Grandoreiro Banking Trojan with New TTPs | Zscaler Blog

By Niraj Shivtarkar

Published: 2022-08-18 · Archived: 2026-04-05 18:27:08 UTC

Introduction

Recently Zscaler ThreatLabz observed a Grandoreiro campaign targeting organizations in the Spanish-speaking nations of Mexico and Spain that work across a variety of different industry verticals such as Automotive, Chemicals Manufacturing and others. In this campaign, the threat actors impersonate government officials from the Attorney General's Office of Mexico City and from the Public Ministry in the form of spear-phishing emails in order to lure victims to download and execute "Grandoreiro" a prolific banking trojan that has been active since at least 2016, and that specifically targets users in Latin America. Grandoreiro is written in Delphi and utilizes techniques like binary padding to inflate binaries, Captcha implementation for sandbox evasion, and command-and-control (CnC) communication using patterns that are identical to LatentBot.

Key Features of this Attack:

- Grandoreiro targets organizations in the Spanish-speaking nations of Mexico and Spain across various industry verticals
- The threat actors in this campaign impersonate Mexican Government Officials
- Multiple anti-analysis techniques are used by Grandoreiro Loader along with implementation of Captcha for evading Sandboxes
- The Grandoreiro Loader sends across a Check-In Request with all the required User, System and Campaign information
- The Grandoreiro uses a binary padding technique to evade sandboxes, adding multiple BMP images to the resource section of the binary and inflating the size to 400+ MB
- The CnC Communication pattern of 2022 Grandoreiro is now completely identical to the LatentBot with "ACTION=HELLO" beacon and ID based communication

In-depth analysis of the Grandoreiro campaign and corresponding Infection chain has been explained below.

Campaign Details:

ThreatLabz has analyzed multiple infection chains for this Grandoreiro campaign, which began in June 2022 and is still ongoing. Based on our analysis, we can infer that the threat actors in this case are **attempting to target organizations in the Spanish-speaking countries of Mexico and Spain**. Industries targeted in this campaign include:

- Chemicals Manufacturing
- Automotive
- Civil and Industrial Construction
- Machinery

- Logistics - Fleet management services

Infection Chain:

The infection chain employed by the threat actors in this campaign is quite similar to previous Grandoreiro campaigns. It begins with a spear-phishing email written in Spanish, targeting victims in Mexico and Spain. The email consists of an embedded link which when clicked redirects the victim to a website that further downloads a malicious ZIP archive on the victim's machine. The ZIP archive is bundled with the Grandoreiro Loader module with a PDF Icon in order to lure the victim into execution; this is responsible for downloading, extracting and executing the final 400MB “Grandoreiro” payload from a Remote HFS server which further communicates with the CnC Server using traffic identical to LatentBot

Let’s dive into the spear-phishing emails received by the victims. The phishing emails are divided into two sets based on the lures used by the threat actors.

Set I - Impersonating Government Officials - Provisional Archiving Resolution:
The first set of phishing emails observed during the campaign were those in which the threat actors impersonated Government officials, instructing the victims to download and share the Provisional Archiving Resolution. Below are the details of the phishing emails:

1.)
Subject (Spanish) : Fiscalia General del Gobierno (RESOLUCIÓN13062022)
Subject (English) : Government Attorney General (RESOLUTION 13062022)

As can be seen in the above screenshot, the threat actors are posing as the current Attorney General of Mexico “Alejandro Gertz Manero” The email subject and the signature are of the Attorney General’s Office “Fiscalia General de Justicia" making the email seem legit. The content in this case notifies the victims about the Provisional Archiving Resolution and asks them to download and share the Resolution before a specified date, after which the payment would not be refunded. If the victim clicks on the embedded link to download the resolution, it redirects to a malicious domain: **http[:]//barusgorlerat[.]me** as shown in the screenshot, and then downloads a ZIP file from the remote server consisting of the Grandoreiro Loader.

2.)
We also came across a similar lure where the threat actors masquerade as “Alejandra Solano - from the Public Ministry - Early Decision and Litigation Section” and ask the Victim to download and share the Provisional Archiving Resolution. In this case, the embedded link redirects to another domain: **http[:]//damacenapirescontab[.]com** as shown in the screenshot below.

Subject (Spanish) :RV [EXTERNAL] Notificación del Ministerio Público - MP08062022 3:59:54 PM
Subject (English) : RV [EXTERNAL] Notification of the Public Ministry - MP08062022 3:59:54 PM

Set II - Cancellation of Mortgage Loan and Deposit Voucher Slip

In this set, there are two types of phishing email lures. The first is regarding the cancellation of a mortgage loan, in which the threat actors ask the victim to download a mortgage cancellation form by opening the embedded link as shown in the below screenshot. Once the link is opened it redirects to the malicious domain: **http[:]//assesorattlas[.]me** which then further downloads a ZIP File consisting of the Grandoreiro Loader.

Subject (Spanish) : Hola agonzaleza Baja del préstamo hipotecario 12:05:38 PM

Subject (English) : Hi Agonz, Low Mortgage Loan 12:05:38 PM

The second one consists of two similar emails targeted towards two different organizations in Mexico. Here, the victim is asked to download a deposit voucher/slip by clicking on the hyperlink. Once the link is opened, it downloads a ZIP File consisting of the Grandoreiro Loader from **http[:]//assesorattlas[.]me** and **http[:]//perfomacepnneu[.]me** as shown in the below screenshot.

Subject (Spanish) : Sr.(a) alfonso.vera Comprobante deposito 05-Jul-22 8:06:09 PM

Subject (English) : Sr. (a) alfonso.vera Proof of deposit 05-Jul-22 8:06:09 PM

Subject (Spanish) : RV Comprobante deposito 28-jun-22 5:11:45 PM

Subject (English) : RV Deposit voucher 28-jun-22 5:11:45 PM

After analyzing all the phishing emails in our dataset, we were able to establish a common pattern between the emails on the basis of similar content to lure the victims, and the pattern of the embedded links (**Pattern: domain.tld/?timestamp),** sometimes seen along with targeted countries (**domain.tld/country/?timestamp**) that were used to download the Grandoreiro Loader from the remote HFS server.

By observing this pattern, we can state that the Grandoreiro campaign might be conducted by a single threat actor across various organizations in Mexico and Spain. The pattern can also be beneficial to track other related campaigns as well.

Once the victim clicks on the embedded link, the user is redirected to download a ZIP File onto the machine from the following different URLs where all the downloaded files drop the Grandoreiro Loader. The file names correspond to the email lures being used:

- 35[.]181[.]59[.]254/info99908hhzzb.zip
- 35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012
- 35[.]181[.]59[.]254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494
- 52[.]67[.]27[.]173/deposito(1110061313).zip
- 54.232.38.61/notificacion(flfit48202).zip
- 54.232.38.61/notificacion(egmux24178).zip

Next, let’s examine the ZIP File named **“informacion16280LIFSD.zip”** which is downloaded from the following

remote server **35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012** once the victim clicks on the embedded link in the Spear phishing email.

The ZIP archive bundles two files:

- A31136.xml
- infonpeuz52271VVCYX.exe

In this case, the first file A31136.xml is not a XML file but a portable executable with the original name "Extensions.dll" and signed with a valid "ASUSTEK COMPUTER INCORPORATION" certificate. It is benign in nature as shown in the screenshot below, and never loaded by the Loader module.

The second file bundled inside the ZIP archive **"infonpeuz52271VVCYX.exe"** is the Grandoreiro Loader module written in Delphi and masking itself with a PDF Icon compiled on 14th June 2022 in order to lure the victims into execution.

When the loader module is executed by the victim, it initially creates a Mutex **"ZTP@11"** by calling CreateMutexA()

Then it loads the "TForm1" Class Object from the resource section "RCData", and the forms in Delphi are defined by the TForm class itself.

Further, the loader module performs the following anti-analysis checks before executing the critical functions.

i) **Detect Analysis Tools:** The malware detects the below mentioned analysis tools by decrypting the tool names using a XOR-based Decryption routine. It then takes a snapshot of currently executing processes in the system using CreateToolhelp32Snapshot() and walks through the process list using Process32First() and Process32Next(). If any of the analysis tools exist, the malware execution is terminated.

Regmon.exe	Filemon.exe	Procmon.exe	Wireshark.exe	Procexp64.exe
Procexp.exe	ProcessHacker.exe	PCHunter64.exe	PCHunter32.exe	JoeTrace.exe

List of Detected Analysis Tools

The second method that the malware uses to detect the analysis tools is to compare the text of the window names with analysis tools (including TCPView and RegShot in this case) by using GetWindowTextW(), FindWindowW, and EnumWindows() APIs.

ii) **Detect Execution Directory:** In this case, the malware checks the directory in which it is being executed. If the below mentioned directory names are used, it terminates itself with a comparison logic in place.

- C:\insidetm
- C:\analysis

iii) **Anti-Debug Technique:** In this case, the Grandoreiro executes the IsDebuggerPresent() to determine whether the current process is being executed in the context of a debugger. If the result is non-zero, the malware terminates

itself as shown below in the screenshot.

iv) **Vmware I/O Port Anti-VM Technique:** In this case, the malware checks whether the execution is occurring in a virtual environment (Vmware) by reading data from the I/O Port "0x5658h" (VX) used by Vmware. It achieves this by setting up the registers.

If, after execution of "in" instruction (executed in order to pull data from the port "VX") the EBX register consists of the magic Number "VMXh" the malware is executed in a virtualized environment and thus further terminates itself.

After completing the anti-analysis checks, the malware decrypts a **URL** by passing an encrypted string to the string decryption routine. The string decryption routine performs XOR-based decryption.

This string decryption routine has been used previously in the older variants of Grandoreiro for decrypting strings and API calls in order to evade detection. The Grandoreiro string decryptor can be found here, developed by the SpiderLabs Team at TrustWave.

The Grandoreiro Loader then sends across a GET Request to the previously decrypted URL: **"http[:]//15[.]188[.]63[.]127/$TIME"** which provides in response the URL to download the next stage.

Next, the malware executes the URLDownloadToFile() API function with the szURL argument as the remote HFS server URL **"http://15[.]188[.]63[.]127:36992/zxeTYhO.xml"** in order to download the Final Payload of the Grandoreiro Banking Trojan

The downloaded Grandoreiro Final Payload is a 9MB ZIP archive that is extracted dynamically, and the bundled executable (disguised as zxeTYhO.png) inside the archive is written in a folder whose name is generated at runtime in the "**C:\ProgramData''** directory. Also the PE file masquerading as "zxeTYhO.png" is renamed to **ASUSTek[random_string].exe,** generated with a random string generation logic, and changes on every execution.

Furthermore, the Stage-1 Grandoreiro module collects the following System and User information where all the strings are decrypted at runtime via the similar String Decryption Function.

i) Username - Retrieves Username via GetUserNameW()

ii) ComputerName - Retrieves Computer name via GetComputerNameW

iii) Operating System and Version - Retrieves the Operating System and its version from the Windows NT\\CurrentVersion and ProductName registry hive.

iv) Antivirus - Retrieves the Antivirus Program installed on the machine via a WMI query

v) Check Installed Programs - In this case the Grandoreiro module checks whether the following programs are installed by accessing the Program Files folder (Path: C:\Program Files\ and C:\Program Files (x86)\ ) or the AppData Folder (Path: C:\Users\\AppData\Local)

Crypto Wallets:

Binance	Electrum	Coinomi	BitBox	OPOLODesk	LedgerLive	Bitcoin Core

Banking, Anti-Malware Programs and Mail Clients:

AppBrad Bradesco	Sicoobnet	Navegador C6 Bank	Aplicativo Itau	Topaz OFD Warsaw	Diebold Warsaw	Outlook

If any of the listed programs are installed on the machine, the malware stores the program names to a list for further usage.

Once all of the above mentioned User and System information has been gathered by the malware, it then decrypts the Check-In URL along with required parameters via the XOR-based String decryption routine used previously and concatenates the parameters with the corresponding gathered information.

After completion of the concatenation, the loader sends across a **POST Check-In Request** to the **Host: "barusgorlerat[.]me** with all the gathered User, System, and Campaign information arranged along with the different parameters.

Once the Check-In request is sent to the remote server, the loader executes the Grandoreiro Final Payload which was downloaded, extracted, and renamed previously.

Grandoreiro - Final Payload:

The Grandoreiro Final Payload written in Delphi was downloaded previously from the remote HFS server **"http://15[.]188[.]63[.]127:36992/zxeTYhO.xml"** as a 9.2 MB ZIP file which is then extracted and executed by the Grandoreiro Loader. The extracted file is a 414MB Portable Executable file disguised with a ".png" extension which is later renamed to ".exe" dynamically by the loader and also the final payload is signed with an **"ASUSTEK DRIVER ASSISTANTE"** digital certificate to appear legitimate and evade detection.

As seen in the older Grandoreiro samples, a similar **"Binary Padding"** technique is used here in order to inflate the file size of the binary to around 400MB by adding two ~200MB Bitmap images in the resource section as shown in the screenshot below. This technique works as an anti-sandbox technique as it helps in evading sandboxes as most of them have a file size limit for execution.

The final payload maintains persistence on the Machine by leveraging the Run Registry key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) which would allow the payload to be executed on startup.

In the following Grandoreiro variant, the Payload writes an .**ini** file (Name: ASUSTekGvaxvh.ini) in the directory

of execution which consists of all the following information as shown in the screenshot. The values in the Configuration file are encrypted using a XOR-based Encryption routine with a key that changes in every sample.

The Command & Control communications have been updated from the 2020 variant. Previously there were *some* similarities between the Grandoreiro and LatentBot communications (as exhibited here), but they were not identical. However, in the latest 2022 sample, the communication pattern has been upgraded by the threat actors and now it is completely identical to LatentBot where the name of the CnC Subdomain is generated via a Domain Generation Algorithm just as the older Grandoreiro variants. The identical LatentBot beacon command "ACTION=HELLO" and the ID-Based communication

Identical to LatentBot, the Command & Control server provides the Cookie value as a response to the "ACTION=HELLO" beacon which is further used as an ID for communication in the latest Grandoreiro sample.

Furthermore, Grandoreiro includes the following backdoor capabilities for espionage purposes:

- **Keylogging**
- **Auto-Updation for newer versions and modules**
- **Web-Injects and restricting access to specific websites**
- **Command execution**
- **Manipulating windows**
- **Guiding the victim's browser to a certain URL**
- **C2 Domain Generation via DGA (Domain Generation Algorithm)**
- **Imitating mouse and keyboard movements**

While finalizing our article, we came across another ongoing Grandoreiro campaign with an extra anti-sandbox technique used by the malware authors. This technique requires a Captcha to be filled manually to execute the malware in the victim's machine. The malware is not executed until or unless the Captcha is filled.

We have analyzed the following malware in our Lab and found that the network communication is similar to the one analyzed in the blog and it also follows "ACTION=HELLO" beacon and ID based communication as inherited from LatentBot.

Zscaler Sandbox Coverage:

Conclusion:

The threat actors behind Grandoreiro Banking malware are continuously evolving their tactics and malware to successfully carry out attacks against their targets by incorporating new anti-analysis tricks to evade security solutions; inheriting features from other Malware families. The Zscaler ThreatLabz team will continue to monitor these attacks to help keep our customers safe

IOCs:

Embedded Domains: (Same used for Check-In Request)

http[:]//barusgorlerat[.]me
http[:]//damacenapirescontab[.]com
http[:]//assesorattlas[.]me
http[:]//perfomacepnneu[.]me

Grandoreiro Loader URLs:

35[.]181[.]59[.]254/info99908hhzzb.zip
35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012
35[.]181[.]59[.]254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494
52[.]67[.]27[.]173/deposito(1110061313).zip
54[.]232[.]38[.]61/notificacion(flfit48202).zip
54[.]232[.]38[.]61/notificacion(egmux24178).zip

Final Grandoreiro Payload URLs with Check-In URL:

15[.]188[.]63[.]127/$TIME
167[.]114[.]137[.]244/$TIME
15[.]188[.]63[.]127:36992/zxeTYhO.xml
15[.]188[.]63[.]127:36992/vvOGniGH.xml
15[.]188[.]63[.]127[:]36992/eszOscat.xml
15[.]188[.]63[.]127:36992/YSRYIRIb.xml
167[.]114[.]137[.]244:48514/eyGbtR.xml
barusgorlerat[.]me/MX/
assesorattlas[.]me/MX/
assesorattlas[.]me/AR/
atlasassessorcontabilidade[.]com/BRAZIL/
vamosparaonde[.]com/segundona/
mantersaols[.]com/MEX/MX/
premiercombate[.]eastus.cloudapp.azure.com/PUMA/

Grandoreiro CnC:

Pcbbcrjcgbcghjpbcgkccbjorkhhjcjj[.]fantasyleague[.]cc -> fantasyleague[.]cc
jmllmedvhgmhldjgmhvmmlljhvgdzvzz[.]dynns[.]com
ciscofreak[.]com
chjjhjmomaoheoojjbynnyjiidfcncc.cable-modem.org -> cable-modem.org
odbbdbmgmagdfggbbnynnyjiidfcncc.blogsyte.com -> blogsyte.com
ifnnfnmcmacfdccnnjynnyjiidfcncc.collegefan.org -> collegefan.org

MD5 Hashes:

Grandoreiro Loader:
970f00d7383e44538cac7f6d38c23530
724f26179624dbb9918609476ec0fce4

2ec2d539acfe23107a19d731a330f61c
6433f9af678fcd387983d7afafae2af2
56416fa0e5137d71af7524cf4e7f878d
7ea19ad38940ddb3e47c50e622de2aae

Grandoreiro Final Payload:

e02c77ecaf1ec058d23d2a9805931bf8
6ab9b317178e4b2b20710de96e8b36a0
5b7cbc023390547cd4e38a6ecff5d735
531ac581ae74c0d2d59c22252aaac499

Explore more Zscaler blogs

Source: https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals