# Banload

As the adoption of online banking within Brazil continues to grow, a corresponding rise in banking malware targeting this developing market is also being observed.

The prolific Brazilian cybercrime group behind the banking malware “Banload” have implemented an interesting new driver component, internally called ‘FileDelete’, to remove software drivers and executables belonging to anti-malware and banking protection programs. The goal behind this driver is to enable fraud through credential theft and account-takeover operations on a victim’s machine.

This trojan target the anti-malware software drivers and executables and deletes them and below are few samples:

C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportAegle64.sys

C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportEI64.sys

C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportHades64.sys

C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportKE64.sys

C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportPG64.sys

C:\Program Files (x86)\Trusteer\Rapport\bin\RapportMgmtService.exe

C:\Program Files (x86)\Trusteer\Rapport\bin\RapportService.exe

C:\Program Files\Trusteer\Rapport\bin\RapportAegle.sys

C:\Program Files\Trusteer\Rapport\bin\RapportEI.sys

C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys

C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe

C:\Program Files\Trusteer\Rapport\bin\RapportService.exe

C:\Program Files\AVAST Software\Avast\AvastUI.exe

C:\Program Files\AVAST Software\Avast\AvLaunch.exe

C:\Program Files\AVAST Software\Avast\AvEmUpdate.exe

C:\Program Files\AVG\Antivirus\AvEmUpdate.exe

C:\Program Files\AVG\Antivirus\AVGUI.exe

C:\Program Files\AVG\Antivirus\AvLaunch.exe

## File Properties

1. SHA-256 - ab935f5bfc756a7d085c0ec952c3bcadff44e37d4153f6bb3d6bda34199481ca
2. File type - Win32 EXE (PE32+ executable for MS Windows)
3. X509 Certificates –
   1. Thawte Code Signing CA - G2
   2. M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA
   3. thawte Primary Root CA
   4. GlobalSign TSA for Standard
   5. GlobalSign Timestamping CA
4. Imports - ntoskrnl.exe

## Yara Strings and Description

1. !This program cannot be run in DOS mode.
   1. This is windows executable file.
2. IrpFileDelete
   1. Kernel-mode Driver Targets AV Solutions
   2. The malware utilizes IRP using IoAllocateIrp and then forces deletion using IrpFileDelete function.
   3. The malware then forces deletion of the file passing the object handle from the previous call. Then to IoGetBaseFileSystemDeviceObject and IoGetNextIrpStackLocation, adjusting both IrpSetFileAttributes and IrpFileDelete function.
   4. The developer left quite a few notable DbgPrint elements meant to debug the flow of the driver such as “Normal Call MJ[%d] %p”, “Force Delete …” etc.
3. ntoskrnl.exe
   1. The driver malware consists of 6 sections with 25 imports from ntoskrnl and 1 from HAL.dll. The driver malware is rather simple and consists of debugging elements with the program database (PDB) path as

“F:\Sistema\Drivers-Denis\FileDelete\FileDelete\x64\Debug\B.sys.”

1. Indicators of Compromise (IOCs)
   1. PDB: F:\Sistema\Drivers-Denis\FileDelete\FileDelete\Debug\B.pdb
   2. PDB: F:\Sistema\Drivers-Denis\FileDelete\FileDelete\x64\Debug\B.pdb
2. Digital Signatures
   1. Thawte Code Signing CA - G2
   2. M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA
   3. thawte Primary Root CA
   4. GlobalSign TSA for Standard
   5. GlobalSign Timestamping CA

Reason: A digital certificate allows the malware to have a lower static detection among security solutions that implicitly trust code with a valid signature.

The FileDelete driver is installed via the group Golang loader, leveraging PowerShell, and it is digitally signed with a certificate with the name “M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA”.

## References:

1. <https://labs.sentinelone.com/cybercrime-banload-banking-malware-fraud/>
2. <https://bazaar.abuse.ch/sample/b976d31b09eb89271af890b2e20044d8db82060d32e70df317f45f0200aeeac4/#yara>
3. <https://bazaar.abuse.ch/browse/yara/suspicious_msi_file/>
4. <https://blog.scilabs.mx/en/2020/07/14/cosmic-banker-campaign-is-still-active-revealing-link-with-banload-malware/>