Sign in

mbevilacqua / appcompatprocessor Public

Notifications Fork 25 Star 196

Code Issues 5 Pull requests 1 Actions Projects Wiki Security Insight

appcompatprocessor / AppCompatSearch.txt

Executable File · 143 lines (126 loc) · 7.67 KB

Code Blame Raw

```
### Global Config
### RegexSignatures Section - defines regex signatures used by the serach module against FilePath\F
### Format is [SignatureName]=REGEX_EXPRESSION / (REGEX_FILTER)
### Note that filter separator is: " / " and REGEX_FILTER must go between "()".
<RegexSignatures>
# Classic example of missplaced svchost.exe:
[Missplaced svchost]=\\svchost\.exe / (\\(Windows|WINNT)\\(System32|SysWOW64)\\svchost\.exe)

# Other missplaced stuff you probably want to be aware of
[Missplaced System File]=\\(cmd|lsass|rundll|rundll32|net|net1|taskeng|conhost|powershell|csvde|nlt

# Bad extensions
[Bad extensions]=\.(jpg|gif|bmp|png|txt|dat|sql|dmp|log)$

# Archivers on odd locations
[RAR]=\\rar(32|64)?\.exe$ / (\\WinRAR|\\wrar)
[7zip]=\\7za\.exe$ / ((\\VMware Player|\\utilities|\\tools[^\\]*|\\PortableApps\\|\\Lenovo\\System

# Misspelt Windows binaries example (use the leven module for this!)
[Misspeling svchost]=\\(scvhost|svch0st|svchosts|svchots|suchost|svchost\.)\.exe
[Misspeling rundll]=\\(rundll|rundll64)\.exe

# Stuf running where it normally shouldn't
[Exec Profile container]=\\((Users|Documents and Settings))\\[^\\]*\..{}3$
[Exec Profile root]=\\(Users|Documents and Settings)\\[^\\]*\\[^\\]\..{}3$
[Exec NetworkService]=\\(Users|Documents and Settings)\\NetworkService\\
[Exec System profile]=\\Windows\\system32\\config\\systemprofile\\
[Exec Recycle.Bin]=C:\\$Recycle\.Bin\\[^\\]*\.
[Exec Recycler]=C:\\RECYCLER\\[^\\]*\.
[Exec Web|Intel]=C:\\(Web|Intel)\\[^\\]*\.
[Exec Windows Subfolder Root]=C:\\(Windows|Winnt)\\(Debug|addins)\\[^\\]*\.
[Exec Windows Subfolder Any]=C:\\(Windows|Winnt)\\(repair|security)\\
[Exec Cookies]=\\Cookies\\[^\\]*\.
[Exec MachineKeys]=\\RSA\\MachineKeys\\
[Exec ProgramData/Gamarue]=\\ProgramData\\ms[^\\]*\.exe$
[Exec ProgramData]=\\ProgramData\\[^\\]*\..{}3$
[Exec Start Menu]=\\(Users|Documents and Settings)\\[^\\]*\\Start Menu\\[^\\]*\..{}3$
[Exec AppData]=\\(Users|Documents and Settings)\\[^\\]*\\AppData\\[^\\]*\..{}3$
[Exec Identities]=\\(Users|Documents and Settings)\\[^\\]*\\AppData\\Roaming\\Identities\\[^\\]*\..
[Exec Remote tsclient]=\\tsclient\\

# PLugX candidate sigs generously shared by Luis Rocha @countuponsec
[PlugX]=\\AShld\.exe
[PlugX]=\\CamMute\.exe / (\\Program Files\\Lenovo\\Communications Utility\\CAMMUTE\.exe)
[PlugX]=\\chrome_frame_helper\.exe / (\\program files( \(x86\)){0,1}\\Google\\Chrome\\application\\
[PlugX]=\\dvcemumanager\.exe / (\\Program Files( \(x86\)){0,1}\\Microsoft Device Emulator\\1\.0\\dv
[PlugX]=\\fsguidll\.exe
[PlugX]=\\fsstm\.exe
[PlugX]=\\Gadget\.exe / (\\Program Files\\Windows Media Player\\WMPSideShowGadget\.exe)
[PlugX]=\\hhc\.exe / (\\Program Files( \(x86\)){0,1}\\HTML Help Workshop\\hhc\.exe)
[PlugX]=\\hkcmd\.exe / (\\Windows\\System32\\hkcmd\.exe)
[PlugX]=\\LoLTWLauncher\.exe
[PlugX]=\\Mc\.exe / (\\Program Files( \(x86\)){0,1}\\(microsoft visual studio|Microsoft SDKs|Window
[PlugX]=\\mcf\.exe
[PlugX]=\\mcupdui\.exe
[PlugX]=\\mcut\.exe
[PlugX]=\\MsMpEng\.exe / (\\program files\\(Microsoft Security Client|Windows Defender)(\\AntiMalwa
[PlugX]=\\msseces\.exe / (\\Program Files\\Microsoft Security Client\\msseces\.exe)
[PlugX]=\\NvSmart\.exe
[PlugX]=\\OInfoP11\.exe / (\\Program Files( \(x86\)){0,1}\\Common Files\\Microsoft Shared\\MSINFO\\
[PlugX]=\\ACLUI\.DLL
[PlugX]=\\OleView\.exe / (\\Program Files( \(x86\)){0,1}\\(Microsoft SDKs|Windows Kits|microsoft vi
[PlugX]=\\POETWLauncher\.exe
[PlugX]=\\RasTls\.exe
[PlugX]=\\rc\.exe / (\\Program Files( \(x86\)){0,1}\\(microsoft.net|Windows Kits|Microsoft SDKs|mic
[PlugX]=\\RunHelp\.exe
[PlugX]=\\sep_NE\.exe
#[PlugX]=\\setup\.dll
[PlugX]=\\tplcdclr\.exe
[PlugX]=\\Ushata\.exe
[PlugX distnoted.exe]=\\distnoted\.exe / (Common Files\\Apple\\Apple Application Support)
[PLugX vmtoolsd.exe]=\\vmtoolsd.\exe / (\\VMware\\VMware Tools)
```

```

# Metasploit-dropped files with random file names
[Metasploit]=\\windows\\temp\\[a-zA-Z]{16}\.(exe|bat) / (VerifyAndInstall\.exe)

# Finds WinRAR directories in the Default User, All Users, and Network User accounts. This may indi
[WinRAR1]=\\Network user\\Application Data\\WinRAR
[WinRAR2]=\\All users\\Application Data\\WinRAR
[WinRAR3]=\\Default User\\Application Data\\WinRAR

# Known Bad / Dual use classics
[Known bad - dual use: rexec]=\\rexec\.exe
[Known bad - dual use: xcmd]=\\xcmd\.exe
[Known bad - dual use: servpw64]=\\servpw64
[Known bad - dual use: quarks]=\\quarks
[Known bad - dual use: psexec]=\\PsExe / (\\PSTools\\)
[Known bad - dual use: lcx]=\\lcx\.exe
[Known bad - dual use: nc]=\\nc\.exe
[Known bad - dual use: sdelete]=\\sdelete\.exe
[Known bad - dual use: nmap]=\\nmap\.exe
[Known bad - dual use: nping]=\\nping\.exe
[Known bad - dual use: zenmap]=\\zenmap\.exe
[Known bad - dual use: ndiff]=\\ndiff\.exe
[Known bad - dual use: ncat]=\\ncat\.exe
[Known bad - dual use: winrm]=\\winrm\.cmd
[Known bad - dual use: winrs]=\\winrs\.cmd
[Known bad - dual use: nbtscan]=\\nbtscan\.exe
[Known bad - dual use: WMIExec]=wmiexec
[Known bad - dual use: SMBScan]=smbscan
[Known bad - dual use: osql]=\\osql\.exe$ / (\\Microsoft SQL Server\\)
[Known bad - dual use: procdump]=\\(procdump|pdump|pc)(64)+\\.exe / (\\SysInternals\\)

### Cred Dumping
[Dumper - Common Names]=\\(q32|q64|wceaux|w86|q86|quarkpwd[^\\]*|m64|m32|hash32|hash64|64|32|w32|w6
[Dumper - GsecDump]=\\(g64\-|g32\-|gsecdump\.exe|gcx64\.|gcx32\.|gec\.|gse\.exe)
[Dumper - Other]=\\(pwhash|pwdump|fgdump)[^\\]*

# Generic methodology
[One character + ext]=\\.\..{1,3}$ / (\\cygwin\\|\\GnuWin32\\|Opera\\k\.(exe|bat)|\\R\\r-|\\Git\\us
[Numeric vbs]=\\.(\d)*\.vbs
[Char + Numeric vbs]=\\..(\d)*\.vbs
[Short file one directory from root]=C\:\\(?!(Windows|Bin))[a-zA-Z]{1,10}\\(?!hh)[a-zA-Z0-9]{1,3}\.
[Alternate Data Stream]=(\.|\\)[a-z0-9]{2,20}\:[a-z0-9\s\_\.]{1,40}
[Decoy Docs]=\.(wav|mp4|mp3|pdf|pptx|doc|docx|xlsx)\.(pif|exe|scr)
[Batch file in windows dir]=\\Windows\\[a-z]{1,10}\.bat$
[Numeric EXE in Windows or System32]=\\(Windows|system32)\\[0-9]{2,20}\.exe
[Short EXE in systemdrive]=C\:\\[a-z0-9\-\_]{1,5}\.[a-z0-9]{2,3}$
```

```
[Short EXE in Systemdrive]=C\:\\[a-z0-9\-\_]{1,5}\.[a-z0-9]{2,3}$
[Root of RarSFX .exe]=\\RarSFX\d\\[^\\]*\.exe / (\\RarSFX\d\\lsetup\.exe|\\intiupdater\.exe)

# KnownBad
# Backdoor.Adwind search for a runkey using this legitimate but missplaced copy of java
[Backdoor.Adwind]=\\(Users|Documents and Settings)\\[^\\]*\\AppData\\Roaming\\Oracle\\bin\\javaw.ex

# Classic attacker staging folders
[Staging Root]=C:\\(Recovery|Intel|Web)\\
[Staging1]=C:\\(Windows|Winnt)\\(Help|Web|Media|ime|Debug|Fonts)\\ / (\\WINDOWS\\IME\\im[^\\]*_1\\I
[Staging System Volume Information]=\\System Volume Information\\
[Staging perf.]=\\(perflogs|perfdata)\\

# Generic startup persistance flagging
[Startup persistence]=\\Start Menu\\Programs\\Startup

# Execution using a volume name in the ’dot’ namespace. Used by some malware with encrytped VFS's
# Uroburos example shimcache entry: "01/01/10 xx:xx:xx N/A 900ff1\rexec.exe N/A False"
# Signature is good but will unfortunately hit on everything ShimCache parses incorrectly.
[Exec from VFS]=^(?!SYSVOL)(?!UNC)(?!\\\?)(?![A-Z]:)[^\\:]*\\ / (None\\None)

# Interesting entries pointing to USB drives (experimental)
[USB]=^STORAGE#Volume#_.._USBSTOR#

</RegexSignatures>
### End of regex signatures
```