**Banload Malware signature Identification using Yara Rule**

Introduction of the Malware:

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

Infection Channel:

This malware Dropped by other malware, downloaded from the Internet.

BANLOAD malware variants arrive on the systems as files dropped by other malware or as files downloaded unknowingly by users when visiting malicious sites. When executed, these connect to malicious URLs to download other malware on already infected systems which leads to further infection. BANLOAD variants are known to download [BANKER](http://about-threats.trendmicro.com/Malware.aspx?language=us&name=BANKER) malware variants.

Attack:

In 2010, cybercriminals took advantage of the Haiti earthquake as a spam trap. The spammed messages written in Portuguese tricked users into clicking a link that supposedly contains photos of the earthquake. This led to a malicious website that downloads [TROJ\_BANLOAD.JAE](http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_BANLOAD.JAE).

Cybercriminals also copied the site of the Ministry of Labour and Employment in Brazil to spread [TROJ\_BANLOAD.JMO](http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_BANLOAD.JMO). When executed, it gathers email addresses and downloads BANKER variants.

## 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
5. Memory Resident: Yes
6. Payload: Downloads files

Installation:

This Trojan drops the following copies of itself into the affected system:

* %System%\incognito.exe
* %Program Files%\Common Files\Files.exe
* %System%\aqlb.hjo
* %Windows%\system\{malware file name}.exe

(%System% is the Windows system folder, which is usually C:\Windows\System32.. %Program Files% is the default Program Files folder, usually C:\Program Files in Windows 2000, Server 2003, and XP (32-bit), Vista (32-bit), and 7 (32-bit), or C:\Program Files (x86) in Windows XP (64-bit), Vista (64-bit), and 7 (64-bit).%Windows% is the Windows folder, which is usually C:\Windows.)

It drops the following files:

* %Windows%\Envia.txt
* %User Profile%\fxconfig.bat
* %Current%\{malware name}-up.txt
* %Program Files%\Common Files\Microsoft Shared\Web Folders\MSONSEXT409.dll

(%Windows% is the Windows folder, which is usually C:\Windows.. %User Profile% is the current user's profile folder, which is usually C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003, or C:\Users\{user name} on Windows Vista and 7.. %Program Files% is the default Program Files folder, usually C:\Program Files in Windows 2000, Server 2003, and XP (32-bit), Vista (32-bit), and 7 (32-bit), or C:\Program Files (x86) in Windows XP (64-bit), Vista (64-bit), and 7 (64-bit).)

**Downloads and Installs Additional Malware**  
Files detected as TrojanDownloader:Win32/Banload can download other malware by connecting to remote servers, usually via HTTP or FTP. These downloaded malware are usually members of the [Win32/Banker](http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32%2fBanker) family; trojans that steal banking credentials and other sensitive data, and send it back to a remote attacker.

**Modifies Internet Settings**  
TrojanDownloader:Win32/Banload modifies the system's Internet settings by modifying the system registry to bypass the network proxy setting:  
Adds value: "ProxyBypass"  
With value: "1"  
To subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\

AutoStart Technique:

This Trojan adds the following registry entries to enable its automatic execution at every system startup:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows\CurrentVersion\Run  
{random string} = "{malware path and file name}.exe"

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Active Setup\Installed Components\ {ADEEAF15-7FE8-DEDD-3FFF-4DF56EBB1DFB}  
StubPath = "{malware path and file name}.exe"

It modifies the following registry entries to enable its automatic execution at every system startup:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows NT\CurrentVersion\Winlogon  
Shell = "Explorer.exe rundll32.exe {malware file name) lhoweid"

(Note: The default value data of the said registry entry is Explorer.exe.)

Additional Details:

This Trojan connects to the following possibly malicious URL:

* http://{BLOCKED}ana-walker.com/site/msdos.exe
* http://www.{BLOCKED}rg.br/v2/env/msdos.exe
* http://www.{BLOCKED}kanan.net//espace\_pro/msdos.exe
* http://www.{BLOCKED}eton.ru/por/setup64.exe
* http://{BLOCKED}chomes.in/images/images.rar
* http://{BLOCKED}olhado.com.br/js/images.rar
* http://{BLOCKED}l-levata.com/js/images.rar
* http://{BLOCKED}.com/js/images.rar
* http://{BLOCKED}x-arq.com/js/images.rar
* http://{BLOCKED}igoseamigos2010.kit.net/images.rar
* http://{BLOCKED}lacionandoamigos.kit.net/images.rar
* http://{BLOCKED}lpemacla.kit.net/images.rar
* http://{BLOCKED}nanet2006.kit.net/images.rar
* http://{BLOCKED}usamonteloavalanche.kit.net/images.rar
* http://{BLOCKED}igossysters.kit.net/images.rar
* http://{BLOCKED}perbonus.kit.net/images.rar
* http://{BLOCKED}amigos2010.kit.net/images.r
* http://www.{BLOCKED}nvirtual.com/index.php
* http://www.{BLOCKED}a.net/image/top\_02.gif
* http://{BLOCKED}.{BLOCKED}.0.28/img/imag1.gif
* http://{BLOCKED}x.mogsoft.de/gallery2dir/themes/ice/compactone.exe
* http://{BLOCKED}x.mogsoft.de/gallery2dir/themes/ice/compress.exe

## Yara Strings to detect Banload Malware 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. The malware is trying to delete any AV solutions present on the victim machine. And in order to do that it has the paths of various antivirus software are present in the code.

These path files can be used to identify the malware. The condition is such that it identify if there are paths of different AVs on a single file.

* "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\\AVAST Software\\Avast\\AvastUI.exe"

1. “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

The malware uses the filedelete function in order to delete files from the victim machine. The string above can be used to identify it.

1. 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
2. URL: “http://th.symcb.com”

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/>
5. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=TrojanDownloader%3AWin32%2FBanload