PDM2 test results

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | End verdict | Processing sequence  (ini-file) | PDM2 Result  (emulator) | | Reason | PDM2 Result  (real) | Reason |
| 1 | REPORT\_EVENT\_P2P\_SC\_RDL  L"Worm.P2P.generic";  // SC+RDL+ | Register self path in P2PKey  (P2P\_SC\_RDL\_1.txt) | -----  100 SelfCopyToPeerToPeerFolder | | Missing functionality of working with:   * AddPeer2PeerPath, * IsPeer2PeerPath * SearchPeer2PeerPaths   In:   * OnRegValueSetStrPre | NO | Missing functionality of working with:   * AddPeer2PeerPath, * IsPeer2PeerPath * SearchPeer2PeerPaths   In:  OnRegValueSetStrPre  OnRegValueSetPost – absent - willbe |
| Self copy to DestFolder,  Register DestFolder in P2PKey  (P2P\_SC\_RDL\_2\_1.txt) | 80 OnSelfCopyNot2Temp  50 SelfCopy  100 SelfCopyToPeerToPeerFolder | | NO |
| Register DestFolder in P2PKey,  Self copy to DestFolder  (P2P\_SC\_RDL\_2\_2.txt) | 80 OnSelfCopyNot2Temp  50 SelfCopy  100 SelfCopyToPeerToPeerFolder | | NO |
| Parent … |  | |  |  |  |
| 2 | REPORT\_EVENT\_SC\_AR  "Trojan.generic"; //SC+AR+ | Write DestFolder to ARKey,  Launch Dest Process  (SC\_AR\_1.txt) | ? | | Can`t reproduce |  |  |
| Write DestFolder to ARKey,  Self copy to DestFolder  (SC\_AR\_2\_1.txt) | 100 SelfCopyAutoRun  80 OnSelfCopyNot2Temp  50 Installer  50 OnInstallNotSelf  50 SelfCopy | |  | OK |  |
| Self copy to DestFolder,  Write DestFolder to ARKey  (SC\_AR\_2\_2.txt) | 100 SelfCopyAutoRun  80 OnSelfCopyNot2Temp  50 Installer  50 OnInstallNotSelf  50 SelfCopy | |  | OK |  |
| SelfCopy to DestFolder,  Write DestFolder to win.ini  (SC\_AR\_3.txt) | 80 OnSelfCopyNot2Temp  50 SelfCopy | | PrivateProfileString (run) enterpreted like c:\win.ini | OK | PrivateProfileString (run) enterpreted like registry operations |
| Rename File To Startup Folder  (SC\_AR\_4.txt) | 100 SelfCopyToStartup  80 OnSelfCopyNot2Temp  50 Installer  50 OnInstallNotSelf  50 SelfCopy | |  | NO  Will be fixed | OnFileRenamePost absent |
| Write DestFolder to ARKey,  Rename file to DestFolder  (SC\_AR\_5.txt) | 100 SelfCopyAutoRun  80 OnSelfCopyNot2Temp  50 Installer  50 OnInstallNotSelf  50 SelfCopy | |  | NO  Will be fixed |
| 3 | REPORT\_EVENT\_SC\_ARsrc | Not used | | | |  |  |
| 4 | REPORT\_EVENT\_SCN  "Worm.generic"; // SCN+; | Launch process from network  (SCN\_1.txt) | ------ | | There is no checking of network path in CreateProcessPre | NO  Wait from Microsoft | There is no checking of network path in CreateProcessPre |
| Self Copy to Network path  (SCN\_2.txt) | 100 SelfCopyToNetwork  80 OnSelfCopyNot2Temp  50 SelfCopy | |  | NO ??? | isExecutable() return false |
| ? |  | |  |  |  |
| 5 | REPORT\_EVENT\_P2P\_SCN  "Worm.P2P.generic";  // SCN+(P2P); | Launch process from P2P folder  (P2P\_SCN\_1.txt) | ? | | Can`t reproduce |  |  |
| Self Copy to P2P folder  (P2P\_SCN\_2.txt) | 100 SelfCopyToPeerToPeerFolder  80 OnSelfCopyNot2Temp  50 SelfCopy | |  | OK  ??? | m\_pEnvironmentHelper-> FileSizeByName() always terurn 0 becouse in OnCopyFilePre |
| 6 | REPORT\_EVENT\_SC2STARTUP  "Trojan.generic";  // SC2STARTUP+; | Launch process from Startup folder  (SC2STARTUP\_1.txt) | ? | | Can`t reproduce |  |  |
| Self Copy to Startup folder  (SC2STARTUP\_2.txt) | 100 SelfCopyToStartup  80 OnSelfCopyNot2Temp  50 Installer  50 OnInstallNotSelf  50 SelfCopy | |  | OK |  |
| 7 | REPORT\_EVENT\_SC\_MULTIPLE  "Worm.P2P.generic";  // SC+(MULTIPLE); | Self Copy to misc dest folder more then 2 times,  Launch process from dest folder  (SC\_MULTIPLE\_1.txt) |  | | Can`t reproduce |  |  |
| Self Copy to misc DestFolder more then 2 times  (SC\_MULTIPLE\_2.txt) | 100 SelfCopyMultiple  80 OnSelfCopyNot2Temp  50 SelfCopy | |  | OK |  |
| 8 | REPORT\_EVENT\_RDR  "RootShell";  // RDR+; | Create CMD.EXE process with redirected handles to socket  (RDR\_1.txt) | ----- | | Missed appropriate event and heuristic | NO  Will not be | Missed appropriate event and heuristic |
| 9 | REPORT\_EVENT\_REGMODIFY  "Registry access" | Reg Guard | | | |  |  |
| 10 | REPORT\_EVENT\_HIDDEN\_OBJ  "Hidden object" | ? |  | |  |  |  |
| 11 | REPORT\_EVENT\_INVADER  "Invader" | CreateRemoteThread with LoadLibrary Func addr, and DllNameParam  (INVADER\_1.txt) | 100 ProcessInvader | |  | NO  Wait from Microsoft | OnThreadCreatePre absent |
| Call CreateRemoteThread with code injection  (INVADER\_2.txt) | 100 ProcessInvader | |  | NO  Wait from Microsoft  Will not actual | absent  OnThreadCreatePre  OnWriteProcessMemoryPre |
| Call SetThreadContext with modified EIP to LoadLibraryA  (INVADER\_3.txt) | 100 ProcessInvader | |  | NO  Wait from Microsoft  Will be fixed | absent  OnThreadCreatePre  OnThreadSetContextPre |
| Write to another process memory  (INVADER\_4.txt) | 100 ProcessInvader | |  | NO  Will not actual | absent  OnWriteProcessMemoryPre |
| ? |  | |  |  |  |
| ? |  | |  |  |  |
| 12 | REPORT\_EVENT\_APPG  "Critical application" | App Guard | | | |  |  |
| 13 | REPORT\_EVENT\_APPG\_CHANGED  "Application changed" |  |  |
| 14 | REPORT\_EVENT\_IMG\_CHANGED  "Integrity violation" |  |  |
| 15 | REPORT\_EVENT\_APPG\_ASCHILD  "Running as child" |  |  |
| 16 | REPORT\_EVENT\_APPG\_BROWSER  "Starting Internet Browser" |  |  |
| 17 | REPORT\_EVENT\_INVADER\_LOADER  "Invader (loader)" | SetWindowsHookEx to all process  (INVADER\_LOADER\_1.txt) | 80 DllInvader | | SetWindowsHookExW absent  SetWindowsHookExA only  Work only if dll in m\_CreatedImagesList | NO  Will not be | absent  OnSetWindowsHook |
| SetWindowsHookEx to specified thread  (INVADER\_LOADER\_2.txt) | ----- | | OnSetWindowsHook()  if (dwThreadId != 0)  return vtVerdict\_Default; | NO  Will not be | absent  OnSetWindowsHook |
| ? |  | |  |  |  |
| 18 | REPORT\_EVENT\_STRANGEKEY  "Suspicious registry value" | NtCreateKey with not correct key  (STRANGEKEY\_1.txt) | ----- | | * NtCreateKey function emulation absent * Appropriate Heuristic absent | NO  Will be fixed | OnRegValueSetStrPre no come |
| 19 | REPORT\_EVENT\_SYSCHANGE  "Strange behaviour" | R0 |  | |  |  |  |
| NtOpenSection with SECTION\_MAP\_WRITE  (SYSCHANGE\_1.txt) | -----  100 OnPhysicalMemoryAccess(Write) | | * NtOpenSection function emulation absent * Appropriate Heuristic absent | NO | Missed appropriate event and heuristic |
| 20 | REPORT\_EVENT\_HIDDEN\_INSTALL  "Hidden install" | Copy exe-file to DestFolder and register it in simple AR key  (HIDDEN\_INSTALL\_1\_1.txt) | 50 Installer  50 OnInstallNotSelf | | There are no heuristic rules to connect this events | NO  OnInstallNotSelf | There are no heuristic rules to connect this events |
| Register Exe from DestFolder in simple AR key,  Copy exe-file to DestFolder  (HIDDEN\_INSTALL\_1\_2.txt) | 50 Installer  50 OnInstallNotSelf | | NO |
| Copy exe-file to DestFolder and Write DestFolder to win.ini  (HIDDEN\_INSTALL\_2\_1.txt) | ----- | | Missing functionality of working with:   * Win.ini; * PrivateProfileString(run) | NO | There are no heuristic rules to connect this events |
| Write DestFolder to win.ini,  Copy exe-file to DestFolder (HIDDEN\_INSTALL\_2\_2.txt) | ----- | | NO |
| Copy exe-file to DestFolder  and launch it  (HIDDEN\_INSTALL\_3.txt) | ----- | | There are no appropriate heuristic rules | NO | There are no heuristic rules to connect this events |
| 21 | REPORT\_EVENT\_BUFFEROVERRUN  "Buffer overrun" | R0 |  | |  |  |  |
| 22 | REPORT\_EVENT\_DEP  "Data Execution" | R0 |  | |  |  |  |
| 23 | REPORT\_EVENT\_HOSTS  "Hosts file modification" | Add new record to host-file  (HOSTS\_1.txt) | 70 AntiAV  30 HostsAdded | | * OnHostsAdded() call only for adding avhosts * Infinite loop of exceptions (fopen, fwrite, fclose) | NO  OnAntiAV  (no alert) |  |
| Rename modified host-file to original host-file  (HOSTS\_2.txt) | 70 AntiAV  30 HostsAdded | | NO  Will be fixed | OnFileRenamePost absent |
| 24 | REPORT\_EVENT\_KEYLOGGER  "Keylogger" | R0 |  | |  |  |  |
|  | |  |  |  |
| 25 | REPORT\_EVENT\_DOWNLOADER  "Trojan Downloader" |  |  | |  |  |  |
| 26 | REPORT\_EVENT\_TROJAN\_GEN  "Trojan.generic"  ("Trojan.cryptor") | Modify 3 OLE files (OLE sign must be changed)  (TROJAN\_GEN\_1.txt) | ----- | | * heuristic rule absent * Infinite loop of exceptions (fopen, fwrite, fclose) | NO | heuristic rule absent |
| Add new 3 or more record to host-file with AV-Hosts  (TROJAN\_GEN\_2.txt) | 100 AntiAVMultiple  70 AntiAV  30 HostsAdded | | * OnHostsAdded() call only for adding avhosts * Infinite loop of exceptions (fopen, fwrite, fclose) | NO  OnAntiAV  (no alert) |  |
| Rename multiple-modified host-file to original host-file  (TROJAN\_GEN\_3.txt) | 100 AntiAVMultiple  70 AntiAV  30 HostsAdded | | NO  Will be fixed | OnFileRenamePost absent |
| Add value in regkey “image file execution options\\avp.exe”  (TROJAN\_GEN\_4.txt) | 100 RegAvpImageFileExecOptions | |  | NO | no verdict flag modification |
| Modify 5 PE-files in ProgramFiles folder    (TROJAN\_GEN\_5.txt)  Worm.P2P.generic | 100 Infector  100 SelfCopyMultiple  80 OnSelfCopyNot2Temp  50 SelfCopy | | * SHGetFolderPath absent (CSIDL\_PROGRAM\_FILES) * Infinite loop of exceptions (fopen, fwrite, fclose) | OK |  |
| 27 | REPORT\_EVENT\_TASKMGR\_PROT  "TaskManager protection" | R0 |  | |  |  |  |
| 28 | REPORT\_EVENT\_DRIVER\_INS  "Suspicious driver installation" | Copy drv to %System%\drivers and Registry drv name in  REGISTRY\SYSTEM\ CurrentControlSet\Services  (DRIVER\_INS\_1\_1.txt) | 80 InstallDriver | | OnRegKeyCreatePost() empty (rem`d) | NO | OnRegKeyCreatePost() empty (rem`d) |
| Registry drv name in  REGISTRY\SYSTEM\ CurrentControlSet\Services and Copy drv in %System%\drivers  (DRIVER\_INS\_1\_2.txt) | 80 InstallDriver | | NO |
| Register drv name,  Register drv ImagePath  Copy drv to %System%\drivers,  Register drv Type  (DRIVER\_INS\_2.txt) | 80 InstallDriver  50 Installer  50 OnInstallNotSelf | | ? | NO ???  (Reg\_QueryValueEx not implemented) | Reg\_QueryValueEx ("ImagePath") return false |
| Register drv name,  Copy drv to %System%\drivers,  Register drv Type  Register drv ImagePath  (DRIVER\_INS\_3.txt) | 80 InstallDriver  50 Installer  50 OnInstallNotSelf | | ? | NO ???  (Reg\_QueryValueEx not implemented) | Reg\_QueryValueEx("type") return false |
| Copy drv to %System%\drivers,  Restore drv TypeImage by RegRestoreKey  (DRIVER\_INS\_4.txt) | 80 InstallDriver | | ? | NO  Wait from Microsoft | RegRestoreKey control absent |
| 29 | REPORT\_EVENT\_HIDDEN\_SEND  "Hidden data sending" | SetWindowText to browser window (IE)  (HIDDEN\_SEND\_1.txt) | ----- | | Missed appropriate event and heuristic | NO  Will not be | Missed appropriate event and heuristic |
| IBackgroundCopyJob::Resume()  (HIDDEN\_SEND\_2.txt) | ----- | | Missed appropriate event and heuristic | NO | Missed appropriate event and heuristic |
| 31 | REPORT\_EVENT\_MASS\_MAILER  "Mass-mailer software" | ? |  | |  |  |  |
| 32 | REPORT\_EVENT\_BROWSERCONTROL  "Internet Browser Control" | Open url throw DDE-functions (IExplore, WWW\_OpenURL)  (BROWSERCONTROL\_1.txt) | ----- | | Missed appropriate event and heuristic | NO  Will not be | Missed appropriate event and heuristic |
| 33 | REPORT\_EVENT\_MAX |  |  | |  |  |  |
| Only in PDM2 | | | | | |  |  |
| 34 | “AntiAV” | Try to kill process of 1 antivirus trend  (KILL\_AV\_1.txt) | 70 AntiAV | ? | | NO  Wait from Microsoft | OnProcessTerminatePre absent |
| Start 1 AV process with STOP %SERVICE% param  (KILL\_AV\_3.txt) | 70 AntiAV  30 KillService | NO  OnAntiAV  (no alert) |  |
| 35 | “AntiAVMultiple” | Try to kill process of >2 antivirus trends  (KILL\_AV\_2.txt) | 100 AntiAVMultiple  70 AntiAV |  | | NO  Wait from Microsoft | OnProcessTerminatePre absent |
| Start >2 AV process with STOP %SERVICE% param  (KILL\_AV\_4.txt) | 100 AntiAVMultiple  70 AntiAV  30 KillService | NO  OnAntiAV  (no alert) |  |
| 36 | “IEStartPage” | Change StartPage of IE in registry  (START\_PAGE\_1.txt) | 100 IEStartPage |  | | NO  IEStartPage  (no alert) |  |
| 37 | "SecurityViolation" | Add self path to FiteWall trusted application list  (SEC\_VIOLATION\_1.txt) | 100 SecurityViolation |  | | (no alert) |  |
| Set Microsoft FireWall state setting in registry to 0  (SEC\_VIOLATION\_2.txt) | 100 SecurityViolation |  | | (no alert) |  |
| Temporally disable WFP on calc.exe (by undocument use of sfc\_os.dll)  (SEC\_VIOLATION\_3.txt) | 100 SecurityViolation |  | | ???  (no alert) | Missed appropriate event and heuristic |
| IWebBrowser2\_\_put\_Visible | ??? |  | |  |  |
| 38 | “KillSystemFiles” | Kill >4 sys files  (KILL\_SYS\_FILES\_1.txt) | 100 KillSystemFiles |  | |  |  |
| 39 | “PswAccess” | Try to access to psw files  (ACCESS\_PSW\_FILES\_1.txt) | 50 PswAccess | Only if CreateFile fail | | ???  (no alert) |  |
| 40 | “PswAccessMultiple” | Try to multiple access to psw files  (ACCESS\_PSW\_FILES\_2.txt) | 100 PswAccessMultiple  50 PswAccess | ???  (no alert) |  |
| 41 | “StartSystemFileSuspended” | Create system process with CREATE\_SUSPENDED flag  (START\_SUSP\_SYS\_1.txt) | 100 StartSystemFileSuspended |  | | NO  Wait from Microsoft | OnProcessCreatePre absent |
| 42 | “StartWithSystemName” | Copy exe-file to folder with system name and start it  (START\_WITH\_SYS\_NAME\_1.txt) | 100 StartWithSystemName |  | | NO  Wait from Microsoft | OnProcessCreatePre absent |
| 43 | “OnChangeSystemRegistry” | ??? |  |  | |  |  |
| 44 | “OnInstallInNTFSStream” |  |  | Streams not supported by emulator | |  |  |
| 45 | “OnDeleteSelf” | Delete self by (CMD.EXE / c del %SelfPath%)  (DELETE\_SELF\_1.txt) | 80 OnDeleteSelf |  | |  |  |