus through the presence of a library

type: call
pid: 3496
cid: 66

Detects Sandboxie through the presence of a library

type: call
pid: 3496
cid: 64

Checks the presence of disk drives in the registry, possibly for anti-virtualization

Deletes its original binary from disk

type: call
pid: 1988
cid: 705

Attempts to remove evidence of file being downloaded from the Internet

file: C:\Users\ama\AppData\Roaming\vhbagga:Zone.Identifier
type: call
pid: 1988
cid: 706

Explorer.exe process established HTTP connections

Domain:Port: humydrole.com:80
type: call
pid: 1988
cid: 851
HTTPMethod:URI: POST:/tmp/index.php
type: call
pid: 1988

cid: 852

Yara rule detections observed from a process memory dump/dropped files/CAPE

Hit: PID 1988 trigged the Yara rule 'shellcode_get_eip'
Hit: PID 1988 trigged the Yara rule 'SmokeLoader'
Hit: PID 3496 trigged the Yara rule 'shellcode_patterns'
Hit: PID 3496 trigged the Yara rule 'embedded_pe'

CAPE detected the SmokeLoader malware

SmokeLoader: [{'Yara': '4843deb1bb251604c562234f7a9b81d0346ee72b150300fe48eeb7e46d163157'}]

Screenshots

No screenshots available.

Network Analysis

Hosts Involved

Direct	IP Address	Country Name
N	190.218.32.77	unknown
Y	93.184.220.29	unknown

DNS Requests

Name	Response
humydrole.com	A 187.209.155.200 A 123.213.233.131 A 181.168.176.36 A 175.120.254.9 A 187.228.32.163 A 211.171.233.129 A 14.33.209.147 A 201.119.114.170 A 211.119.84.112 A 190.218.32.77

TCP Connections

IP Address	Port
190.218.32.77	80

UDP Connections

IP Address	Port
239.255.255.250	3702
239.255.255.250	3702
239.255.255.250	1900
192.168.122.255	138

HTTP Requests

URL	Data

http://humydrole.com/tmp/index.php	POST /tmp/index.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vbknthgegfteqy.org/ User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Content-Length: 217 Host: humydrole.com

Dropped Files

Nothing to display.

Payloads

4843deb1bb251604c562234f7a9b81d0346ee72b150300fe48eeb7e46d163157
cd1166628963f9db3681a8f7fa4293672fd56b0ccda0245fd4e4e83f8383c2d3
a1e98eaa5d764ee7102955bdabbd99ee429c71d3c743345e8dd2ab9f4b004454
622e1de69f658b77d194d72c4682eb5f97327a24f5349c8a3cc66661963618b8

Behavior Summary

Mutexes
- 282908983CE8432C3810BDE7979C8EE710660A23

Executed Commands
Nothing to display.

Created Services
Nothing to display.

Started Services
Nothing to display.

Processes

3928.exe PID: 3496, Parent PID: 4028
explorer.exe PID: 1988, Parent PID: 1932
svchost.exe PID: 848, Parent PID: 484

Accessed Files
- C:\Windows\System32\ntdll.dll
- C:\Users\Public\Desktop\Acrobat Reader DC.lnk
- C:\
- C:\Program Files (x86)
- C:\Program Files (x86)\desktop.ini
- C:\Users\ama\AppData\Roaming\vhbagga
- C:\Users\ama\AppData\Local\Temp\3928.exe
- C:\Users\ama\AppData\Roaming\vhbagga:Zone.Identifier
- C:\Windows\System32\advapi32.dll
- C:\Users\ama\AppData\Roaming\cicjaij
- C:\Users\ama\Desktop
- C:\Users\ama\Desktop\
- C:\Users\ama
- C:\Users\ama\
- C:\Users

- C:\Users\
- C:
- \??\MountPointManager
- C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll
- C:\Users\ama\Desktop\oficializado.xlsx
- C:\Windows\System32\Tasks
- C:\Windows\System32\Tasks\
- C:\Windows\System32\Tasks\Adobe Acrobat Update Task
- C:\Windows\System32\Tasks\Firefox Default Browser Agent 282908983CE8432C
- C:\Windows\Tasks\Firefox Default Browser Agent 282908983CE8432C.job
- \Device\LanmanDatagramReceiver

Read Files
- C:\Users\ama\AppData\Local\Temp\3928.exe

Modified Files
- C:\Users\ama\AppData\Roaming\vhbagga

Deleted Files
- C:\Users\ama\AppData\Roaming\vhbagga
- C:\Users\ama\AppData\Local\Temp\3928.exe
- C:\Users\ama\AppData\Roaming\vhbagga:Zone.Identifier
- C:\Windows\Tasks\Firefox Default Browser Agent 282908983CE8432C.job
- C:\Windows\System32\Tasks\Firefox Default Browser Agent 282908983CE8432C

Registry Keys
- DisableUserModeCallbackFilter
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\IDE
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI
- HKEY_CURRENT_USER\Control Panel\Personalization\Desktop Slideshow
- HKEY_CLASSES_ROOT\.lnk
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\(Default)
- HKEY_CLASSES_ROOT\.lnk\OpenWithProgids
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.lnk\OpenWithProgids
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.lnk
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.lnk\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.lnk\UserChoice
- HKEY_CLASSES_ROOT\lnkfile
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\CurVer
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\ShellEx\{00021500-0000-0000-C000-000000000046}\(Default)
- HKEY_CLASSES_ROOT\CLSID\{00021401-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\DisableProcessIsolation
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\NoOplock
- HKEY_CLASSES_ROOT\ExplorerCLSIDFlags\{00021401-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\UseInProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\UseOutOfProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\EnableShareDenyNone
- HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
- HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
- HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\System.NamespaceCLSID
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\{28636AA6-953D-11D2-B5D6-00C04FD918D0} 6
- HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version

- 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\System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
- HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-40-a7-e2
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-40-a7-e2\WpadDecision
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-40-a7-e2\WpadDecisionTime
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
- HKEY_CLASSES_ROOT\.xlsx
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\(Default)
- HKEY_CLASSES_ROOT\.xlsx\OpenWithProgids
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\OpenWithProgids
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice
- HKEY_CLASSES_ROOT\Excel.Sheet.12
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\CurVer
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\ShellEx\DataHandler
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\ShellEx\DataHandler
- HKEY_CLASSES_ROOT\SystemFileAssociations\.xlsx
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\ShellEx\DataHandler
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\PerceivedType
- HKEY_CLASSES_ROOT\SystemFileAssociations\document
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\Clsid
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\CLSID\(Default)
- HKEY_CLASSES_ROOT*
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\ShellEx\DataHandler
- HKEY_CLASSES_ROOT\AllFilesystemObjects
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\ShellEx\DataHandler
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DontUseDelegatingTransfer
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\.xlsx
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\DefaultDropEffect
- HKEY_CLASSES_ROOT\Kind.document
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Kind.Document\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DefaultDropEffect
- 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_CLASSES_ROOT\Folder
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\DragDropHandlers
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\shellex\DragDropHandlers
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR32

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR32\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR32\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\{BD472F60-27FA-11cf-B8B4-444553540000}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\{BD472F60-27FA-11cf-B8B4-444553540000}\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\shellex\DragDropHandlers
- HKEY_CLASSES_ROOT\CLSID\{BD472F60-27FA-11CF-B8B4-444553540000}\shellex\MayChangeDefaultMenu
- HKEY_CLASSES_ROOT\CLSID\{B41DB860-8EE4-11D2-9906-E49FADC173CA}\shellex\MayChangeDefaultMenu
- HKEY_CLASSES_ROOT\CLSID\{B41DB860-64E4-11D2-9906-E49FADC173CA}\shellex\MayChangeDefaultMenu
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\ShellEx\DropHandler
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\shellex\DropHandler\(Default)
- 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\.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\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\ShellEx\DropHandler
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shellex\DropHandler\(Default)
- HKEY_CLASSES_ROOT\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\DisableProcessIsolation
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\NoOplock
- HKEY_CLASSES_ROOT\ExplorerCLSIDFlags\{86C86720-42A0-1069-A2E8-08002B30309D}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\UseInProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\UseOutOfProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\ShellEx\{00021500-0000-0000-C000-000000000046}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\InfoTip
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\InfoTip
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\OTNEEDSSFCACHE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NO_WEBVIEW
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\UNBINDABLE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\PINDLL
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NEEDSFILESYSANCESTOR
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOTAFILESYSTEM
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_NOVERBS
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_LIMITEDQI
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\COCREATESHELLFOLDERONLY
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NEEDSSTORAGEANCESTOR
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOLEGACYWEBVIEW
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_XPQCMFLAGS
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOIPROPERTYSTORE

- HKEY_CLASSES_ROOT\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\InProcServer32
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\InprocServer32\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\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\{993be281-6695-4ba5-8a2a-7aacbfaab69e}\InProcServer32
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\msoshext.dll
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E} {0000013A-0000-0000-C000-000000000046} 0xFFFF
- HKEY_CLASSES_ROOT\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\EnableShareDenyNone
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\14.0\Common\Security
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Security
- HKEY_CURRENT_USER\Software\Microsoft\Security
- HKEY_CLASSES_ROOT\CLSID
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{88d96a0c-f192-11d4-a65f-0040963251e5}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{88D96A0C-F192-11D4-A65F-0040963251E5}\InsecureQI
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\14.0\Common\OpenXMLFormat
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common
- HKEY_CURRENT_USER\Software\Microsoft\Office\Common\AllowConsecutiveSlashesInUrlPathComponent
- HKEY_LOCAL_MACHINE\Software\Microsoft\Msxml60
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\FriendlyTypeName
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\(Default)
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\PropertySystem
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PropertySystem\FormatForDisplayHelper
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\Romance Standard Time\Dynamic DST

Read Registry Keys

- DisableUserModeCallbackFilter
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\ShellEx\{00021500-0000-0000-C000-000000000046}\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\DisableProcessIsolation
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\NoOplock
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\UseInProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\UseOutOfProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00021401-0000-0000-C000-000000000046}\EnableShareDenyNone
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\System.NamespaceCLSID
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\{28636AA6-953D-11D2-B5D6-00C04FD918D0} 6
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-40-a7-e2\WpadDecision
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-40-a7-e2\WpadDecisionTime
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.xlsx\PerceivedType
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\CLSID\(Default)
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DontUseDelegatingTransfer
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\.xlsx
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Kind.Document\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes*\DefaultDropEffect
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DefaultDropEffect

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR32\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\WinRAR32\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Folder\ShellEx\DragDropHandlers\{BD472F60-27FA-11cf-B8B4-444553540000}\SuppressionPolicy
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\lnkfile\shellex\DropHandler\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\IsShortcut
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shellex\DropHandler\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\DisableProcessIsolation
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\NoOplock
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\UseInProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{86C86720-42A0-1069-A2E8-08002B30309D}\UseOutOfProcHandlerCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\InfoTip
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.xlsx\InfoTip
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\OTNEEDSSFCACHE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NO_WEBVIEW
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\UNBINDABLE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\PINDLL
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NEEDSFILESYSANCESTOR
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOTAFILESYSTEM
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_NOVERBS
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_LIMITEDQI
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\COCREATESHELLFOLDERONLY
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NEEDSSTORAGEANCESTOR
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOLEGACYWEBVIEW
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\CTXMENU_XPQCMFLAGS
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\NOIPROPERTYSTORE
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\InprocServer32\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\InprocServer32\LoadWithoutCOM
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E} {0000013A-0000-0000-C000-000000000046} 0xFFFF
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{993BE281-6695-4BA5-8A2A-7AACBFAAB69E}\EnableShareDenyNone
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{88D96A0C-F192-11D4-A65F-0040963251E5}\InsecureQI
- HKEY_CURRENT_USER\Software\Microsoft\Office\Common\AllowConsecutiveSlashesInUrlPathComponent
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\FriendlyTypeName
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Excel.Sheet.12\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PropertySystem\FormatForDisplayHelper

Modified Registry Keys

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA

Deleted Registry Keys

Nothing to display.

Resolved APIs

- kernel32.dll.FlsAlloc
- kernel32.dll.FlsGetValue

- kernel32.dll.FlsSetValue
- kernel32.dll.FlsSetValue
- kernel32.dll.FlsFree
- kernel32.dll.VirtualProtect
- kernel32.dll.GlobalAlloc
- kernel32.dll.GetLastError
- kernel32.dll.Sleep
- kernel32.dll.VirtualAlloc
- kernel32.dll.CreateToolhelp32Snapshot
- kernel32.dll.Module32First
- kernel32.dll.CloseHandle
- kernel32.dll.LoadLibraryA
- kernel32.dll.VirtualFree
- kernel32.dll.GetVersionExA
- kernel32.dll.TerminateProcess
- kernel32.dll.ExitProcess
- kernel32.dll.SetErrorMode
- ntdll.dll.RtlExitUserThread
- cryptsp.dll.CryptHashData
- cryptsp.dll.CryptGetHashParam
- cryptsp.dll.CryptDestroyHash
- cryptsp.dll.CryptReleaseContext
- advapi32.dll.LookupAccountNameW
- xmllite.dll.CreateXmlWriter
- xmllite.dll.CreateXmlWriterOutputWithEncodingName
- ole32.dll.CoInitializeEx
- advapi32.dll.RegDeleteTreeA
- advapi32.dll.RegDeleteTreeW
- ole32.dll.CoTaskMemAlloc
- ole32.dll.StringFromIID
- nsi.dll.NsiAllocateAndGetTable
- cfgmgr32.dll.CM_Open_Class_Key_ExW
- iphlpapi.dll.ConvertInterfaceGuidToLuid
- iphlpapi.dll.GetIfEntry2
- iphlpapi.dll.GetIpForwardTable2
- iphlpapi.dll.GetIpNetEntry2
- iphlpapi.dll.FreeMibTable
- ole32.dll.CoTaskMemFree
- nsi.dll.NsiFreeTable
- ole32.dll.CoUninitialize
- shlwapi.dll.StrCmpNW
- ws2_32.dll.GetAddrInfoW
- ws2_32.dll.WSASocketW
- ws2_32.dll.#2
- ws2_32.dll.#21
- ws2_32.dll.#9
- ws2_32.dll.WSAIoctl
- ws2_32.dll.FreeAddrInfoW
- ws2_32.dll.#6
- ws2_32.dll.#5
- ws2_32.dll.WSARecv
- ws2_32.dll.WSASend
- ws2_32.dll.#22
- ws2_32.dll.#3
- ws2_32.dll.#116
- comctl32.dll.#329
- comctl32.dll.#321
- comctl32.dll.#386