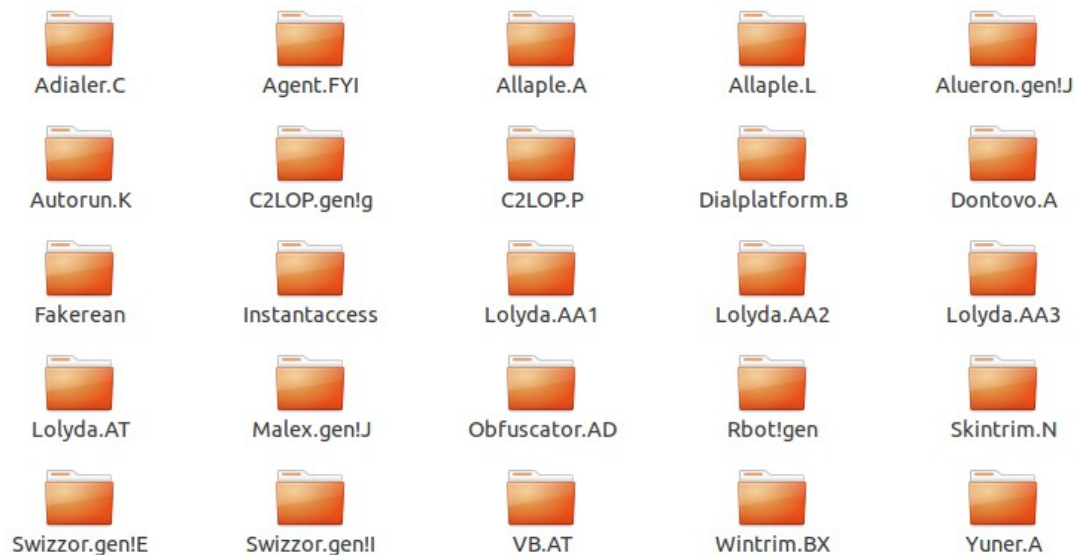


Propostas de Projeto TCC 2017

Prof. Edmar Rezende

Repositório de Malware



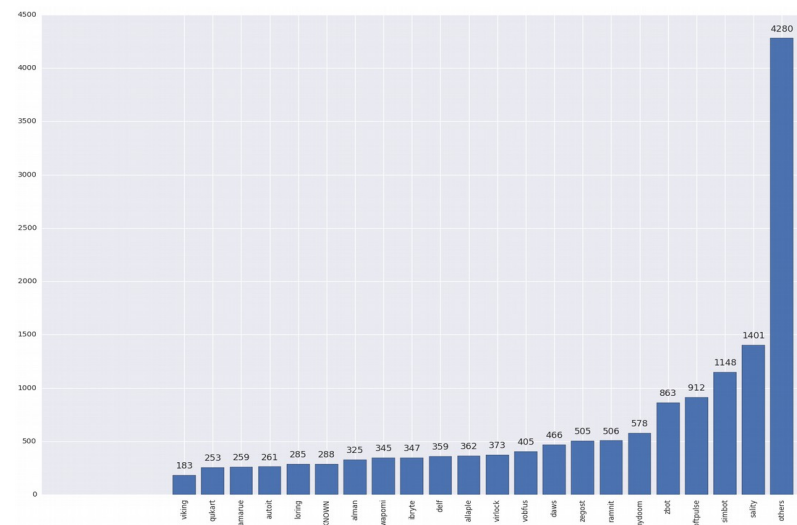
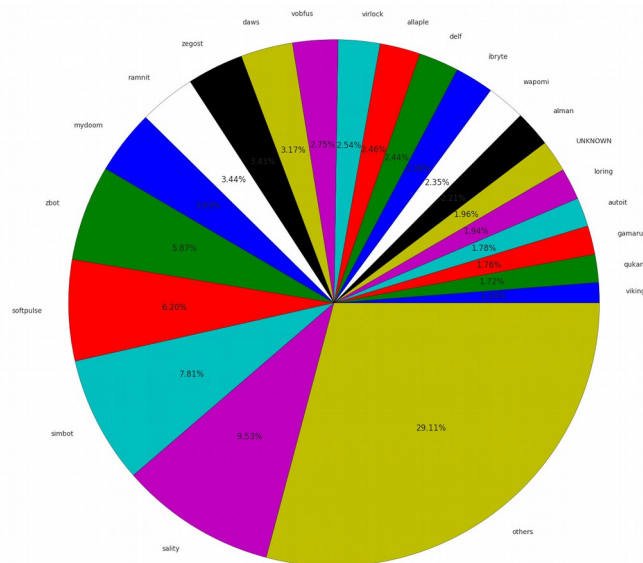
10.136 malware

20 famílias

5.571 Android

180 famílias

■ viking: 183 (1.24%)
■ qikart: 253 (1.72%)
■ gamarue: 259 (1.76%)
■ autoit: 261 (1.78%)
■ loring: 285 (1.94%)
■ UNKNOWN: 288 (1.96%)
■ alman: 325 (2.21%)
■ wapomi: 345 (2.35%)
■ bryte: 347 (2.36%)
■ defl: 359 (2.44%)
■ allapple: 362 (2.46%)
■ verlock: 373 (2.54%)
■ vobfus: 405 (2.75%)
■ dave: 466 (3.17%)
■ zegost: 505 (3.43%)
■ ramnit: 506 (3.44%)
■ mydoom: 578 (3.93%)
■ zbot: 863 (5.87%)
■ softpulse: 912 (6.20%)
■ simbot: 1148 (7.81%)
■ sality: 1401 (9.53%)
■ others: 4280 (29.11%)



Análise de Malware

Análise Estática

```
push    ecx ; s
call    ds:connect
test    eax, eax
jz      short loc_401604

Sleep and loop back

loc_401604:
; size_t
push    44h
push    0 ; int
lea     eax, [ebp+StartupInfo]
push    eax ; void *
call    _memset
add     esp, 0Ch
mov     [ebp+StartupInfo.cb], 44h
mov     [ebp+StartupInfo.dwFlags], 101h
mov     [ebp+StartupInfo.wShowWindow], 0
mov     ecx, [ebp+s]
mov     [ebp+StartupInfo.hStdError], ecx
mov     edx, [ebp+s]
mov     [ebp+StartupInfo.hStdOutput], edx
mov     eax, [ebp+s]
mov     [ebp+StartupInfo.hStdInput], eax
lea     ecx, [ebp+ProcessInformation]
push    ecx ; lpProcessInformation
lea     edx, [ebp+StartupInfo]
push    edx ; lpStartupInfo
push    0 ; lpCurrentDirectory
push    0 ; lpEnvironment
push    0 ; dwCreationFlags
push    1 ; bInheritHandles
push    0 ; lpThreadAttributes
push    0 ; lpProcessAttributes
push    offset CommandLine ; "cmd.exe"
push    0 ; lpApplicationName
call    ds:CreateProcessA
test    eax, eax
jnz     short loc_401678

call    ds:GetLastError
```

Análise Dinâmica

| Time | Process Name | PID | Operation | Path | Result | Detail |
|----------|------------------|------|---------------------|-------------------------------------|-------------------|--|
| 12:41... | SearchIndexer... | 1620 | FileSystemControlC: | | SUCCESS | Control: FSCTL_READ_USN_JOURNAL |
| 12:41... | SearchIndexer... | 1620 | FileSystemControlC: | | SUCCESS | Control: FSCTL_READ_USN_JOURNAL |
| 12:41... | svchost.exe | 908 | QueryNameInfo... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | Name: \Program Files\ESET\ESET NO... |
| 12:41... | svchost.exe | 908 | CreateFile | C:\Program Files\ESET\ESET NOD32... | SUCCESS | Desired Access: Generic Read, Disposi... |
| 12:41... | svchost.exe | 908 | CreateFileMapo... | C:\Program Files\ESET\ESET NOD32... | FILE LOCKED WI... | SyncType: SyncTypeCreateSection, Pag... |
| 12:41... | svchost.exe | 908 | QueryStandardl... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | AllocationSize: 1,343,488, EndOfFile: 1,3... |
| 12:41... | svchost.exe | 908 | CreateFileMapo... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | SyncType: SyncTypeOther |
| 12:41... | svchost.exe | 908 | CloseFile | C:\Program Files\ESET\ESET NOD32... | SUCCESS | |
| 12:41... | svchost.exe | 908 | CreateFile | C:\Program Files\ESET\ESET NOD32... | SUCCESS | Desired Access: Generic Read, Disposi... |
| 12:41... | svchost.exe | 908 | QueryStandardl... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | AllocationSize: 1,343,488, EndOfFile: 1,3... |
| 12:41... | svchost.exe | 908 | CreateFileMapo... | C:\Program Files\ESET\ESET NOD32... | FILE LOCKED WI... | SyncType: SyncTypeCreateSection, Pag... |
| 12:41... | svchost.exe | 908 | QueryStandardl... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | AllocationSize: 1,343,488, EndOfFile: 1,3... |
| 12:41... | svchost.exe | 908 | CreateFileMapo... | C:\Program Files\ESET\ESET NOD32... | SUCCESS | SyncType: SyncTypeOther |
| 12:41... | svchost.exe | 908 | CloseFile | C:\Program Files\ESET\ESET NOD32... | SUCCESS | |
| 12:41... | svchost.exe | 908 | ReadFile | C:\Windows\System32\wintrust.dll | SUCCESS | Offset: 288,256, Length: 1,536, I/O Flag... |
| 12:41... | svchost.exe | 908 | CreateFile | C:\Program Files\ESET\ESET NOD32... | SUCCESS | Desired Access: Generic Read, Disposi... |
| 12:41... | svchost.exe | 908 | ReadFile | C:\Windows\System32\imagehlp.dll | SUCCESS | Offset: 60,416, Length: 2,048, I/O Flags... |
| 12:41... | svchost.exe | 908 | ReadFile | C:\Windows\System32\imagehlp.dll | SUCCESS | Offset: 25,600, Length: 31,232, I/O Flan... |

Showing 1,624,846 of 1,877,838 events (86%) Backed by virtual memory

Propostas

Análise automática

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File

URL

Search

No file selected

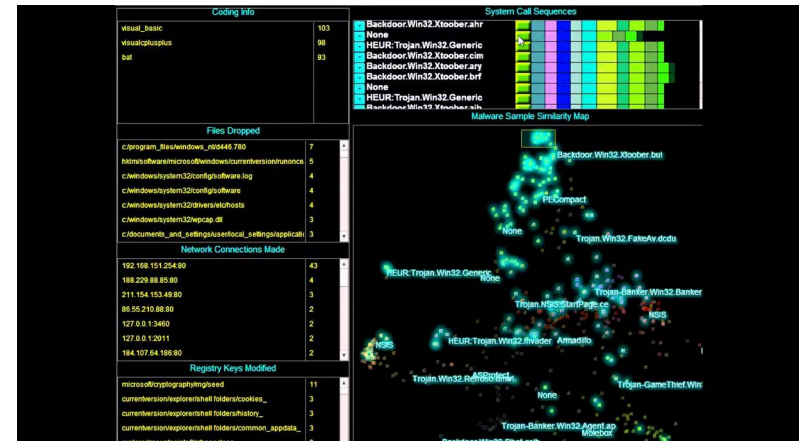
Choose File

Maximum file size: 128MB

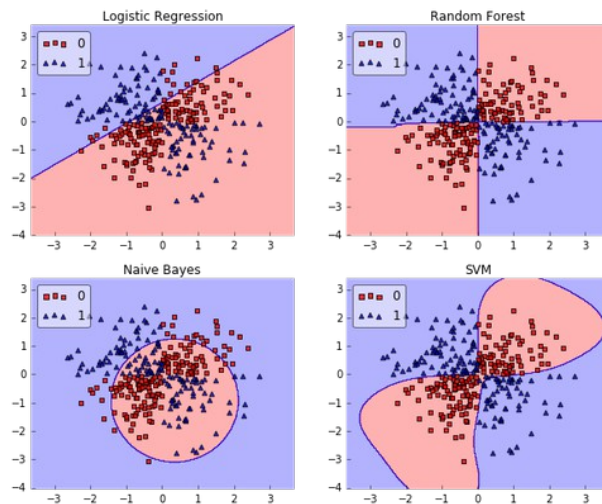
By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

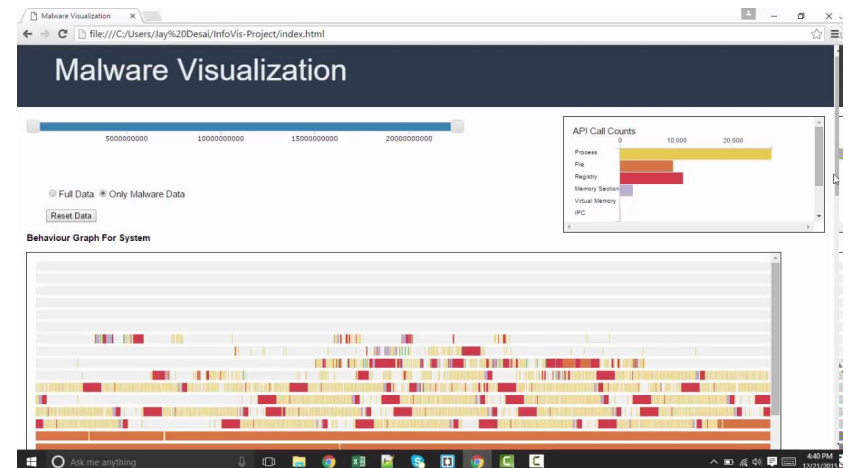
Visualização



Machine Learning



Interatividade



Candidatos

