A. It is a Data Structure used by the operational system internally.
B. The IsDebuggerPresent, BeingDebugged, and ProcessHeap fields.
1. The strings show that this program will do something with the cmd.exe, which could possibly be extracting information out of the %SYSTEMROOT%\system32\ directory and sending it to http://www.practicalmalwareanalysis.com.

```
HHtpHHtl
YY^
command.com
COMSPEC
*D@
EEE
 (8PX
700WP
`h````
ppxxxx
(null)
(null)
__GLOBAL_HEAP_SELECTED
__MSVCRT_HEAP_SELECT
runtime error
TLOSS error
SING error
DOMAIN error
R6028
- unable to initialize heap
R6027
- not enough space for lowio initialization
R6026
- not enough space for stdio initialization
R6025
- pure virtual function call
R6024
- not enough space for _onexit/atexit table
R6019
- unable to open console device
R6018
- unexpected heap error
R6017
- unexpected multithread lock error
R6016
- not enough space for thread data
abnormal program termination
R6009
- not enough space for environment
R6008
- not enough space for arguments
```

```
GetLastError
ReadFile
WriteFile
Sleep
CopyFileA
ExpandEnvironmentStringsA
DeleteFileA
KERNEL32.dll
RegQueryValueExA
RegOpenKeyExA
RegSetValueExA
RegCreateKeyExA
RegDeleteValueA
CreateServiceA
CloseServiceHandle
ChangeServiceConfigA
OpenServiceA
OpenSCManagerA
DeleteService
ADVAPI32.dll
ShellExecuteA
SHELL32.dll
WS2_32.dll
ExitProcess
TerminateProcess
GetCurrentProcess
GetTimeZoneInformation
GetSystemTime
GetLocalTime
DuplicateHandle
GetCommandLineA
GetVersion
SetStdHandle
GetFileType
SetHandleCount
GetStdHandle
GetStartupInfoA
CreatePipe
GetExitCodeProcess
WaitForSingleObject
```

```
HeapFree
RtlUnwind
MultiByteToWideChar
GetStringTypeA
GetStringTypeW
SetFilePointer
VirtualAlloc
LCMapStringA
LCMapStringW
GetProcAddress
LoadLibraryA
FlushFileBuffers
GetFileAttributesA
CreateProcessA
CompareStringA
CompareStringW
SetEnvironmentVariableA
,e@
TN@
cmd.exe
 >> NUL
/c del
Configuration
SOFTWARE\Microsoft \XPS
\kernel32.dll
 HTTP/1.0
GET
`````
`````
NOTHING
CMD
DOWNLOAD
UPLOAD
SLEEP
ups
http://www.practicalmalwareanalysis.com
 Manager Service
.exe
%SYSTEMROOT%\system32\
k:%s h:%s p:%s per:%s
```

2. 42 out of 71 different scanning services have flagged this program as malicious, with a lot of them specifying (Trojan.Win32)

| engine (71/71) | score (42/71) | date (dd.mm.yyyy) | age (days) |
|---|---|---|---|
| Bkav | W32.AIDetect.malware2 | 17.11.2022 | 11 |
| Lionic | Trojan.Win32.Generic.4!c | 17.11.2022 | 11 |
| Elastic | malicious (high confidence) | 17.11.2022 | 11 |
| Cynet | Malicious (score: 100) | 17.11.2022 | 11 |
| CMC | clean | 17.11.2022 | 11 |
| CAT-QuickHeal | clean | 17.11.2022 | 11 |
| ALYac | clean | 17.11.2022 | 11 |
| Cylance | Unsafe | 18.11.2022 | 10 |
| Zillya | Trojan.Agent.Win32.781743 | 17.11.2022 | 11 |
| Sangfor | Trojan.Win32.Agent.5BGSI0 | 10.11.2022 | 18 |
| K7AntiVirus | clean | 17.11.2022 | 11 |
| Alibaba | Trojan:Win32/Generic.d849ed30 | 27.05.2019 | 1281 |
| K7GW | clean | 15.11.2022 | 13 |
| Cybereason | malicious.4c91d4 | 30.03.2021 | 608 |
| Baidu | clean | 18.03.2019 | 1351 |
| VirIT | Trojan.Win32.Generic.BWKO | 17.11.2022 | 11 |
| Cyren | W32/Agent.DBF.gen!Eldorado | 17.11.2022 | 11 |
| Symantec | ML.Attribute.HighConfidence | 17.11.2022 | 11 |
| tehtris | clean | 18.11.2022 | 10 |
| ESET-NOD32 | a variant of Win32/Agent.QSX | 17.11.2022 | 11 |
| APEX | Malicious | 16.11.2022 | 12 |
| Paloalto | clean | 18.11.2022 | 10 |
| ClamAV | Win.Dropper.Ulise-9937584-0 | 17.11.2022 | 11 |
| Kaspersky | clean | 17.11.2022 | 11 |
| BitDefender | clean | 17.11.2022 | 11 |
| NANO-Antivirus | Trojan.Win32.Agent.eaypws | 17.11.2022 | 11 |
| ViRobot | clean | 17.11.2022 | 11 |
| MicroWorld-eScan | clean | 17.11.2022 | 11 |
| Avast | Win32:Evo-gen [Trj] | 17.11.2022 | 11 |
| Rising | Trojan.Agent!8.B1E (TFE:5:liyXqtF1pEG) | 17.11.2022 | 11 |
| Ad-Aware | clean | 17.11.2022 | 11 |

3. The "/c del" command tells us that this program wants to delete something (maybe itself). "cmd.exe" is the program opening the command prompt, and "ShellExecuteA" tells us that its going to execute shell commands after opening the command prompt.

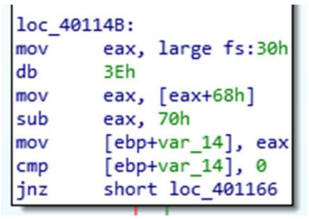
```
push    eax             ; lpParameters
push    offset File     ; "cmd.exe"
push    0               ; lpOperation
push    0               ; hwnd
call    ds:ShellExecuteA
push    0               ; uExitCode
call    sub_403864
```

```
push    edx             ; lpszLongPath
call    ds:GetShortPathNameA
mov     edi, offset aCDel ; "/c del "
lea     edx, [ebp+Parameters]
or      ecx, 0FFFFFFFFh
xor     eax, eax
repne scasb
```

4. The two instructions are an indicator of the ProcessHeap Flag technique. The addresses are 0000000000401130 and 0000000000401136 respectively.

```
loc_401130:
mov     eax, large fs:30h
mov     eax, [eax+18h]
db      3Eh
mov     eax, [eax+10h]
mov     [ebp+var_10], eax
cmp     [ebp+var_10], 0
jz      short loc_40114B
```

5. These three instructions indicate the use of the NTGlobalFlag technique. The addresses are 0000000000040114B, 0000000000401151, 0000000000401155 respectively.




6. The final two instructions indicate the use of the IsDebuggerPresent function. The addresses are 0000000000401117 and 000000000040111D respectively.