Verdict generate description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | End verdict | Heuristic  with condition | Primary events  with condition | Processing sequence  (ini-file) |
| 1 | REPORT\_EVENT\_P2P\_SC\_RDL  L"Worm.P2P.generic";  // SC+RDL+ | CheckP2PKey  m\_pActivityCheck-> IsP2PKey()  (SelfCopy) | CJob::RegistryEvent Interceptor\_SetValueKey | Register self path in P2PKey  (P2P\_SC\_RDL\_1.txt) |
| Self copy to DestFolder,  Register DestFolder in P2PKey  (P2P\_SC\_RDL\_2\_1.txt) |
| Register DestFolder in P2PKey,  Self copy to DestFolder  (P2P\_SC\_RDL\_2\_2.txt) |
| Parent … |
| 2 | REPORT\_EVENT\_SC\_AR  "Trojan.generic"; //SC+AR+ | CheckSelfCopy()  m\_RegHistory. Contain()  (Modify Simple AutoRunKeys) | CJob::ProcessEvent MJ\_SYSTEM\_CREATE\_PROCESS  (launch with different name) | Write DestFolder to ARKey,  Launch Dest Process  (SC\_AR\_1.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Write DestFolder to ARKey,  Self copy to DestFolder  (SC\_AR\_2\_1.txt) |
| CheckAutorunKey  m\_SelfCopyHistory. IsCopy2Path() | CJob::RegistryEvent Interceptor\_SetValueKey  (Modify Simple AutoRunKeys) | Self copy to DestFolder,  Write DestFolder to ARKey  (SC\_AR\_2\_2.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (Modify AutoRunKeys in win.ini) | SelfCopy to DestFolder,  Write DestFolder to win.ini  (SC\_AR\_3.txt) |
| CheckRename  (DestFileName  In StartupPaths or in RegHistory) | CJob::FileEvent IRP\_MJ\_SET\_INFORMATION  (FileRenameInformation) | Rename File To Startup Folder  (SC\_AR\_4.txt) |
| Write DestFolder to ARKey,  Rename file to DestFolder  (SC\_AR\_5.txt) |
| 3 | REPORT\_EVENT\_SC\_ARsrc | Not used | | |
| 4 | REPORT\_EVENT\_SCN  "Worm.generic"; // SCN+; | CheckSelfCopy()  (IsNetworkPath) | CJob::ProcessEvent MJ\_SYSTEM\_CREATE\_PROCESS  (launch with different name) | Launch process from network  (SCN\_1.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Self Copy to Network path  (SCN\_2.txt) |
|  | PDM::MsgReceive  pmc\_REMOTE\_GLOBAL && pm\_IWGEN\_SELF\_MAILER\_DETECTED | ? |
| 5 | REPORT\_EVENT\_P2P\_SCN  "Worm.P2P.generic";  // SCN+(P2P); | CheckSelfCopy()  (in NetPaths &&  (SelfCopyList>=2 || FileSize<50\*1024)) | CJob::ProcessEvent MJ\_SYSTEM\_CREATE\_PROCESS  (launch with different name) | Launch process from P2P folder  (P2P\_SCN\_1.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Self Copy to P2P folder  (P2P\_SCN\_2.txt) |
| 6 | REPORT\_EVENT\_SC2STARTUP  "Trojan.generic";  // SC2STARTUP+; | CheckSelfCopy()  (to StartupPaths) | CJob::ProcessEvent MJ\_SYSTEM\_CREATE\_PROCESS  (launch with different name) | Launch process from Startup folder  (SC2STARTUP\_1.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Self Copy to Startup folder  (SC2STARTUP\_2.txt) |
| 7 | REPORT\_EVENT\_SC\_MULTIPLE  "Worm.P2P.generic";  // SC+(MULTIPLE); | CheckSelfCopy()  (SelfCopyList > 2) | CJob::ProcessEvent MJ\_SYSTEM\_CREATE\_PROCESS  (launch with different name) | Self Copy to misc dest folder more then 2 times,  Launch process from dest folder  (SC\_MULTIPLE\_1.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Self Copy to misc DestFolder more then 2 times  (SC\_MULTIPLE\_2.txt) |
| 8 | REPORT\_EVENT\_RDR  "RootShell";  // RDR+; | RedirectedInOut | CJob::ProcessEvent  MJ\_CREATE\_ PROCESS\_NOTIFY\_EXTEND  (FLAG\_STDIN\_REMOTE && FLAG\_STDOUT\_REMOTE) | Create CMD.EXE process with redirected handles to socket  (RDR\_1.txt) |
| 9 | REPORT\_EVENT\_REGMODIFY  "Registry access" | Reg Guard | | |
| 10 | REPORT\_EVENT\_HIDDEN\_OBJ  "Hidden object" | SearchHidden | PDM::MsgReceive  pmc\_PDM\_SCHEDULED\_EVENT && pm\_PDM\_SCHEDULED\_ SCAN\_FOR\_HIDDEN\_PROCESS | ? |
| 11 | REPORT\_EVENT\_INVADER  "Invader" | MakeInvaderAlert  (CheckInvaderAlert (WriteToADDR1 || WriteToADDR2) || LoadLibrary was changed) | CJob::ProcessEvent  MJ\_SYSTEM\_ CREATE\_REMOTE\_THREAD  Call CheckInvaderAlert | CreateRemoteThread with LoadLibrary Func addr, and DllNameParam  (INVADER\_1.txt) |
| Call CreateRemoteThread with code injection  (INVADER\_2.txt) |
| CJob::ProcessEvent  MJ\_SYSTEM\_ SET\_THREAD\_CONTEXT (DestProcId!=WorkingProcId)  Call CheckInvaderAlert | Call SetThreadContext with modified EIP to LoadLibraryA  (INVADER\_3.txt) |
| CJob::ProcessEvent MJ\_SYSTEM\_ WRITE\_PROCESS\_MEMORY | Write to another process memory  (INVADER\_4.txt) |
| CJob::ProcessEvent MJ\_SYSTEM\_ USER\_SET\_WINDOWS\_HOOK\_EX  To ModifiedImagesList | ? |
| CJob::ProcessEvent MJ\_SYSTEM\_ USER\_SETWINEVENTHOOK | ? |
| 12 | REPORT\_EVENT\_APPG  "Critical application" | App Guard | | |
| 13 | REPORT\_EVENT\_APPG\_CHANGED  "Application changed" | App Guard | | |
| 14 | REPORT\_EVENT\_IMG\_CHANGED  "Integrity violation" | App Guard | | |
| 15 | REPORT\_EVENT\_APPG\_ASCHILD  "Running as child" | App Guard | | |
| 16 | REPORT\_EVENT\_APPG\_BROWSER  "Starting Internet Browser" | App Guard | | |
| 17 | REPORT\_EVENT\_INVADER\_LOADER  "Invader (loader)" |  | CJob::ProcessEvent  MJ\_SYSTEM\_ USER\_SET\_WINDOWS\_HOOK\_EX | SetWindowsHookEx to all process  (INVADER\_LOADER\_1.txt) |
| SetWindowsHookEx to specified thread  (INVADER\_LOADER\_2.txt) |
| CJob::ProcessEvent  MJ\_SYSTEM\_ USER\_SETWINEVENTHOOK | ? |
| 18 | REPORT\_EVENT\_STRANGEKEY  "Suspicious registry value" |  | CJob::RegistryEvent Interceptor\_CreateKey  pParamValueName->ParamSize != (lstrlen(pwchValName) + 1 ) \* sizeof(WCHAR) | NtCreateKey with not correct key  (STRANGEKEY\_1.txt) |
| 19 | REPORT\_EVENT\_SYSCHANGE  "Strange behaviour" |  | CJob::ProcessEvent MJ\_SYSTEM\_SYSENTER\_CHANGED | R0 |
| CJob::ProcessEvent MJ\_SYSTEM\_ ACCESS\_PHYSICAL\_MEM | NtOpenSection with SECTION\_MAP\_WRITE  (SYSCHANGE\_1.txt) |
| 20 | REPORT\_EVENT\_HIDDEN\_INSTALL  "Hidden install" | CheckAutorunKey  !pProcess-> m\_bInstaller | CJob::RegistryEvent Interceptor\_SetValueKey  (Modify Simple AutoRunKeys) | Copy exe-file to DestFolder and register it in simple AR key  (HIDDEN\_INSTALL\_1\_1.txt) |
| Register Exe from DestFolder in simple AR key,  Copy exe-file to DestFolder  (HIDDEN\_INSTALL\_1\_2.txt) |
| CJob::FileEvent IRP\_MJ\_CLEANUP  (Modify AutoRunKeys in win.ini) | Copy exe-file to DestFolder and Write DestFolder to win.ini  (HIDDEN\_INSTALL\_2\_1.txt) |
| Write DestFolder to win.ini,  Copy exe-file to DestFolder (HIDDEN\_INSTALL\_2\_2.txt) |
|  | CJob::ProcessEvent  MJ\_SYSTEM\_CREATE\_PROCESS ||  MJ\_SYSTEM\_CREATE\_PROCESS\_EX | Copy exe-file to DestFolder  and launch it  (HIDDEN\_INSTALL\_3.txt) |
| 21 | REPORT\_EVENT\_BUFFEROVERRUN  "Buffer overrun" |  | CJob::R3Event  pwchFuncParam && pwchFuncName | R0 |
| 22 | REPORT\_EVENT\_DEP  "Data Execution" |  | CJob::R3Event  pwchFuncParam && pwchFuncName && CALLFROMDATAINDEX | R0 |
| 23 | REPORT\_EVENT\_HOSTS  "Hosts file modification" | CheckConfigFiles  "%windir%\\system32\\drivers\\etc\\hosts" | CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file)  (!bSelfCopy && !nDestWasExecutable) | Add new record to host-file  (HOSTS\_1.txt) |
| CJob::FileEvent IRP\_MJ\_SET\_INFORMATION  FileRenameInformation | Rename modified host-file to original host-file  (HOSTS\_2.txt) |
| 24 | REPORT\_EVENT\_KEYLOGGER  "Keylogger" |  | CJob::ProcessEvent  MJ\_SYSTEM\_KEYLOGGER\_DETECTED | R0 |
| CJob::R3Event  R3\_REGISTERINPUTDEVICES |
| 25 | REPORT\_EVENT\_DOWNLOADER  "Trojan Downloader" | PDMAskAction\_ HiddenInstall  DownloadInfo.m\_dwDataSize > 0x200 &&  DownloadInfo. m\_pData == m\_RequestProps. m\_ImagePath |  |  |
| 26 | REPORT\_EVENT\_TROJAN\_GEN  "Trojan.generic"  ("Trojan.cryptor") | CheckCryptor  pProcess->  m\_pHistory  (etModifyFile || etDeleteFile) &&  nCryptCount == 3 | CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) (!bSelfCopy && !nDestWasExecutable) | Modify 3 OLE files (OLE sign must be changed)  (TROJAN\_GEN\_1.txt) |
| CheckHost Registration  m\_HostsCount > 3 | CJob::FileEvent IRP\_MJ\_CLEANUP  (close dest file) | Add new 3 or more record to host-file with AV-Hosts  (TROJAN\_GEN\_2.txt) |
| CJob::FileEvent IRP\_MJ\_SET\_INFORMATION  FileRenameInformation | Rename multiple-modified host-file to original host-file  (TROJAN\_GEN\_3.txt) |
|  | CJob::RegistryEvent Interceptor\_SetValueKey  IsAVPExecute | Add value in regkey “image file execution options\\avp.exe”  (TROJAN\_GEN\_4.txt) |
|  | CJob::FileEvent IRP\_MJ\_CLEANUP  !m\_bInstaller && … &&  (m\_PFModifiedList.Count==5) | Modify 5 PE-files in ProgramFiles folder    (TROJAN\_GEN\_5.txt)  Worm.P2P.generic |
| 27 | REPORT\_EVENT\_TASKMGR\_PROT  "TaskManager protection" |  | CJob::ProcessEvent  MJ\_SYSTEM\_CREATE\_SECTION  SECTION\_MAP\_EXECUTE &&  (pProcess-> IsType(\_SPRC\_FLAG\_TASKMGR))… | R0 |
| 28 | REPORT\_EVENT\_DRIVER\_INS  "Suspicious driver installation" | CheckDrvReg | Interceptor\_CreateKey (CheckRegisterDriver)  “HKEY\_LOCAL\_MACHINE\ SYSTEM\CurrentControlSet\Services\KEY”  "%SystemRoot%\\ system32\\drivers\\KEY.sys" in ModifiedImagesList | Copy drv to %System%\drivers and Registry drv name in  REGISTRY\SYSTEM\ CurrentControlSet\Services  (DRIVER\_INS\_1\_1.txt) |
| Registry drv name in  REGISTRY\SYSTEM\ CurrentControlSet\Services and Copy drv in %System%\drivers  (DRIVER\_INS\_1\_2.txt) |
| CJob::RegistryEvent Interceptor\_SetValueKey  pwchKeyName ==  [\\registry\\machine\\system\\controlset???\\services\\\*](file:///\\registry\\machine\\system\\controlset%3f%3f%3f\\services\\*)  pwchValueName == "type" | Register drv name,  Register drv ImagePath  Copy drv to %System%\drivers,  Register drv Type  (DRIVER\_INS\_2.txt) |
| CJob::RegistryEvent Interceptor\_SetValueKey  pwchKeyName ==  [\\registry\\machine\\system\\controlset???\\services\\\*](file:///\\registry\\machine\\system\\controlset%3f%3f%3f\\services\\*)  pwchValueName == "imagepath" | Register drv name,  Copy drv to %System%\drivers,  Register drv Type  Register drv ImagePath  (DRIVER\_INS\_3.txt) |
|  | CJob::RegistryEvent Interceptor\_RestoreKey  MatchWithPattern( \\registry\\machine\\system\\controlset???\\services\\\*) | Copy drv to %System%\drivers,  Restore drv TypeImage by RegRestoreKey  (DRIVER\_INS\_4.txt) |
| 29 | REPORT\_EVENT\_HIDDEN\_SEND  "Hidden data sending" |  | CJob::ProcessEvent MJ\_SYSTEM\_ INTERPROC\_MESSAGE  (IsType(\_SPRC\_FLAG\_INETBORWSER)) &&  (MsgId == WM\_SETTEXT) | SetWindowText to browser window (IE)  (HIDDEN\_SEND\_1.txt) |
| CJob::R3Event R3\_BACKGROUNDCOPY JOB\_RESUME | IBackgroundCopyJob::Resume()  (HIDDEN\_SEND\_2.txt) |
| 31 | REPORT\_EVENT\_MASS\_MAILER  "Mass-mailer software" |  | PDM::MsgReceive pm\_IWGEN\_ MASS\_MAILER\_DETECTED | ? |
| 32 | REPORT\_EVENT\_BROWSERCONTROL  "Internet Browser Control" |  | MJ\_SYSTEM\_ USER\_POST\_MESSAGE::  WM\_DDE\_INITIATE  bBrowserTarget && “iexplore” | Open url throw DDE-functions (IExplore, WWW\_OpenURL)  (BROWSERCONTROL\_1.txt) |
| 33 | REPORT\_EVENT\_MAX | Not used | | |