**Comparison of PDM and PDM2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | PDM  (m\_pPDM-> m\_pReportEvent-> OnEvent) | PDM  Condition | PDM2 | AskProps.m\_EventTypeMisc description |
| CActivityCheck | | | | |
| 1 | CheckSelfCopy | m\_RegHistory.Contain() |  | REPORT\_EVENT\_SC\_AR |
| m\_StartupPaths.ContainSubstrForPath() | ***OnSelfCopyToStartup()*** | REPORT\_EVENT\_ SC2STARTUP |
| IsNetworkPath() | ***OnSelfCopyToNetwork()*** | REPORT\_EVENT\_SCN |
| m\_NetPaths.ContainSubstrForPath() | ***OnSelfCopyToPeerToPeerFolder*** | REPORT\_EVENT\_P2P\_SCN |
| pProcess->m\_SelfCopyList.Count() > 2 | ***OnSelfCopyMultiple()*** | REPORT\_EVENT\_ SC\_MULTIPLE |
| 2 | CheckAutorunKey | m\_SelfCopyHistory.IsCopy2Path() | ***OnSelfCopyAutoRun()*** | REPORT\_EVENT\_SC\_AR |
| pProcess-> m\_ModifiedImagesList.ContainPath() |  | REPORT\_EVENT\_ HIDDEN\_INSTALL |
| 3 | CheckRename | m\_StartupPaths.ContainSubstrForPath() || m\_RegHistory.Contain() | cEventHandlerHeuristic:: OnFileRenamePost() call OnSelfCopy() | REPORT\_EVENT\_SC\_AR |
| 4 | CheckConfigFiles | ComparePath("%windir%\\system32\\drivers\\etc\\hosts") | cEventHandlerHeurHosts:: OnFileCloseModifiedPost  if in arrAntiVirusDomains call OnHostsAdded() which call OnAntiAV() | REPORT\_EVENT\_HOSTS |
| 5 | CheckCryptor | pProcess->m\_pHistory  (etModifyFile || etDeleteFile) &&  nCryptCount == 3 |  | REPORT\_EVENT\_ TROJAN\_GEN,  REPORT\_SUBEVENT\_ CRYPTOR |
| 6 | CheckP2PKey | IsP2PKey() | cEventHandlerHeuristic:: m\_Peer2PeerPaths used in cEventHandlerHeuristic:: OnSelfCopy() | REPORT\_EVENT\_ P2P\_SC\_RDL  pwcsP2PRegKeys[] =  "\\KAZAA\\",  "\\IMESH\\CLIENT\\",  "\\GROKSTER\\" … |
| 7 | RedirectedInOut | No condition |  | REPORT\_EVENT\_RDR |
| 8 | CheckDrvReg | \\SystemRoot\\ | cEventHandlerHeurInstall:: OnFileCloseModifiedPost()  Call OnInstallDriver() | REPORT\_EVENT\_ DRIVER\_INS |
| 9 | Reg\_Request | Direct call of m\_pReportEvent->OnEvent |  |  |
| 10 | Appg\_Request | Direct call of m\_pReportEvent->OnEvent |  |  |
| 11 | Generic\_Request | Direct call of m\_pReportEvent->OnEvent |  |  |
| cHostsFileObj | | | | |
| 12 | CheckHostRegistration | m\_HostsCount > 3 |  | REPORT\_EVENT\_ TROJAN\_GEN  pchHostsCheck[] = {  ".avp.",  ".kaspersky.",  ".kaspersky-labs.",  ".mcafee."… |
| CJob | | | | |
| 13 | MakeInvaderAlert | Almost direct call of  m\_pReportEvent->OnEvent |  | REPORT\_EVENT\_INVADER |
| 14 | CheckInvaderAlert | Call MakeInvaderAlert() |  |  |
| 15 | CheckCommand | …  Call m\_pActivityCheck->Generic\_Request |  | REPORT\_EVENT\_ APPG\_BROWSER |
| CJob::RegistryEvent | | | | |
| 16 | Interceptor\_ RestoreKey | MatchWithPattern( \\registry\\machine\\system\\controlset???\\services\\\*) | cEventHandlerHeurInstall:: OnRegKeyCreatePost(), OnRegValueSetStrPre() , OnRegValueSetPre()  Call OnInstallDriver()  cEventHandlerHeurInstall:: OnRegAutoRunRegisterResolved()  call OnInstall()  OnInstallDriver(),OnInstall()  call OnInstallInNTFSStream() | REPORT\_EVENT\_ DRIVER\_INS |
| m\_pActivityCheck->NeedRegistryRequest()  call m\_pActivityCheck->Reg\_Request |  | REPORT\_EVENT\_ REGMODIFY |
| 17 | Interceptor\_ CreateKey | MatchWithPattern( \\REGISTRY\\MACHINE\\SECURITY) |  | REPORT\_EVENT\_ STRANGEKEY |
| 18 | Interceptor\_ DeleteKey | m\_pActivityCheck->NeedRegistryRequest()  call m\_pActivityCheck->Reg\_Request() |  | REPORT\_EVENT\_ REGMODIFY |
| 19 | Interceptor\_ SetValueKey | MatchWithPattern( [\\registry\\machine\\system\\controlset???\\services\\\*](file:///\\registry\\machine\\system\\controlset%3f%3f%3f\\services\\*) &&  MatchWithPattern(pwchValueName, L"type", false);  call m\_pActivityCheck->CheckDrvReg() | SingleEvent\_RegistryPre  Call m\_event\_mgr. OnRegValueSetPre()  call m\_event\_mgr. OnRegValueSetStrPre()  cEventHandlerHeurKillAV:: OnRegValueSetStrPre call m\_pEventMgr-> OnRegAvpImageFileExecOptions  cEventHandlerHeuristic:: OnRegValueSetStrPre  (".COM",".EXE", …) ||  m\_RegAutoRuns.IsAutoRun() call m\_pEventMgr-> OnChangeSystemRegistry() |  |
| MatchWithPattern( [\\registry\\machine\\system\\controlset???\\services\\\*](file:///\\registry\\machine\\system\\controlset%3f%3f%3f\\services\\*) &&  !MatchWithPattern(pwchValueName, L"type", false);  call m\_pActivityCheck->CheckDrvReg() |  |
| m\_pActivityCheck->IsP2PKey()  call m\_pActivityCheck->CheckP2PKey() |  |
| m\_pActivityCheck->IsAVPExecute() | REPORT\_EVENT\_ TROJAN\_GEN |
| m\_RegCheck.IsAutoRunsKey()  call m\_pActivityCheck->CheckAutorunKey() |  |
| m\_pActivityCheck->NeedRegistryRequest()  call m\_pActivityCheck->Reg\_Request() | REPORT\_EVENT\_ REGMODIFY |
| 20 | Interceptor\_ DeleteValueKey, QueryValueKey | m\_pActivityCheck->NeedRegistryRequest()  call m\_pActivityCheck->Reg\_Request() |  | REPORT\_EVENT\_ REGMODIFY |
| CJob::ProcessEvent | | | | |
| 21 | MJ\_SYSTEM\_ CREATE\_PROCESS | !pProcessParent->m\_bInstaller &&  pProcessParent->m\_ModifiedImagesList. ContainPath(pParamImagePath->ParamValue) && … | RegisterProcess call m\_event\_mgr.  OnProcessCreatePost()  SingleEvent\_System:: MJ\_EXIT\_PROCESS call m\_event\_mgr. OnProcessExitPost()  cEventHandlerHeuristic:: OnProcessCreatePre() call  OnStartSystemFileSuspended, OnStartWithSystemName()  cEventHandlerHeurKillAV:: OnProcessCreatePost() call m\_pEventMgr->OnKillService()  cEventHandlerHeurKillAV:: OnProcessTerminatePre() call m\_pEventMgr->OnAntiAV()  OnAntiAV() call OnAntiAVMultiple() | REPORT\_EVENT\_ HIDDEN\_INSTALL |
| m\_pActivityCheck-> NeedStartProcessRequest()  call m\_pActivityCheck->Appg\_Request() | REPORT\_EVENT\_APPG,  REPORT\_EVENT\_  APPG\_CHANGED,  REPORT\_EVENT\_ APPG\_ASCHILD |
| pEvt->m\_EventFlags & \_EVENT\_FLAG\_POSTPROCESSING  call m\_pActivityCheck->CheckSelfCopy() |  |
| 22 | MJ\_CREATE\_ PROCESS\_NOTIFY\_EXTEND | (ConFlag & …\_FLAG\_STDIN\_REMOTE) &&  (ConFlag & …\_FLAG\_STDOUT\_REMOTE)  Call m\_pActivityCheck->RedirectedInOut() |  |  |
| 23 | MJ\_SYSTEM\_ WRITE\_PROCESS\_MEMORY | !(pEvt->m\_EventFlags & \_EVENT\_FLAG\_POSTPROCESSING) &&  (Offset!=0x10000 && Offset!=0x20000 && Offset!=0x30000 &&  m\_pPDM->m\_TaskManagerProt.m\_bEnabled && pProcessDst->IsType(\_SPRC\_FLAG\_TASKMGR)) | cEventHandlerHeurInvader:: OnWriteProcessMemoryPre() call m\_pEventMgr-> OnProcessInvader() | AUTO DENY |
| !(pEvt->m\_EventFlags & \_EVENT\_FLAG\_POSTPROCESSING) &&  m\_Invader.m\_bEnabled &&  m\_pProcessList->IsEqualProcessNames()  call MakeInvaderAlert() |  |  |
| (0x20000 == Offset) &&  !pProcessDst->m\_CheckCommandCompleted  Call CheckCommand() |  |  |
| 24 | MJ\_SYSTEM\_ CREATE\_REMOTE\_THREAD | Call CheckInvaderAlert() | SingleEvent\_System:: MJ\_SYSTEM\_CREATE\_THREAD call m\_event\_mgr. OnThreadCreatePost()  SingleEvent\_System:: MJ\_SYSTEM\_ TERMINATE\_THREAD\_NOTIFY call m\_event\_mgr. OnThreadTerminatePost()  cEventHandlerHeurInvader:: OnThreadCreatePre() call m\_pEventMgr-> OnProcessInvader() |  |
| 25 | MJ\_SYSTEM\_ CREATE\_SECTION | (access & SECTION\_MAP\_EXECUTE) &&  m\_pActivityCheck->NeedLoadImageRequest()  call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ IMG\_CHANGED |
| (access & SECTION\_MAP\_EXECUTE) &&  (pProcess->IsType(\_SPRC\_FLAG\_TASKMGR))… |  | REPORT\_EVENT\_ TASKMGR\_PROT |
| 26 | MJ\_SYSTEM\_ SET\_THREAD\_CONTEXT | DestProcId != WorkingProcId  Call CheckInvaderAlert() | cEventHandlerHeurInvader:: OnThreadSetContextPre() call m\_pEventMgr-> OnProcessInvader() |  |
| 27 | MJ\_SYSTEM\_USER\_ SET\_WINDOWS\_HOOK\_EX | m\_ModifiedImagesList.ContainPath()  Call MakeInvaderAlert() | cEventHandlerHeurInvader:: OnSetWindowsHook() call m\_pEventMgr->OnDllInvader() |  |
| Not sys dll`s &&  Not \_SPRC\_FLAG\_USER\_TRUST | REPORT\_EVENT\_ INVADER\_LOADER |
| 28 | MJ\_SYSTEM\_ USER\_POST\_MESSAGE::  WM\_DDE\_EXECUTE | bInetUrl &&  pProcessDst->IsType(\_SPRC\_FLAG\_INETBORWSER)  Call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ APPG\_BROWSER |
| 29 | MJ\_SYSTEM\_ USER\_POST\_MESSAGE::  WM\_DDE\_INITIATE | bBrowserTarget && “iexplore”  call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ BROWSERCONTROL |
| 30 | MJ\_SYSTEM\_ SYSENTER\_CHANGED | call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ SYSCHANGE |
| 31 | MJ\_SYSTEM\_ ACCESS\_PHYSICAL\_MEM | Call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ SYSCHANGE |
| 32 | MJ\_SYSTEM\_ KEYLOGGER\_DETECTED | Almost  Direct call of m\_pReportEvent->OnEvent |  | REPORT\_EVENT\_ KEYLOGGER |
| 33 | MJ\_SYSTEM\_ INTERPROC\_MESSAGE | (IsType(\_SPRC\_FLAG\_INETBORWSER)) &&  (MsgId == WM\_SETTEXT) |  | REPORT\_EVENT\_ HIDDEN\_SEND |
| 34 | MJ\_SYSTEM\_USER\_ SETWINEVENTHOOK | m\_ModifiedImagesList.ContainPath()  call MakeInvaderAlert() |  |  |
| Remaning conditions… |  | REPORT\_EVENT\_ INVADER\_LOADER |
| CJob::R3Event | | | | |
| 35 | R3\_ACTIVEDESKTOP\_ SETWALLPAPER,  R3\_SHOWHTMLDIALOG | bInetUrl || bHtmlFile  call m\_pActivityCheck->Generic\_Request() |  | REPORT\_EVENT\_ APPG\_BROWSER |
| 36 | R3\_BACKGROUNDCOPY JOB\_RESUME | Almost  Direct call of m\_pReportEvent->OnEvent |  | REPORT\_EVENT\_ HIDDEN\_SEND |
| 37 | R3\_REGISTER INPUTDEVICES | Almost  Direct call of m\_pReportEvent->OnEvent |  | REPORT\_EVENT\_ KEYLOGGER |
| 38 | … | pwchFuncParam && pwchFuncName |  | REPORT\_EVENT\_ BUFFEROVERRUN,  REPORT\_EVENT\_DEP |
| CJob::FileEvent | | | | |
| 39 | IRP\_MJ\_CLEANUP | "WIN.INI" &&  (("windows","run") || ("windows","load"))  Call m\_pActivityCheck->CheckAutorunKey() | cEventHandlerHeuristic:: OnFileCloseModifiedPre/Post call OnRegAutoRunRegisterResolved  which call OnStartWithSystemName(), OnSelfCopyAutoRun()  cEventHandlerHeuristic:: OnFileCloseModifiedPre/Post call  m\_pEventMgr->OnSelfCopy()  cEventHandlerHeuristic:: OnSelfCopy() call OnSelfCopyAutoRun(), OnSelfCopyToStartup(), OnSelfCopyToNetwork(), OnSelfCopyToPeerToPeerFolder OnSelfCopyMultiple() |  |
| !CheckSelfCopy() && !nDestWasExecutable  Call CheckConfigFiles(), CheckCryptor() |  |
| !m\_bInstaller && … &&  (m\_PFModifiedList.Count() == 5) | REPORT\_EVENT\_ TROJAN\_GEN, REPORT\_SUBEVENT\_ INFECTOR |
| 40 | IRP\_MJ\_ SET\_INFORMATION | FileRenameInformation &&  (pEvt->m\_EventFlags & \_EVENT\_FLAG\_POSTPROCESSING)  Call CheckConfigFiles(), CheckRename() | SingleEvent\_File  Call m\_event\_mgr. OnFileCloseModifiedPost() |  |
| FileRenameInformation  Call m\_pActivityCheck->CheckRename() | SingleEvent\_File  Call m\_event\_mgr. OnFileCloseModifiedPre() |  |
|  |  |  | cEventHandlerHeurKillFiles:: OnFileDeletePost()  srvIsWinSystemFile() &&  ( nDeletedSystemFiles > 4)  call OnKillSystemFiles() |  |
|  |  |  | cEventHandlerHeurPsw:: OnFileCreateFail()  if in psw\_folders,  cEventHandlerHeurPsw:: OnProtectedStorageAccessPre  call OnPswAccess(), (>=3) OnPswAccessMultiple() |  |
|  |  |  | cEventHandlerHeurVirus:: OnFileCloseModifiedPre(), OnFileCloseModifiedPost()  call OnInfector() |  |
| OTHER | | | | |
| 41 | PDM::MsgReceive | pm\_IWGEN\_SELF\_MAILER\_DETECTED |  | REPORT\_EVENT\_SCN |
| pm\_IWGEN\_MASS\_MAILER\_DETECTED |  | REPORT\_EVENT\_ MASS\_MAILER |
| pmc\_PDM\_SCHEDULED\_EVENT && pm\_PDM\_SCHEDULED\_SCAN\_FOR\_HIDDEN\_PROCESS  call m\_pProcessList->SearchHidden() |  |  |
| 42 | CProcessList::  SearchHidden() | ??? |  | REPORT\_EVENT\_ HIDDEN\_OBJ |