A.R.F v2.0 – 28d.10m.2012

Documentation updates:

i) Minor updates to the Methods documentation part.

ii) Added code example for SpyLDRGenericDetect method.

A.R.F v2.0 – 26d.10m.2012

New Classes were added:

i) VirtualMachineDetection

ii) SandBoxDetection

iii) SpyProcessToolDetection

iv) CheckSumCalculator

Methods added to existing Classes:

i) OutputDebugStringExcepDetection() in SehDbgDetection Class

ii) HWdBreakPointSeh() in HardwareBreakPointDetection class

Modifications made in existing Methods:

i) Added to the SetProcessList:

processlist[31] = "SbieCtrl.exe";

processlist[32] = "SpyStudio.exe";

processlist[33] = "SbieSvc.exe";

processlist[34] = "apimonitor-x86.exe";

ii) Added to the SetModulesList:

moduleslist[14] = "DeviareCOM.dll";

moduleslist[15] = "Nektra.Deviare2.dll";

moduleslist[16] = "SbieDll.dll";

moduleslist[17] = "apimonitor-drv-x86.sys";

A.R.F v1.1 – 17d.01m.2011

Minor modifications to the following functions:

i) bool ListWindowClassDetection(string * arraymemlocation , int listsize);

ii) int ProcessDetection(string * arraymemlocation , int listsize);

iii) int ModuleDetection(string * arraymemlocation, int listsize);

Now the memory occupied by the corresponding dynamic arrays becomes again free for use and the pointers get reset to NULL before exiting these functions.

This update solves an increasing memory usage impact which would occur in case you would like to use these functions several times in your code.

A.R.F v1.0 – 28d/12m/2010

i) An **unused variable warning issue** during compiling in **ApiBreakPoint method** has now been fixed. The variable was the **const BYTE bp**. Now it has been correctly assigned and the **0xCC has been removed from the if statement**.
This issue had no impact at all, but of course it had to be fixed.

ii) A **minor modification** in the **ListWindowClassDetection method** in order to avoid increasing the **string * list pointer** during the last interation of the loop since it was not needed.
This issue had no impact at all, but of course it had to be fixed.

Cheers,

Kyriakos Economou