ДОДАТОК А

Список використаних ознак

1. MS-DOS Stub/e_lfanew
2. MS-DOS Stub/e_crlc
3. Coff Header/NumberOfSections
4. Coff Header/NumberOfSymbols
5. Coff Header/PointerToSymbolTable
6. Coff Header/SizeOfOptionalHeader
7. Coff Header/Characteristics
8. Optional Header/SizeOfInitializedData
9. Optional Header/SizeOfUninitializedData
10. Optional Header/BaseOfCode
11. Optional Header/DllCharacteristics
12. Optional Header/SizeOfStackReserve
13. Optional Header/SizeOfHeapReserve
14. Optional Header/SectionAlignment
15. Optional Header/SizeOfHeapCommit
16. Optional Header/FileAlignment
17. Optional Header/SizeOfImage
18. Optional Header/NumberOfRvaAndSizes
19. Optional Header/SizeOfHeaders
20. Optional Header/SizeOfStackCommit
21. DLL Referred/Gdiplus.dll
22. DLL Referred/Rpcrt4.dll
23. DLL Referred/Comdlg32.dll
24. DLL Referred/Wtsapi32.dll
25. DLL Referred/Imm32.dll
26. DLL Referred/Mscoree.dll
27. DLL Referred/Gdi32.dll
28. DLL Referred/Oleacc.dll
29. DLL Referred/Version.dll
30. DLL Referred/Userenv.dll
31. DLL Referred/Msvcrt.dll
32. DLL Referred/Shell32.dll
33. DLL Referred/Wintrust.dll
34. DLL Referred/Uxtheme.dll
35. DLL Referred/Wininet.dll
36. DLL Referred/Iphlpapi.dll
37. DLL Referred/Winspool.drv
38. DLL Referred/Winmm.dll
39. DLL Referred/Setupapi.dll
40. DLL Referred/Advapi32.dll
41. DLL Referred/Ole32.dll
42. DLL Referred/Shlwapi.dll
43. DLL Referred/Ntdll.dll
44. DLL Referred/Mpr.dll
45. DLL Referred/Netapi32.dll
46. DLL Referred/User32.dll
47. DLL Referred/Oleaut32.dll
48. DLL Referred/Urlmon.dll
49. DLL Referred/Comctl32.dll
50. DLL Referred/Crypt32.dll
51. DLL Referred/Ws2_32.dll
52. DLL Referred/Psapi.dll
53. DLL Referred/Msimg32.dll
54. API Referred/Createfilew
55. API Referred/Createfilea
56. API Referred/Getmodulehandlew
57. API Referred/Getmodulehandlea

58. API Referred/Getmodulehandleexw
59. API Referred/Heapsetinformation
60. API Referred/Loadlibrarya
61. API Referred/Rtllookupfunctionentry
62. API Referred/Virtualalloc
63. API Referred/Openprocesstoken
64. API Referred/Openprocess
65. API Referred/Rtlcapturecontext
66. API Referred/Setunhandledexceptionfilter
67. API Referred/Getenv
68. API Referred/Createprocessasusera
69. API Referred/Createprocessasuserw
70. API Referred/Duplicatehandle
71. API Referred/Loadicona
72. API Referred/Virtualprotect
73. API Referred/Virtualprotectex
74. API Referred/Writeprocessmemory
75. API Referred/Createdirectorya
76. API Referred/Createdirectoryw
77. API Referred/Rtlvirtualunwind
78. API Referred/Openfile
79. API Referred/Reopenfile
80. API Referred/Ntcreatefile
81. API Referred/Ntsetinformationfile
82. API Referred/Setfileinformationbyhandle
83. API Referred/Movefilea
84. API Referred/Movefilew
85. API Referred/Movefileexa
86. API Referred/Movefileexw
87. API Referred/Copyfilea
88. API Referred/Copyfilew
89. API Referred/Copyfileexw
90. API Referred/Copyfileexa
91. API Referred/Ntopenfile
92. API Referred/Deletefilew
93. API Referred/Deletefilea
94. API Referred/Findfirstfilea
95. API Referred/Findfirstfilew
96. API Referred/Findfirstfileexa
97. API Referred/Findfirstfileexw
98. API Referred/Replacefilea
99. API Referred/Replacefilew
100. API Referred/Writefile
101. API Referred/Writefileex
102. API Referred/Suspendthread
103. API Referred/Ntsuspendprocess
104. API Referred/Ntsuspendthread
105. Section/text
106. Section/data
107. Section/rsrc
108. Section/rdata
109. Section/reloc
110. General/NumberOfReferredDLLs
111. General/NumberOfReferredAPIs
112. General/NumberOfReferredAPIOrdinals
113. General/NumberOfSections
114. General/NumberOfExportTableSymbols
115. General/NumberOfRelocSectionItems

ДОДАТОК Б

Результат роботи програми

Витяг даних з заголовку

```
----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0         0x0   e_magic:                       0x5A4D
0x2         0x2   e_cblp:                        0x50
0x4         0x4   e_cp:                          0x2
0x6         0x6   e_crlc:                        0x0
0x8         0x8   e_cparhdr:                     0x4
0xA         0xA   e_minalloc:                    0xF
0xC         0xC   e_maxalloc:                    0xFFFF
0xE         0xE   e_ss:                          0x0
0x10        0x10  e_sp:                          0xB8
0x12        0x12  e_csum:                        0x0
0x14        0x14  e_ip:                          0x0
0x16        0x16  e_cs:                          0x0
0x18        0x18  e_lfarlc:                      0x40
0x1A        0x1A  e_ovno:                        0x1A
0x1C        0x1C  e_res:
0x24        0x24  e_oemid:                       0x0
0x26        0x26  e_oeminfo:                     0x0
0x28        0x28  e_res2:
0x3C        0x3C  e_lfanew:                      0x100

----------NT_HEADERS----------

[IMAGE_NT_HEADERS]
0x100       0x0   Signature:                     0x4550

----------FILE_HEADER----------

[IMAGE_FILE_HEADER]
0x104       0x0   Machine:                       0x14C
0x106       0x2   NumberOfSections:              0x8
0x108        0x4    TimeDateStamp:                   0x5B226D52 [Thu Jun 14
13:27:46 2018 UTC]
0x10C       0x8   PointerToSymbolTable:          0x0
0x110       0xC   NumberOfSymbols:              0x0
0x114       0x10  SizeOfOptionalHeader:         0xE0
0x116       0x12  Characteristics:              0x818F
Flags:        IMAGE_FILE_32BIT_MACHINE,       IMAGE_FILE_BYTES_REVERSED_HI,
IMAGE_FILE_BYTES_REVERSED_LO,                   IMAGE_FILE_EXECUTABLE_IMAGE,
IMAGE_FILE_LINE_NUMS_STRIPPED,                IMAGE_FILE_LOCAL_SYMS_STRIPPED,
IMAGE_FILE_RELOCS_STRIPPED

----------OPTIONAL_HEADER----------

[IMAGE_OPTIONAL_HEADER]
0x118       0x0   Magic:                         0x10B
0x11A       0x2   MajorLinkerVersion:            0x2
0x11B       0x3   MinorLinkerVersion:            0x19
0x11C       0x4   SizeOfCode:                    0x10400
0x120       0x8   SizeOfInitializedData:         0x52400
0x124       0xC   SizeOfUninitializedData:       0x0
0x128       0x10  AddressOfEntryPoint:           0x1181C
0x12C       0x14  BaseOfCode:                    0x1000
```

```
      0x130      0x18  BaseOfData:                    0x12000
      0x134      0x1C  ImageBase:                     0x400000
      0x138      0x20  SectionAlignment:              0x1000
      0x13C      0x24  FileAlignment:                 0x200
      0x140      0x28  MajorOperatingSystemVersion:   0x5
      0x142      0x2A  MinorOperatingSystemVersion:   0x0
      0x144      0x2C  MajorImageVersion:             0x6
      0x146      0x2E  MinorImageVersion:             0x0
      0x148      0x30  MajorSubsystemVersion:         0x5
      0x14A      0x32  MinorSubsystemVersion:         0x0
      0x14C      0x34  Reserved1:                     0x0
      0x150      0x38  SizeOfImage:                   0x6D000
      0x154      0x3C  SizeOfHeaders:                 0x400
      0x158      0x40  CheckSum:                      0x3D140DE
      0x15C      0x44  Subsystem:                     0x2
      0x15E      0x46  DllCharacteristics:            0x8140
      0x160      0x48  SizeOfStackReserve:           0x100000
      0x164      0x4C  SizeOfStackCommit:            0x4000
      0x168      0x50  SizeOfHeapReserve:            0x100000
      0x16C      0x54  SizeOfHeapCommit:             0x1000
      0x170      0x58  LoaderFlags:                   0x0
      0x174      0x5C  NumberOfRvaAndSizes:          0x10
      DllCharacteristics:                 IMAGE_DLLCHARACTERISTICS_DYNAMIC_BASE,
IMAGE_DLLCHARACTERISTICS_NX_COMPAT,
IMAGE_DLLCHARACTERISTICS_TERMINAL_SERVER_AWARE

      ----------PE Sections----------

      [IMAGE_SECTION_HEADER]
      0x1F8      0x0   Name:                          .text
      0x200      0x8   Misc:                          0xF25C
      0x200      0x8   Misc_PhysicalAddress:          0xF25C
      0x200      0x8   Misc_VirtualSize:              0xF25C
      0x204      0xC   VirtualAddress:                0x1000
      0x208      0x10  SizeOfRawData:                 0xF400
      0x20C      0x14  PointerToRawData:              0x400
      0x210      0x18  PointerToRelocations:          0x0
      0x214      0x1C  PointerToLinenumbers:          0x0
      0x218      0x20  NumberOfRelocations:           0x0
      0x21A      0x22  NumberOfLinenumbers:           0x0
      0x21C      0x24  Characteristics:               0x60000020
      Flags: IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
      Entropy: 6.375879 (Min=0.0, Max=8.0)
      MD5     hash: 0da5d73ffbc41792fa65a09058a91476
      SHA-1   hash: 1398791fc2e15be62c9d251bc6b2f5256af1e5f9
      SHA-256                                                              hash:
869e41576cc4d9d095cf7061aa84a29c4c0e5f25b3fe67afc3203e016df397ef
      SHA-512                                                              hash:
591ff9995d3aed34fe2b940323049049dee39500470e7d89f4511856bc8b841049a5ce64fe6cdbdc
b05e29c55ac6dae3e21de0cc0f1f22cfd77abbbaa96e4db4

      [IMAGE_SECTION_HEADER]
      0x220      0x0   Name:                          .itext
      0x228      0x8   Misc:                          0xFA4
      0x228      0x8   Misc_PhysicalAddress:          0xFA4
      0x228      0x8   Misc_VirtualSize:              0xFA4
      0x22C      0xC   VirtualAddress:                0x11000
      0x230      0x10  SizeOfRawData:                 0x1000
      0x234      0x14  PointerToRawData:              0xF800
      0x238      0x18  PointerToRelocations:          0x0
      0x23C      0x1C  PointerToLinenumbers:          0x0
      0x240      0x20  NumberOfRelocations:           0x0
      0x242      0x22  NumberOfLinenumbers:           0x0
      0x244      0x24  Characteristics:               0x60000020
```

```
      Flags: IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
      Entropy: 5.778765 (Min=0.0, Max=8.0)
      MD5     hash: 2eb275566563c3f1d0099a0da7345b74
      SHA-1   hash: 7e44497b20e01a93ca6cf7b5c2c2ea1a01732fcc
      SHA-256                                                         hash:
10547a7743fcc09490636c8cf3d7704c8d4a99356bf9ea3b3dc998e851fed777
      SHA-512                                                         hash:
ac2e78f0ba03d173bf423d99c1688b903b7e4550ef2aa68eade732948ca9b5e5ac235012d647ac69
ae78d2bc8035db1a7fe207752376aa9900db624fcd245471

      [IMAGE_SECTION_HEADER]
      0x248      0x0   Name:                          .data
      0x250      0x8   Misc:                          0xC8C
      0x250      0x8   Misc_PhysicalAddress:          0xC8C
      0x250      0x8   Misc_VirtualSize:             0xC8C
      0x254      0xC   VirtualAddress:                0x12000
      0x258      0x10  SizeOfRawData:                 0xE00
      0x25C      0x14  PointerToRawData:              0x10800
      0x260      0x18  PointerToRelocations:          0x0
      0x264      0x1C  PointerToLinenumbers:          0x0
      0x268      0x20  NumberOfRelocations:           0x0
      0x26A      0x22  NumberOfLinenumbers:           0x0
      0x26C      0x24  Characteristics:               0xC0000040
      Flags:          IMAGE_SCN_CNT_INITIALIZED_DATA,         IMAGE_SCN_MEM_READ,
IMAGE_SCN_MEM_WRITE
      Entropy: 2.302829 (Min=0.0, Max=8.0)
      MD5     hash: 73b859e23f5fd17e00c08db2e0e73dfe
      SHA-1   hash: c8610dc108300c199c915d1a355f792b45afc912
      SHA-256                                                         hash:
01e152d7661f7b4da228ca9bbdb1428d058dc976ae49b38c11a53285a2cc5076
      SHA-512                                                         hash:
6df78eda11800159d0231a1d91750dc92f02db669b4347b7e6f35681deb86aab13291927762bb651
7c5ba1ada394d6d7251e0be47ac37fbff784e6433e2bdded

      [IMAGE_SECTION_HEADER]
      0x270      0x0   Name:                          .bss
      0x278      0x8   Misc:                          0x56BC
      0x278      0x8   Misc_PhysicalAddress:          0x56BC
      0x278      0x8   Misc_VirtualSize:             0x56BC
      0x27C      0xC   VirtualAddress:                0x13000
      0x280      0x10  SizeOfRawData:                 0x0
      0x284      0x14  PointerToRawData:              0x11600
      0x288      0x18  PointerToRelocations:          0x0
      0x28C      0x1C  PointerToLinenumbers:          0x0
      0x290      0x20  NumberOfRelocations:           0x0
      0x292      0x22  NumberOfLinenumbers:           0x0
      0x294      0x24  Characteristics:               0xC0000000
      Flags: IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
      Entropy: 0.000000 (Min=0.0, Max=8.0)
      MD5     hash: d41d8cd98f00b204e9800998ecf8427e
      SHA-1   hash: da39a3ee5e6b4b0d3255bfef95601890afd80709
      SHA-256                                                         hash:
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
      SHA-512                                                         hash:
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0
ff8318d2877eec2f63b931bd47417a81a538327af927da3e

      [IMAGE_SECTION_HEADER]
      0x298      0x0   Name:                          .idata
      0x2A0      0x8   Misc:                          0xE04
      0x2A0      0x8   Misc_PhysicalAddress:          0xE04
      0x2A0      0x8   Misc_VirtualSize:             0xE04
      0x2A4      0xC   VirtualAddress:                0x19000
      0x2A8      0x10  SizeOfRawData:                 0x1000
```

```
      0x2AC      0x14  PointerToRawData:              0x11600
      0x2B0      0x18  PointerToRelocations:          0x0
      0x2B4      0x1C  PointerToLinenumbers:          0x0
      0x2B8      0x20  NumberOfRelocations:           0x0
      0x2BA      0x22  NumberOfLinenumbers:           0x0
      0x2BC      0x24  Characteristics:               0xC0000040
      Flags:         IMAGE_SCN_CNT_INITIALIZED_DATA,         IMAGE_SCN_MEM_READ,
IMAGE_SCN_MEM_WRITE
      Entropy: 4.597813 (Min=0.0, Max=8.0)
      MD5     hash: e9b9c0328fd9628ad4d6ab8283dcb20e
      SHA-1   hash: fd2927174e310130a51bdd648aefde6f89fe0007
      SHA-256                                                              hash:
68a126ba6dddfa52cdc395cca81ae415921071acf02f75b7c00faf9d90353760
      SHA-512                                                              hash:
af00e72b51284f9ca30001699d09bb898f36339a008b7955fbaf0b0e24e3c70242196b3d4dff0456
fbe34c2b15eaea5c0524f8cb10e63fe708f23b040784ad50

      [IMAGE_SECTION_HEADER]
      0x2C0      0x0   Name:                        .tls
      0x2C8      0x8   Misc:                        0x8
      0x2C8      0x8   Misc_PhysicalAddress:        0x8
      0x2C8      0x8   Misc_VirtualSize:           0x8
      0x2CC      0xC   VirtualAddress:              0x1A000
      0x2D0      0x10  SizeOfRawData:              0x0
      0x2D4      0x14  PointerToRawData:           0x12600
      0x2D8      0x18  PointerToRelocations:       0x0
      0x2DC      0x1C  PointerToLinenumbers:       0x0
      0x2E0      0x20  NumberOfRelocations:        0x0
      0x2E2      0x22  NumberOfLinenumbers:        0x0
      0x2E4      0x24  Characteristics:            0xC0000000
      Flags: IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
      Entropy: 0.000000 (Min=0.0, Max=8.0)
      MD5     hash: d41d8cd98f00b204e9800998ecf8427e
      SHA-1   hash: da39a3ee5e6b4b0d3255bfef95601890afd80709
      SHA-256                                                              hash:
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
      SHA-512                                                              hash:
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0
ff8318d2877eec2f63b931bd47417a81a538327af927da3e

      [IMAGE_SECTION_HEADER]
      0x2E8      0x0   Name:                        .rdata
      0x2F0      0x8   Misc:                        0x18
      0x2F0      0x8   Misc_PhysicalAddress:        0x18
      0x2F0      0x8   Misc_VirtualSize:           0x18
      0x2F4      0xC   VirtualAddress:              0x1B000
      0x2F8      0x10  SizeOfRawData:              0x200
      0x2FC      0x14  PointerToRawData:           0x12600
      0x300      0x18  PointerToRelocations:       0x0
      0x304      0x1C  PointerToLinenumbers:       0x0
      0x308      0x20  NumberOfRelocations:        0x0
      0x30A      0x22  NumberOfLinenumbers:        0x0
      0x30C      0x24  Characteristics:            0x40000040
      Flags: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
      Entropy: 0.204488 (Min=0.0, Max=8.0)
      MD5     hash: 3dffc444ccc131c9dcee18db49ee6403
      SHA-1   hash: 45d8f890e32cc1adf7ded113fd19004c8869f419
      SHA-256                                                              hash:
821b0bda5922cc6f5fb74fb3a160e39c97727c21beb1ecf4f96e3bcfad9edbe3
      SHA-512                                                              hash:
7b89dc6e494138a29cea003424aeed055989e97f9497cbbfcc9151479ca6760613273ac48ac569e1
bed9f558f78aadfd399d6a5b220e5707d5a20610dbc3b258

      [IMAGE_SECTION_HEADER]
```

```
      0x310      0x0   Name:                          .rsrc
      0x318      0x8   Misc:                          0x50300
      0x318      0x8   Misc_PhysicalAddress:          0x50300
      0x318      0x8   Misc_VirtualSize:              0x50300
      0x31C      0xC   VirtualAddress:                0x1C000
      0x320      0x10  SizeOfRawData:                 0x50400
      0x324      0x14  PointerToRawData:              0x12800
      0x328      0x18  PointerToRelocations:          0x0
      0x32C      0x1C  PointerToLinenumbers:          0x0
      0x330      0x20  NumberOfRelocations:          0x0
      0x332      0x22  NumberOfLinenumbers:          0x0
      0x334      0x24  Characteristics:              0x40000040
      Flags: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
      Entropy: 4.708451 (Min=0.0, Max=8.0)
      MD5     hash: 9b5d81d1269cb8726c27b52f9968575f
      SHA-1   hash: 46f4c4586b79f6d2033eaef3fc5040ef9ea9e325
      SHA-256                                                                hash:
2d06190a40947b450a5df419fdbf840bcfa6d73556cc8230a50c0b23ae6d6822
      SHA-512                                                                hash:
7f2596cbf9f70a114b35a261835dd7e38fd48a5de3a9cc9540fd1a345c59ab14d02eaa8cf75b6d48
5ecef11cd4fb72fbfe95e43a9eb0d6411d25f3c9fd91383e

      ----------Directories----------

      [IMAGE_DIRECTORY_ENTRY_EXPORT]
      0x178      0x0   VirtualAddress:                0x0
      0x17C      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_IMPORT]
      0x180      0x0   VirtualAddress:                0x19000
      0x184      0x4   Size:                          0xE04
      [IMAGE_DIRECTORY_ENTRY_RESOURCE]
      0x188      0x0   VirtualAddress:                0x1C000
      0x18C      0x4   Size:                          0x50300
      [IMAGE_DIRECTORY_ENTRY_EXCEPTION]
      0x190      0x0   VirtualAddress:                0x0
      0x194      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_SECURITY]
      0x198      0x0   VirtualAddress:                0x3D0B1F8
      0x19C      0x4   Size:                          0x2440
      [IMAGE_DIRECTORY_ENTRY_BASERELOC]
      0x1A0      0x0   VirtualAddress:                0x0
      0x1A4      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_DEBUG]
      0x1A8      0x0   VirtualAddress:                0x0
      0x1AC      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_COPYRIGHT]
      0x1B0      0x0   VirtualAddress:                0x0
      0x1B4      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_GLOBALPTR]
      0x1B8      0x0   VirtualAddress:                0x0
      0x1BC      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_TLS]
      0x1C0      0x0   VirtualAddress:                0x1B000
      0x1C4      0x4   Size:                          0x18
      [IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG]
      0x1C8      0x0   VirtualAddress:                0x0
      0x1CC      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT]
      0x1D0      0x0   VirtualAddress:                0x0
      0x1D4      0x4   Size:                          0x0
      [IMAGE_DIRECTORY_ENTRY_IAT]
      0x1D8      0x0   VirtualAddress:                0x19304
      0x1DC      0x4   Size:                          0xрис4
      [IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT]
```

```
0x1E0      0x0   VirtualAddress:                0x0
0x1E4      0x4   Size:                         0x0
[IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR]
0x1E8      0x0   VirtualAddress:                0x0
0x1EC      0x4   Size:                         0x0
[IMAGE_DIRECTORY_ENTRY_RESERVED]
0x1F0      0x0   VirtualAddress:                0x0
0x1F4      0x4   Size:                         0x0

----------Version Information----------

[VS_VERSIONINFO]
0x61FE0    0x0   Length:                       0x4F4
0x61FE2    0x2   ValueLength:                  0x34
0x61FE4    0x4   Type:                         0x0

[VS_FIXEDFILEINFO]
0x62008    0x0   Signature:                    0xFEEF04BD
0x6200C    0x4   StrucVersion:                 0x10000
0x62010    0x8   FileVersionMS:                0x80027
0x62014    0xC   FileVersionLS:                0xB4
0x62018    0x10  ProductVersionMS:             0x80027
0x6201C    0x14  ProductVersionLS:             0xB4
0x62020    0x18  FileFlagsMask:                0x3F
0x62024    0x1C  FileFlags:                    0x0
0x62028    0x20  FileOS:                       0x4
0x6202C    0x24  FileType:                     0x1
0x62030    0x28  FileSubtype:                  0x0
0x62034    0x2C  FileDateMS:                   0x0
0x62038    0x30  FileDateLS:                   0x0

[StringFileInfo]
0x6203C    0x0   Length:                       0x452
0x6203E    0x2   ValueLength:                  0x0
0x62040    0x4   Type:                         0x1

  [StringTable]
  0x62060    0x0   Length:                       0x42E
  0x62062    0x2   ValueLength:                  0x0
  0x62064    0x4   Type:                         0x1
  LangID: 040904e4

    Comments: This installation was built with Inno Setup.
    CompanyName: MS S.A.
    FileDescription: Windex Setup
    FileVersion: 8.39.0.180
    LegalCopyright: (c) 2019 MS
    ProductName: Windex
    ProductVersion: 1.39

[VarFileInfo]
0x62490    0x0   Length:                       0x44
0x62492    0x2   ValueLength:                  0x0
0x62494    0x4   Type:                         0x1

  [Var]
  0x624B0    0x0   Length:                       0x24
  0x624B2    0x2   ValueLength:                  0x4
  0x624B4    0x4   Type:                         0x0
    Translation: 0x0409 0x04e4

----------Imported symbols----------

[IMAGE_IMPORT_DESCRIPTOR]
```

```
      0x11600    0x0   OriginalFirstThunk:           0x190F0
      0x11600    0x0   Characteristics:              0x190F0
      0x11604    0x4   TimeDateStamp:                   0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11608    0x8   ForwarderChain:               0x0
      0x1160C    0xC   Name:                         0x19518
      0x11610    0x10  FirstThunk:                  0x19304

      oleaut32.dll.SysFreeString Hint[0]
      oleaut32.dll.SysReAllocStringLen Hint[0]
      oleaut32.dll.SysAllocStringLen Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x11614    0x0   OriginalFirstThunk:           0x19100
      0x11614    0x0   Characteristics:              0x19100
      0x11618    0x4   TimeDateStamp:                   0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x1161C    0x8   ForwarderChain:               0x0
      0x11620    0xC   Name:                         0x19560
      0x11624    0x10  FirstThunk:                  0x19314

      advapi32.dll.RegQueryValueExW Hint[0]
      advapi32.dll.RegOpenKeyExW Hint[0]
      advapi32.dll.RegCloseKey Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x11628    0x0   OriginalFirstThunk:           0x19110
      0x11628    0x0   Characteristics:              0x19110
      0x1162C    0x4   TimeDateStamp:                   0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11630    0x8   ForwarderChain:               0x0
      0x11634    0xC   Name:                         0x195A0
      0x11638    0x10  FirstThunk:                  0x19324

      user32.dll.GetKeyboardType Hint[0]
      user32.dll.LoadStringW Hint[0]
      user32.dll.MessageBoxA Hint[0]
      user32.dll.CharNextW Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x1163C    0x0   OriginalFirstThunk:           0x19124
      0x1163C    0x0   Characteristics:              0x19124
      0x11640    0x4   TimeDateStamp:                   0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11644    0x8   ForwarderChain:               0x0
      0x11648    0xC   Name:                         0x195E6
      0x1164C    0x10  FirstThunk:                  0x19338

      kernel32.dll.GetACP Hint[0]
      kernel32.dll.Sleep Hint[0]
      kernel32.dll.VirtualFree Hint[0]
      kernel32.dll.VirtualAlloc Hint[0]
      kernel32.dll.GetSystemInfo Hint[0]
      kernel32.dll.GetTickCount Hint[0]
      kernel32.dll.QueryPerformanceCounter Hint[0]
      kernel32.dll.GetVersion Hint[0]
      kernel32.dll.GetCurrentThreadId Hint[0]
      kernel32.dll.VirtualQuery Hint[0]
      kernel32.dll.WideCharToMultiByte Hint[0]
      kernel32.dll.MultiByteToWideChar Hint[0]
      kernel32.dll.lstrlenW Hint[0]
      kernel32.dll.lstrcpynW Hint[0]
      kernel32.dll.LoadLibraryExW Hint[0]
      kernel32.dll.GetThreadLocale Hint[0]
```

```
      kernel32.dll.GetStartupInfoA Hint[0]
      kernel32.dll.GetProcAddress Hint[0]
      kernel32.dll.GetModuleHandleW Hint[0]
      kernel32.dll.GetModuleFileNameW Hint[0]
      kernel32.dll.GetLocaleInfoW Hint[0]
      kernel32.dll.GetCommandLineW Hint[0]
      kernel32.dll.FreeLibrary Hint[0]
      kernel32.dll.FindFirstFileW Hint[0]
      kernel32.dll.FindClose Hint[0]
      kernel32.dll.ExitProcess Hint[0]
      kernel32.dll.WriteFile Hint[0]
      kernel32.dll.UnhandledExceptionFilter Hint[0]
      kernel32.dll.RtlUnwind Hint[0]
      kernel32.dll.RaiseException Hint[0]
      kernel32.dll.GetStdHandle Hint[0]
      kernel32.dll.CloseHandle Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x11650    0x0   OriginalFirstThunk:           0x191A8
      0x11650    0x0   Characteristics:              0x191A8
      0x11654     0x4    TimeDateStamp:                 0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11658    0x8   ForwarderChain:              0x0
      0x1165C    0xC   Name:                        0x1980A
      0x11660    0x10  FirstThunk:                 0x193BC

      kernel32.dll.TlsSetValue Hint[0]
      kernel32.dll.TlsGetValue Hint[0]
      kernel32.dll.LocalAlloc Hint[0]
      kernel32.dll.GetModuleHandleW Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x11664    0x0   OriginalFirstThunk:           0x191BC
      0x11664    0x0   Characteristics:              0x191BC
      0x11668     0x4    TimeDateStamp:                 0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x1166C    0x8   ForwarderChain:              0x0
      0x11670    0xC   Name:                        0x19856
      0x11674    0x10  FirstThunk:                 0x193D0

      user32.dll.CreateWindowExW Hint[0]
      user32.dll.TranslateMessage Hint[0]
      user32.dll.SetWindowLongW Hint[0]
      user32.dll.PeekMessageW Hint[0]
      user32.dll.MsgWaitForMultipleObjects Hint[0]
      user32.dll.MessageBoxW Hint[0]
      user32.dll.LoadStringW Hint[0]
      user32.dll.GetSystemMetrics Hint[0]
      user32.dll.ExitWindowsEx Hint[0]
      user32.dll.DispatchMessageW Hint[0]
      user32.dll.DestroyWindow Hint[0]
      user32.dll.CharUpperBuffW Hint[0]
      user32.dll.CallWindowProcW Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x11678    0x0   OriginalFirstThunk:           0x191F4
      0x11678    0x0   Characteristics:              0x191F4
      0x1167C     0x4    TimeDateStamp:                 0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11680    0x8   ForwarderChain:              0x0
      0x11684    0xC   Name:                        0x1994E
      0x11688    0x10  FirstThunk:                 0x19408

      kernel32.dll.WriteFile Hint[0]
```

```
      kernel32.dll.WideCharToMultiByte Hint[0]
      kernel32.dll.WaitForSingleObject Hint[0]
      kernel32.dll.VirtualQuery Hint[0]
      kernel32.dll.VirtualProtect Hint[0]
      kernel32.dll.VirtualFree Hint[0]
      kernel32.dll.VirtualAlloc Hint[0]
      kernel32.dll.SizeofResource Hint[0]
      kernel32.dll.SignalObjectAndWait Hint[0]
      kernel32.dll.SetLastError Hint[0]
      kernel32.dll.SetFilePointer Hint[0]
      kernel32.dll.SetEvent Hint[0]
      kernel32.dll.SetErrorMode Hint[0]
      kernel32.dll.SetEndOfFile Hint[0]
      kernel32.dll.ResetEvent Hint[0]
      kernel32.dll.RemoveDirectoryW Hint[0]
      kernel32.dll.ReadFile Hint[0]
      kernel32.dll.MultiByteToWideChar Hint[0]
      kernel32.dll.LockResource Hint[0]
      kernel32.dll.LoadResource Hint[0]
      kernel32.dll.LoadLibraryW Hint[0]
      kernel32.dll.GetWindowsDirectoryW Hint[0]
      kernel32.dll.GetVersionExW Hint[0]
      kernel32.dll.GetVersion Hint[0]
      kernel32.dll.GetUserDefaultLangID Hint[0]
      kernel32.dll.GetThreadLocale Hint[0]
      kernel32.dll.GetSystemInfo Hint[0]
      kernel32.dll.GetSystemDirectoryW Hint[0]
      kernel32.dll.GetStdHandle Hint[0]
      kernel32.dll.GetProcAddress Hint[0]
      kernel32.dll.GetModuleHandleW Hint[0]
      kernel32.dll.GetModuleFileNameW Hint[0]
      kernel32.dll.GetLocaleInfoW Hint[0]
      kernel32.dll.GetLastError Hint[0]
      kernel32.dll.GetFullPathNameW Hint[0]
      kernel32.dll.GetFileSize Hint[0]
      kernel32.dll.GetFileAttributesW Hint[0]
      kernel32.dll.GetExitCodeProcess Hint[0]
      kernel32.dll.GetEnvironmentVariableW Hint[0]
      kernel32.dll.GetDiskFreeSpaceW Hint[0]
      kernel32.dll.GetCurrentProcess Hint[0]
      kernel32.dll.GetCommandLineW Hint[0]
      kernel32.dll.GetCPInfo Hint[0]
      kernel32.dll.InterlockedExchange Hint[0]
      kernel32.dll.InterlockedCompareExchange Hint[0]
      kernel32.dll.FreeLibrary Hint[0]
      kernel32.dll.FormatMessageW Hint[0]
      kernel32.dll.FindResourceW Hint[0]
      kernel32.dll.EnumCalendarInfoW Hint[0]
      kernel32.dll.DeleteFileW Hint[0]
      kernel32.dll.CreateProcessW Hint[0]
      kernel32.dll.CreateFileW Hint[0]
      kernel32.dll.CreateEventW Hint[0]
      kernel32.dll.CreateDirectoryW Hint[0]
      kernel32.dll.CloseHandle Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x1168C    0x0   OriginalFirstThunk:           0x192D4
      0x1168C    0x0   Characteristics:              0x192D4
      0x11690     0x4   TimeDateStamp:                  0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x11694    0x8   ForwarderChain:              0x0
      0x11698    0xC   Name:                        0x19D38
      0x1169C    0x10  FirstThunk:                 0x194E8
```

```
      advapi32.dll.RegQueryValueExW Hint[0]
      advapi32.dll.RegOpenKeyExW Hint[0]
      advapi32.dll.RegCloseKey Hint[0]
      advapi32.dll.OpenProcessToken Hint[0]
      advapi32.dll.LookupPrivilegeValueW Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x116A0    0x0   OriginalFirstThunk:           0x192EC
      0x116A0    0x0   Characteristics:              0x192EC
      0x116A4     0x4   TimeDateStamp:                  0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x116A8    0x8   ForwarderChain:               0x0
      0x116AC    0xC   Name:                         0x19DA4
      0x116B0    0x10  FirstThunk:                   0x19500

      comctl32.dll.InitCommonControls Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x116B4    0x0   OriginalFirstThunk:           0x192F4
      0x116B4    0x0   Characteristics:              0x192F4
      0x116B8     0x4   TimeDateStamp:                  0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x116BC    0x8   ForwarderChain:               0x0
      0x116C0    0xC   Name:                         0x19DC8
      0x116C4    0x10  FirstThunk:                   0x19508

      kernel32.dll.Sleep Hint[0]

      [IMAGE_IMPORT_DESCRIPTOR]
      0x116C8    0x0   OriginalFirstThunk:           0x192FC
      0x116C8    0x0   Characteristics:              0x192FC
      0x116CC     0x4   TimeDateStamp:                  0x0         [Thu Jan  1
00:00:00 1970 UTC]
      0x116D0    0x8   ForwarderChain:               0x0
      0x116D4    0xC   Name:                         0x19DDE
      0x116D8    0x10  FirstThunk:                   0x19510

      advapi32.dll.AdjustTokenPrivileges Hint[0]
```

Витяг сліду IFT

```
lstrcmpiA
GotModulHandleA
LoadLibraryA
Get ProcAddress
HeapAlloc
lstrcpynA
GotModuleHandle
LoadLibraryA
Get ProcAddress
HeapAlloc
Inet_addr
gethostbyname
HeapAlloc
socket
recv
HeapAlloc
memcpy
GetTickCount
HeapAlloc
lstrcpynA
CreateFileA
DeleteFileA
```

Аналіз мережного трафіку

```
Network Traffic: ==================
[UDP] svchost.exe:1032 > 239.255.255.250:1900
[UDP] localhost:1243 > svchost.exe:1204
[UDP] services.exe:680 > 206.254.253.254:16471
[UDP] services.exe:680 > 190.254.253.254:16471
[UDP] localhost:1253 > svchost.exe:1032
[UDP] svchost.exe:1032 > localhost:1253
[UDP] services.exe:680 > 182.254.253.254:16471
[UDP] services.exe:680 > 180.254.253.254:16471
[UDP] services.exe:680 > 135.254.253.254:16471
[UDP] services.exe:680 > 134.254.253.254:16471
[UDP] services.exe:680 > 117.254.253.254:16471
[UDP] services.exe:680 > 115.254.253.254:16471
[UDP] services.exe:680 > 92.254.253.254:16471
[UDP] svchost.exe:1032 > localhost:1242
[UDP] localhost:1243 > svchost.exe:1032
[UDP] svchost.exe:1032 > localhost:1243

Unique Hosts:
==================
115.254.253.254
117.254.253.254
134.254.253.254
135.254.253.254
180.254.253.254
182.254.253.254
190.254.253.254
206.254.253.254
239.255.255.250
```