




 [Product](#) [Solutions](#) [Resources](#) [Open Source](#) [Enterprise](#) [Pricing](#) [Sign in](#) [Sign up](#)


 [mbevilacqua / appcompatprocessor](#) Public


 Notifications


 Fork 25


 Star 196


 **Code**


 Issues 5


 Pull requests 1

 Actions

 Projects

 Wiki

 Security

 Insights

A screenshot of the Android Studio file explorer. At the top, the project name '6c84793' is displayed with a search icon to its right. Below this is a search bar containing the text 'Go to file'. The file list is organized into two main sections: 'Ingest' and 'test'. The 'test' section is expanded, showing a list of files. The file 'AppCompatSearch.txt' is highlighted with a blue background. Other files in the list include '.travis.yml', 'AmCacheParser.py', 'AppCompatProcessor.py', 'LICENSE', 'README.md', 'ShimCacheParser_ACP.py', 'appAux.py', 'appDB.py', 'appLoad.py', 'appSearch.py', 'mpEngineProdCons.py', 'mpEngineWorker.py', 'namedlist.py', 'reconFiles.txt', 'requirements.txt', 'runtest.sh', 'settings.py', and 'setup.py'. Each file is preceded by a document icon.

appcompatprocessor / AppCompatSearch.txt

Matias Bevilacqua · 498b63d · 4 years ago

History

CodeBlameExecutable File · 143 lines (126 loc) · 7.67 KBRawDownload

```
1  ### Global Config
2  ### RegexSignatures Section - defines regex signatures used by the serach module agains
3  ### Format is [SignatureName]=REGEX_EXPRESSION / (REGEX_FILTER)
4  ### Note that filter separator is: " / " and REGEX_FILTER must go between "()".
5  <RegexSignatures>
6  # Classic example of misplaced svchost.exe:
7  [Misplaced svchost]=\\svchost\.exe / (\\(Windows|WINNT)\\(System32|SysWOW64)\\svchost\
8
9  # Other misplaced stuff you probably want to be aware of
10 [Misplaced System File]=\\(cmd|lsass|rundll|rundll32|net|net1|taskeng|conhost|powershe
11
12 # Bad extensions
13 [Bad extensions]=\. (jpg|gif|bmp|png|txt|dat|sql|dmp|log)$
14
15 # Archivers on odd locations
16 [RAR]=\\rar(32|64)?\.exe$ / (\\WinRAR|\\wrar)
17 [7zip]=\\7za\.exe$ / ((\\VMware Player|\\utilities|\\tools[^\\]*|\\PortableApps\\|\\Len
18
19 # Misspelt Windows binaries example (use the leven module for this!)
20 [Misspeling svchost]=\\(scvhost|svch0st|svchosts|svchots|suchost|svchost\\.\\.\\.exe
21 [Misspeling rundll]=\\(rundll|rundll64)\\.exe
22
23 # Stuf running where it normally shouldn't
24 [Exec Profile container]=\\((Users|Documents and Settings)\\)[^\\]*\\.\\.\\.{}3$
25 [Exec Profile root]=\\((Users|Documents and Settings)\\)[^\\]*\\.[^\\]*\\.\\.\\.{}3$
26 [Exec NetworkService]=\\((Users|Documents and Settings)\\)\\NetworkService\\
27 [Exec System profile]=\\Windows\\system32\\config\\systemprofile\\
28 [Exec Recycle.Bin]=C:\\$Recycle\\.Bin\\[^\\]*\\.
29 [Exec Recycler]=C:\\RECYCLER\\[^\\]*\\.
30 [Exec Web|Intel]=C:\\(Web|Intel)\\[^\\]*\\.
31 [Exec Windows Subfolder Root]=C:\\(Windows|Winnt)\\(Debug|addins)\\[^\\]*\\.
32 [Exec Windows Subfolder Any]=C:\\(Windows|Winnt)\\(repair|security)\\
33 [Exec Cookies]=\\Cookies\\[^\\]*\\.
34 [Exec MachineKeys]=\\RSA\\MachineKeys\\
35 [Exec ProgramData/Gamarue]=\\ProgramData\\ms[^\\]*\\.exe$
36 [Exec ProgramData]=\\ProgramData\\[^\\]*\\.\\.\\.{}3$
37 [Exec Start Menu]=\\(Users|Documents and Settings)\\[^\\]*\\Start Menu\\[^\\]*\\.\\.\\.{}3$
38 [Exec AppData]=\\(Users|Documents and Settings)\\[^\\]*\\AppData\\[^\\]*\\.\\.\\.{}3$
39 [Exec Identities]=\\(Users|Documents and Settings)\\[^\\]*\\AppData\\Roaming\\Identie
40 [Exec Remote tsclient]=\\tsclient\\
41
42 # PLugX candidate sigs generously shared by Luis Rocha @countuponse
43 [PlugX]=\\ASHld\\.exe
44 [PlugX]=\\CamMute\\.exe / (\\Program Files\\Lenovo\\Communications Utility\\CAMMUTE\\.exe
45 [PlugX]=\\chrome_frame_helper\\.exe / (\\program files( \\(x86\\))){0,1}\\Google\\Chrome\\a
46 [PlugX]=\\dvcemumanager\\.exe / (\\Program Files( \\(x86\\))){0,1}\\Microsoft Device Emulat
47 [PlugX]=\\fsguidll\\.exe
48 [PlugX]=\\fsstm\\.exe
49 [PlugX]=\\Gadget\\.exe / (\\Program Files\\Windows Media Player\\WMPSideShowGadget\\.exe)
50 [PlugX]=\\hhc\\.exe / (\\Program Files( \\(x86\\))){0,1}\\HTML Help Workshop\\hhc\\.exe)
51 [PlugX]=\\hkcmd\\.exe / (\\Windows\\System32\\hkcmd\\.exe)
52 [PlugX]=\\LoLTWLauncher\\.exe
53 [PlugX]=\\Mc\\.exe / (\\Program Files( \\(x86\\))){0,1}\\(microsoft visual studio|Microsoft
54 [PlugX]=\\mcf\\.exe
55 [PlugX]=\\mcupdui\\.exe
56 [PlugX]=\\mcut\\.exe
57 [PlugX]=\\McMnEng\\.exe / (\\Program Files\\Microsoft Security Client\\Windows Defender\\
```

```
57 [PlugX]=\\msmpeng\\.exe / (\\Program Files\\Microsoft Security Client\\Windows Defender)
58 [PlugX]=\\msseces\\.exe / (\\Program Files\\Microsoft Security Client\\msseces\\.exe)
59 [PlugX]=\\NvSmart\\.exe
60 [PlugX]=\\OInfoP11\\.exe / (\\Program Files( \\(x86\\)){0,1}\\Common Files\\Microsoft Shar
61 [PlugX]=\\ACLUI\\.DLL
62 [PlugX]=\\OleView\\.exe / (\\Program Files( \\(x86\\)){0,1}\\(Microsoft SDKs|Windows Kits|
63 [PlugX]=\\POETWLauncher\\.exe
64 [PlugX]=\\RasTls\\.exe
65 [PlugX]=\\rc\\.exe / (\\Program Files( \\(x86\\)){0,1}\\(microsoft.net|Windows Kits|Micros
66 [PlugX]=\\RunHelp\\.exe
67 [PlugX]=\\sep_NE\\.exe
68 #[PlugX]=\\setup\\.dll
69 [PlugX]=\\tplcdclr\\.exe
70 [PlugX]=\\Ushata\\.exe
71 [PlugX distnoted.exe]=\\distnoted\\.exe / (Common Files\\Apple\\Apple Application Support
72 [PLugX vmtoolsd.exe]=\\vmtoolsd\\.exe / (\\VMware\\VMware Tools)
73
74 # Metasploit-dropped files with random file names
75 [Metasploit]=\\windows\\temp\\[a-zA-Z]{16}\\.exe|bat) / (VerifyAndInstall\\.exe)
76
77 # Finds WinRAR directories in the Default User, All Users, and Network User accounts. T
78 [WinRAR1]=\\Network user\\Application Data\\WinRAR
79 [WinRAR2]=\\All users\\Application Data\\WinRAR
80 [WinRAR3]=\\Default User\\Application Data\\WinRAR
81
82 # Known Bad / Dual use classics
83 [Known bad - dual use: rexec]=\\rexec\\.exe
84 [Known bad - dual use: xcmd]=\\xcmd\\.exe
85 [Known bad - dual use: servpw64]=\\servpw64
86 [Known bad - dual use: quarks]=\\quarks
87 [Known bad - dual use: psexec]=\\PsExe / (\\PSTools\\)
88 [Known bad - dual use: lcx]=\\lcx\\.exe
89 [Known bad - dual use: nc]=\\nc\\.exe
90 [Known bad - dual use: sdelete]=\\sdelete\\.exe
91 [Known bad - dual use: nmap]=\\nmap\\.exe
92 [Known bad - dual use: nping]=\\nping\\.exe
93 [Known bad - dual use: zenmap]=\\zenmap\\.exe
94 [Known bad - dual use: ndiff]=\\ndiff\\.exe
95 [Known bad - dual use: ncat]=\\ncat\\.exe
96 [Known bad - dual use: winrm]=\\winrm\\.cmd
97 [Known bad - dual use: winrs]=\\winrs\\.cmd
98 [Known bad - dual use: nbtscan]=\\nbtscan\\.exe
99 [Known bad - dual use: WMIExec]=wmiexec
100 [Known bad - dual use: SMBScan]=smbscan
101 [Known bad - dual use: osql]=\\osql\\.exe$ / (\\Microsoft SQL Server\\)
102 [Known bad - dual use: procdump]=\\(procdump|pdump|pc)(64)+\\.exe / (\\SysInternals\\)
103
104 ### Cred Dumping
105 [Dumper - Common Names]=\\(q32|q64|wceaux|w86|q86|quarkpwd[^\]*|m64|m32|hash32|hash64|
106 [Dumper - GsecDump]=\\(g64\\-|g32\\-|gsecdump\\.exe|gcx64\\.|gcx32\\.|gec\\.|gse\\.exe)
107 [Dumper - Other]=\\(pwhash|pwdump|fgdump)[^\]*
108
109 # Generic methodology
110 [One character + ext]=\\.\\.\\.\\{1,3}$ / (\\cygwin\\|\\GnuWin32\\|Opera\\k\\.exe|bat)|\\R\\
111 [Numeric vbs]=\\.\\.\\.\\(d)*\\.vbs
112 [Char + Numeric vbs]=\\.\\.\\.\\(d)*\\.vbs
113 [Short file one directory from root]=C:\\(?!\\(Windows|Bin))\\[a-zA-Z]{1,10}\\(?!hh)\\[a-zA-
114 [Alternate Data Stream]=\\.\\.\\[a-z0-9]{2,20}\\:[a-z0-9\\s\\_\\.]{1,40}
115 [Decoy Docs]=\\.\\(wav|mp4|mp3|pdf|pptx|doc|docx|xlsx)\\.\\(pif|exe|scr)
116 [Batch file in windows dir]=\\Windows\\[a-z]{1,10}\\.bat$
117 [Numeric EXE in Windows or System32]=\\(Windows|system32)\\[0-9]{2,20}\\.exe
118 [Short EXE in systemdrive]=C:\\[a-z0-9\\-\\_]{1,5}\\.[a-z0-9]{2,3}$
119 [Root of RarSFX .exe]=\\RarSFX\\d\\[^\]*\\.exe / (\\RarSFX\\d\\lsetup\\.exe|\\intiupdater\\
120
121 # KnownBad
122 # Backdoor.Adwind search for a runkey using this legitimate but missplaced copy of java
123 [Backdoor.Adwind]=\\(Users|Documents and Settings)\\[^\]*\\AppData\\Roaming\\Oracle\\b
124
125 # Classic attacker staging folders
126 [Staging Root]=C:\\(Recovery|Intel|Web)\\
127 [Staging1]=C:\\(Windows|Winnt)\\(Help|Web|Media|ime|Debug|Fonts)\\ / (\\WINDOWS\\IME\\i
128 [Staging System Volume Information]=\\System Volume Information\\
129 [Staging perf.]=\\(perflogs|perfdata)\\
130
131 # Generic startup persistence flagging
```

```
132     [Startup persistence]=\\Start Menu\\Programs\\Startup
133
134     # Execution using a volume name in the 'dot' namespace. Used by some malware with encry
135     # Uroburos example shimcache entry: "01/01/10 xx:xx:xx N/A 900ff1\\rexec.exe N/A False"
136     # Signature is good but will unfortunately hit on everything ShimCache parses incorrect
137     [Exec from VFS]=^(?!SYSVOL)(?!UNC)(?!\\\\?)(?![A-Z:])[^\\:]*\\ / (None\\None)
138
139     # Interesting entries pointing to USB drives (experimental)
140     [USB]=^STORAGE#Volume#_._USBSTOR#
141
142     </RegexSignatures>
143     ### End of regex signatures
```