BanLoad

Contents

[Introduction 2](#_Toc81606994)

[First Attack 2](#_Toc81606995)

[Method of Infection 2](#_Toc81606996)

[How Banload works? 3](#_Toc81606997)

[Installation 3](#_Toc81606998)

[Downloads and Installs Additional Malware 4](#_Toc81606999)

[Modifies Internet Settings 4](#_Toc81607000)

[Payload 4](#_Toc81607001)

[Disables security software 4](#_Toc81607002)

[Steals banking information 4](#_Toc81607003)

[Proxy functionality 4](#_Toc81607004)

[AutoStart Technique 4](#_Toc81607005)

[Additional Details 5](#_Toc81607006)

[MITRE ATT&CK 5](#_Toc81607007)

[Sample File Properties 6](#_Toc81607008)

[Yara Strings and Description 6](#_Toc81607009)

[References 7](#_Toc81607010)

# Introduction

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. Banload is a banking trojan believed to be developed by Brazilian cybercriminals and is used primarily to infect machines in Latin America. One notable aspect of Banload is it's use of custom kernel drivers to evade detection.

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

# First 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.

Cybercriminals also copied the site of the Ministry of Labour and Employment in Brazil to spread TROJ\_BANLOAD.JMO. When executed, it gathers email addresses and downloads BANKER variants.

# Method of Infection

Banload has been around since the last decade. This malware generally arrives on a victim’s system through a spam email containing an archived file or bundled software as an attachment. In a few cases, this malware may also be dropped by other malware or a drive-by download. When executed, Banload downloads other malware, often banking Trojans, on the victim’s system to carry out further infections. We have observed this malware is using the functionality of the legitimate freeware Mep Installer to carry out the infection cycle.

Mep Installer builds installation programs for Windows based on Inno Setup. When Mep Installer executes, it creates a temporary installation file in the %TEMP% directory. Mep Installer has its signature at the offset used in the preceding command:



This temporary installation file checks for the Mep Installer signature. If found, the file will read data from the third argument, which is a zlib-compressed file. The temporary installation file has a zlib decompression procedure. After decompression it drops the executable and runs it.



We have observed that Banload hooks the Mep Installer to trick users into installing the Portuguese version of this software. Once the user gets a Banload-infected Mep Installer, the malware uses same functionality as the genuine Mep Installer to avoid suspicion. The infected version carries the malware inside the zlib-compressed file.

# How Banload works?

## Installation

Win32/Banker can be downloaded into your PC by other malware, often detected as Win32/Banload variants. Banker files can have file extensions of JPEG, SCR, GIF, CPL, VXD, PIF, or MP3. Most Win32/Banker variants target customers of Brazilian banks; however, some variants also target banks in Mexico, Argentina, Spain, France, United Kingdom, and Ireland, to name a few.

Many variants of Win32/Banker drop copies of themselves along with configuration files to different folders on the infected PC, such as the default Windows folder, the default Windows system folder, and the default start-up folder. Its main executable might contain the string cartao, which is the Portuguese word for card. Win32/Banker also often configures itself to automatically run each time Windows starts by editing the system registry, or by installing itself as a Browser Helper Object (BHO) with its own unique GUID.

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 malwares are usually members of the Win32/Banker 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\*

## Payload

### Disables security software

Some variants try to disable security software like antivirus and firewall programs.

### Steals banking information

Many Win32/Banker variants check what browsers are open and what websites the browsers are open to. Specifically, it checks if the webpage title or URL pertain to banking websites. Many variants log keystrokes to record whatever you enter to log onto the website. To be more effective at stealing your banking information, Win32/Banker might display a webpage similar in appearance to your actual banking website, in which case the credentials you enter are directly sent to a hacker. It can also take screenshots of your infected PC if you access the bank login page.

Win32/Banker send the stolen information to a hacker in different ways, including sending an email to the attacker, uploading the stolen information to a hacker's FTP site, and sending the information to the hacker via HTTP POST.

### Proxy functionality

Some Win32/Banker variants drop a malicious configuration script that can redirect your Internet traffic through a hacker-controlled proxy. It does this by setting the following registry entry:

In subkey: *HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings*

Sets value : *"AutoConfigUrl"*

With data: *"<path and file name of script>"*

## AutoStart Technique

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

*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 start-up:

*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 several possibly malicious URL and below are few of them:

* 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

## MITRE ATT&CK

<https://1.bp.blogspot.com/-XIGpCjUkuYw/YB2ip4K_AyI/AAAAAAAAFbA/9yCQZOEK_wcmL2kgUGYgUEkz0lvJiBGIACLcBGAsYHQ/s2020/mitre_attack_18143.png>

# Sample 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
3. 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 to the local directory "C:\G DATA Security Software", and it is digitally signed with a certificate with the name “M2 AGRO DESENVOLVIMENTO DE SISTEMAS LTDA”, signed on March 31, 2019; and it removes software products belonging to AVG, Trusteer Rapport, Avast, and the Bradesco software "scpbrad".

# 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=Win32%2fBanker>
6. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/banload-trojan-targets-brazilians-with-malware-downloads/>
7. <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BANLOAD/>
8. <https://blog.talosintelligence.com/2021/02/threat-roundup-0129-0205.html>
9. <https://www.securityweek.com/hackers-add-security-software-removal-banload-banking-malware?&web_view=true>
10. <https://www.f-secure.com/v-descs/trojan-downloader_w32_banload_fvq.shtml>