**Sample Name – Invoice.xlsx.exe**
**File Type – 32 Bit Executable**

## Static Analysis

**User Interactions:**
Uses HTML coding to display a pop-up to user

*Your computer is in Danger!*
*Windows Security Center has detected spyware/adware infection!*
*It is strongly recommended to use special antispyware tools to prevent data loss.*

**Makes use of following libraries**
KERNEL32.DLL
ADVAPI32.dll
COMCTL32.dll
ole32.dll
SHELL32.dll
USER32.dll
WSOCK32.dll

**Makes use of following functions**
GetModuleFileNameA
GetModuleHandleA
WriteFile
ReadFile
DeleteFileA
CloseHandle
GetFileSize
CreateFileA
CreateThread
CopyFileA
CreateEventA
GetStringTypeA
LoadLibraryA
GetProcAddress
GetOEMCP
GetACP
GetCPInfo
RtlUnwind
GetFileType
ExitProcess
SetHandleCount
GetEnvironmentStringsW
GetEnvironmentStrings
FreeEnvironmentStringsW

FreeEnvironmentStringsA
UnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
CreateDirectoryA
GetWindowsDirectoryA
GetSystemTimeAsFileTime
FileTimeToLocalFileTime
Sleep
GetLastError
WinExec
LCMapStringW
GetStringTypeW
LCMapStringA
MultiByteToWideChar
WideCharToMultiByte
VirtualAlloc
HeapFree
VirtualFree
HeapCreate
HeapDestroy
GetVersion
GetCommandLineA
GetStdHandle
lstrcpynA
HeapReAlloc
HeapAlloc
GetStartupInfoA
RegDeleteKeyA
RegSetValueExA
RegDeleteValueA
RegCreateKeyExA
RegQueryValueExA
RegCloseKey
InitCommonControlsEx
CoInitialize
CoCreateInstance
Shell_NotifyIconA
wsprintfA
ShowWindow
IsWindowVisible
UpdateWindow
GetDesktopWindow
IsChild
IsZoomed
SendMessageA
FindWindowExA
FindWindowA
CreateDialogParamA

LoadIconA
GetMessageA
TranslateMessage
DispatchMessageA
GetFocus

**Network Activity**

Host: download.bravesentry.com
69.50.175.181
GET
http://download.bravesentry.com/download.php?&advid=00000717&u=%u&p=%u HTTP/1.0

**Registry Values Accessed/Modified/Created/Deleted**

Software\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**Files Accessed/Modified/Created/Deleted**

C:\Program Files\BraveSentry\BraveSentry.lic
C:\Program Files\BraveSentry\BraveSentry.exe
C:\Windows\xpupdate.exe
Install.dat

| property | value | value | value |
|---|---|---|---|
| name | .text | .data | .rsrc |
| md5 | C3397B3376ED7CFB2F564F4... | 1983DEAF66B088C0F94606F... | 25849421526A999F4A4C94A... |
| entropy | 6.388 | 4.308 | 3.437 |
| file-ratio (98.21%) | 40.18 % | 10.71 % | 47.32 % |
| raw-address | 0x00000400 | 0x00005E00 | 0x00007600 |
| raw-size (56320 bytes) | 0x00005A00 (23040 bytes) | 0x00001800 (6144 bytes) | 0x00006A00 (27136 bytes) |
| virtual-address | 0x00401000 | 0x00407000 | 0x0040A000 |
| virtual-size (57886 bytes) | 0x00005836 (22582 bytes) | 0x00002078 (8312 bytes) | 0x00006970 (26992 bytes) |
| entry-point | 0x00003510 | - | - |
| characteristics | 0xE0040020 | 0xC0000040 | 0x40000040 |
| writable | x | x | - |
| executable | x | - | - |
| shareable | - | - | - |
| discardable | - | - | - |
| initialized-data | - | x | x |
| uninitialized-data | - | - | - |
| unreadable | - | - | - |
| self-modifying | x | - | - |
| virtualized | - | - | - |
| file | n/a | n/a | n/a |

| type (3) | name | file-offset (3) | signature (3) | no... | size (26758 bytes) | file-ratio (46.66%) | md5 | entropy | language (2) | first |
|---|---|---|---|---|---|---|---|---|---|---|
| icon-group | 1 | 0x0000DF5C | icon-group | - | 20 | 0.03 % | EEEA78B1CDAFB203817AB9C01E3CD177 | 1.919 | neutral | 00 0 |
| icon | 1 | 0x000076E8 | icon | - | 26600 | 46.39 % | 9E6B4AB49CD90F337114500CC3E270B5 | 3.424 | neutral | 28 0 |
| dialog | 101 | 0x0000DED0 | dialog | - | 138 | 0.24 % | 9D727F7304850529749156FCF79A4A95 | 2.910 | Russian | C0 0 |