

Grandoreiro, the global trojan with grandiose goals

By GReAT

Published: 2024-10-22 · Archived: 2026-04-05 18:16:20 UTC

Grandoreiro is a well-known Brazilian banking trojan — part of the [Tetrade](#) umbrella — that enables threat actors to perform fraudulent banking operations by using the victim's computer to bypass the security measures of banking institutions. It's been active since at least 2016 and is now one of the most widespread banking trojans globally.

INTERPOL and law enforcement agencies across the globe are fighting against Grandoreiro, and Kaspersky is cooperating with them, sharing TTPs and IoCs. However, despite the disruption of some local operators of this trojan in [2021](#) and [2024](#), and the arrest of gang members in Spain, Brazil, and [Argentina](#), they're still active. We now know for sure that only part of this gang was arrested: the remaining operators behind Grandoreiro continue attacking users all over the world, further developing new malware and establishing new infrastructure.

Every year we observe new Grandoreiro campaigns targeting financial entities, using new tricks in samples with low detection rates by security solutions. The group has evolved over the years, expanding the number of targets in every new campaign we tracked. In 2023, the banking trojan targeted 900 banks in 40 countries — in 2024, the newest versions of the trojan targeted **1,700 banks and 276 crypto wallets in 45 countries and territories**, located on all continents of the world. Asia and Africa have finally joined the list of its targets, making it a truly global financial threat. In Spain alone, Grandoreiro has been responsible for fraudulent activities amounting to 3.5 million euros in profits, according to conservative estimates — several failed attempts could have yielded beyond 110 million euros for the criminal organization.

In this article, we will detail how Grandoreiro operates, its evolution over time, and the new tricks adopted by the malware, such as the usage of 3 DGAs (domain generation algorithm) in its C2 communications, the adoption of ciphertext stealing encryption (CTS), and mouse behavior tracking, aiming to bypass anti-fraud solutions. This evolution culminates with the appearance of lighter, local versions, now focused on Mexico, positioning the group as a challenge for the financial sector, law enforcement agencies and security solutions worldwide.

Grandoreiro: One malware, many operators, fragmented versions

Grandoreiro is a banking trojan of Brazilian origin that has been active since at least 2016. Grandoreiro is written in the Delphi programming language, and there are many versions, indicating that different operators are involved in developing the malware.

Since 2016, we have seen the threat actors behind Grandoreiro operations regularly improving their techniques to stay unmonitored and active for a longer time. In 2020, Grandoreiro started to expand its attacks in Latin America and later in Europe with great success, focusing its efforts on evading detection using modular installers.

Grandoreiro generally operates as Malware-as-a-Service, although it's slightly different from other banking trojan families. You won't find an announcement on underground forums selling the Grandoreiro package — it seems that access to the source-code or builders of the trojan is very limited, only for trusted partners.

After the arrests of some operators, Grandoreiro split its codebase into lighter versions, with fewer targets. These fragmented versions of the trojan are a reaction to the recent law enforcement operations. This discovery is supported by the existence of two distinct codebases in simultaneous campaigns: newer samples featuring updated code, and older samples which rely on the legacy codebase, now targeting only users in Mexico — customers of around 30 banks.

2022 and 2023 campaigns

Grandoreiro campaigns commonly start with a phishing email written in the target country language. For example, the emails distributed in most of Latin America are in Spanish. However, we also saw the use of Google Ads (malvertising) in some Grandoreiro campaigns to drive users to download the initial stage of infection.

Phishing emails use different lures to make the victim interact with the message and download the malware. Some messages refer to a pending phone bill, others mimic a tax notification, and so on. In early 2022 campaigns, the malicious email included an attached PDF. As soon as the PDF is opened, the victim is prompted with a blurred image except for a part containing “*Visualizar Documento*” (“View Document” in Spanish). When the victim clicks the button, they are redirected to a malicious web page which prompts them to download a ZIP file. Since May 2022, Grandoreiro campaigns include a malicious link inside the email body that redirects the victim to a website that then downloads a malicious ZIP archive on the victim’s machine. These ZIP archives commonly contain two files: a legitimate file and a Grandoreiro loader, which is responsible for downloading, extracting and executing the final Grandoreiro payload.

The Grandoreiro loader is delivered in the form of a Windows Installer (MSI) file that extracts a dynamic link library (DLL) file and executes a function embedded in the DLL. The function will do nothing if the system language is English, but otherwise the final payload is downloaded. Most likely, this means that the analyzed versions didn’t target English-speaking countries. There have also been other cases where a VBS file is used instead of the DLL to execute the final payload.

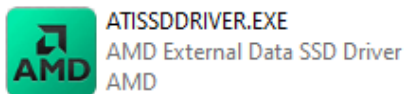


Grandoreiro recent infection flow

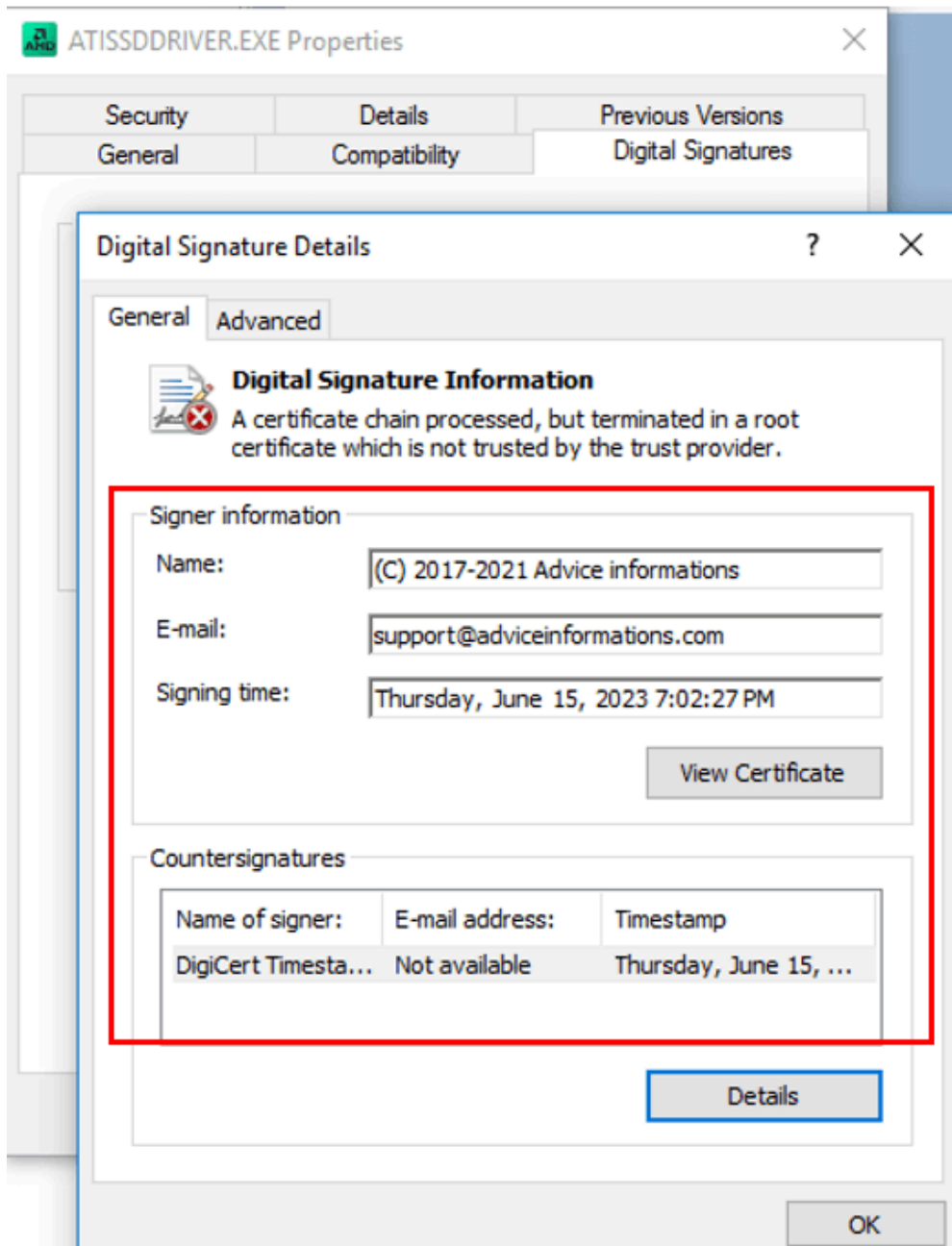
As for the malware itself, in August 2022 campaigns, the final payload was an incredibly big 414 MB portable executable file disguised with a PNG extension (which is later renamed to EXE dynamically by the loader). It masked itself as an ASUS driver using the ASUS icon and was signed with an “ASUSTEK DRIVER ASSISTANTE” digital certificate.

In 2023 campaigns, Grandoreiro used samples with rather low detection rates. Initially, we identified three samples related to these campaigns, compiled in June 2023. All of them were portable executables, 390 MB big, with the original name “[ATISSDDRIVER.EXE](#)” and internal name “ATIECLXX.EXE”. The main purpose of these samples is to monitor the victims’ visits to financial institution websites and steal their credentials. The malware also allows threat actors to remotely control the victim machines and perform fraudulent transactions within them.

In the campaign involving the discussed samples, the malware tries to impersonate an AMD External Data SSD driver and is signed with an “*Advice informations*” digital certificate in order to appear legitimate and evade detection.



Implant impersonating AMD driver

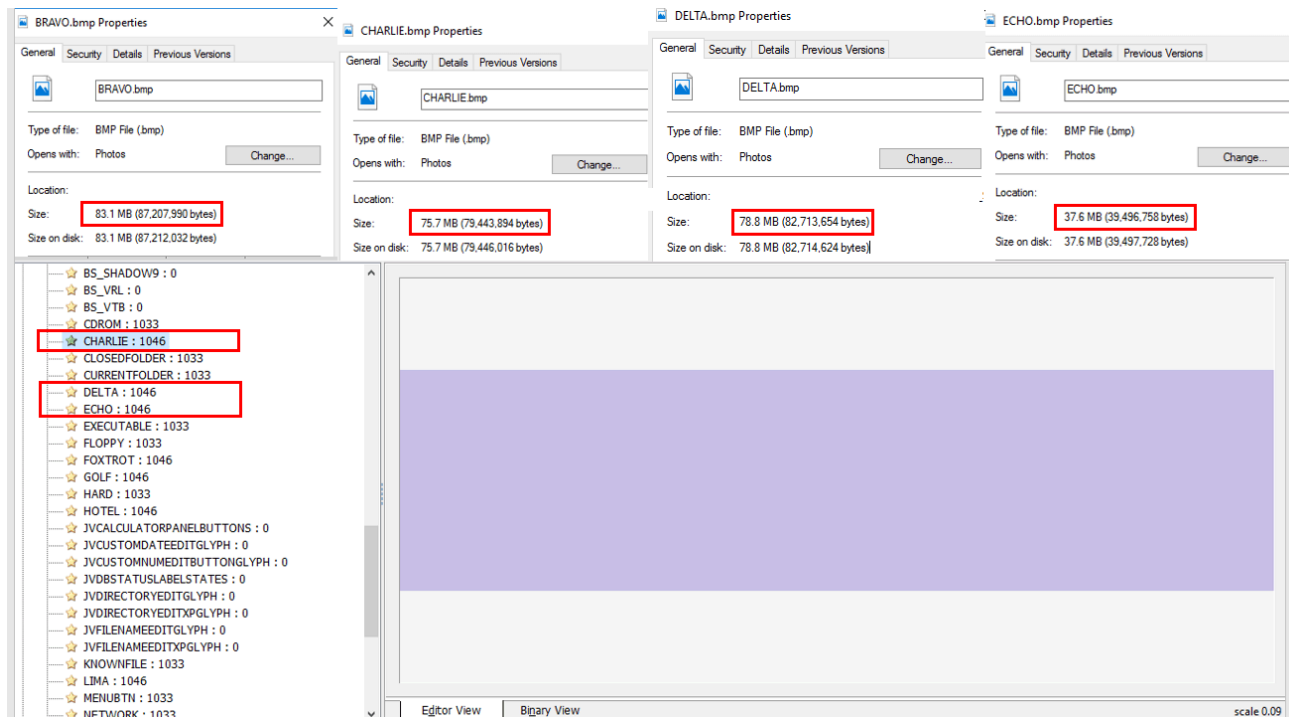


Digital certificate used by Grandoreiro malware

In both cases, the malware is an executable that registers itself to be launched with Windows. However, it is worth noting that in the majority of Grandoreiro attacks, a DLL sideloading technique is employed, using legitimate binaries that are digitally signed to run the malware.

The considerable size of the executables can be explained by the fact that Grandoreiro utilizes a [binary padding technique](#) to inflate the size of the malicious files as a way to evade sandboxes. To achieve this, the attackers add multiple BMP

images to the resource section of the binary. In the example below, the sample included several big images. The sizes of the highlighted images are around 83.1 MB, 78.8 MB, 75.7 and 37.6 MB. However, there are more of them in the binary, and together all the images add ~376 MB to the file.



Binary padding used by Grandoreiro

In both 2022 and 2023 campaigns, Grandoreiro used a well-known XOR-based string encryption algorithm that is shared with other Brazilian malware families. The difference is the encryption key. For Grandoreiro, some magic values were the following:

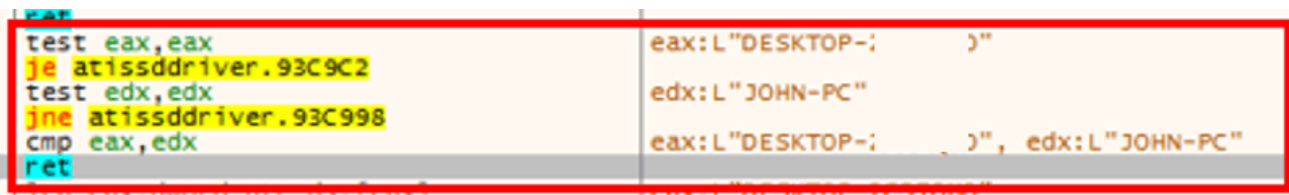
Date	Encryption key
March 2022	F5454DNBVCCEFD3EFMNBVDCMNXCEVD3CMBKJHGFM
March 2022	XD3CMBKJCEFD3EFMF5454NBVDNBVXCCMNXCEVDHGFM
August 2022	BVCKLMBNUIOJKDOSOKOMOI5M4OKYMKLFODIO
June 2023	B00X02039AVBJICXNBJOIKCVXMKOMASUJIERNJIQWNLKFMDOPVXCMUIJBNOXCKMVIOKXCJ UIHNSDIUJNRHUQWEBGYTVasuydhosgkjopdf

The various checks and validations aimed at avoiding detection and complicating malware analysis were also changed in the 2022 and 2023 versions. In contrast with the older Grandoreiro campaigns, we found that some of the tasks that were previously executed by the final payload are now implemented in the first stage loader. These tasks include security checks, anti-debugging techniques, and more. This represents a significant change from previous campaigns.

One of these tasks is the use of the geolocation service <http://ip-api.com/json> to gather the target's IP address location data. In a campaign reported in May 2023 by [Trustwave](#), this task is performed by a JScript code embedded in an MSI installer before the delivery of the final payload.

There are numerous other checks that have been transferred into the loader, although some of them are still present in the banking trojan itself. Grandoreiro gathers host information such as operating system version, hostname, display monitor information, keyboard layout, current time and date, time zone, default language and mouse type. Then the malware retrieves the computer name and compares it against the following strings that correspond to known sandboxes:

- WIN-VUA6POUV5UP;
- Win-StephyPC3;
- difusor;
- DESTOP2457;
- JOHN-PC.



```
test eax,eax
je atissddriver.93C9C2
test edx,edx
jne atissddriver.93C998
cmp eax,edx
ret
```

eax:L"DESKTOP-;)"
edx:L"JOHN-PC"
eax:L"DESKTOP-;)", edx:L"JOHN-PC"

Computer name validation

It also collects the username and verifies if it matches with the “John” or “WORK” strings. If any of these validations match, the malware stops its execution.

Grandoreiro includes detection of tools commonly used by security analysts, such as regmon.exe, procmon.exe, Wireshark, and so on. The process list varies across the malware versions, and it was significantly expanded in 2024, so we’ll share the full list later in this post. The malware takes a snapshot of currently executing processes in the system using the *CreateToolhelp32Snapshot()* Windows API and goes through the process list using *Process32FirstW()* and *Process32NextW()*. If any of the analysis tools exists in the system, the malware execution is terminated.

Grandoreiro also checks the directory in which it is being executed. If the execution paths are *D:\programming* or *D:\script*, it terminates itself.

Another anti-debugging technique implemented in the trojan involves checking for the presence of a virtual environment by reading data from the I/O Port “0x5658h” (VX) and looking for the VMWare magic number *0x564D5868*. The malware also uses the *IsDebuggerPresent()* function to determine whether the current process is being executed in the context of a debugger.

Last but not least, Grandoreiro searches for anti-malware solutions such as AVAST, Bitdefender, Nod32, Kaspersky, McAfee, Windows Defender, Sophos, Virus Free, Adaware, Symantec, Tencent, Avira, ActiveScan and CrowdStrike. It also looks for banking security software, such as [Topaz OFD](#) and Trusteer.

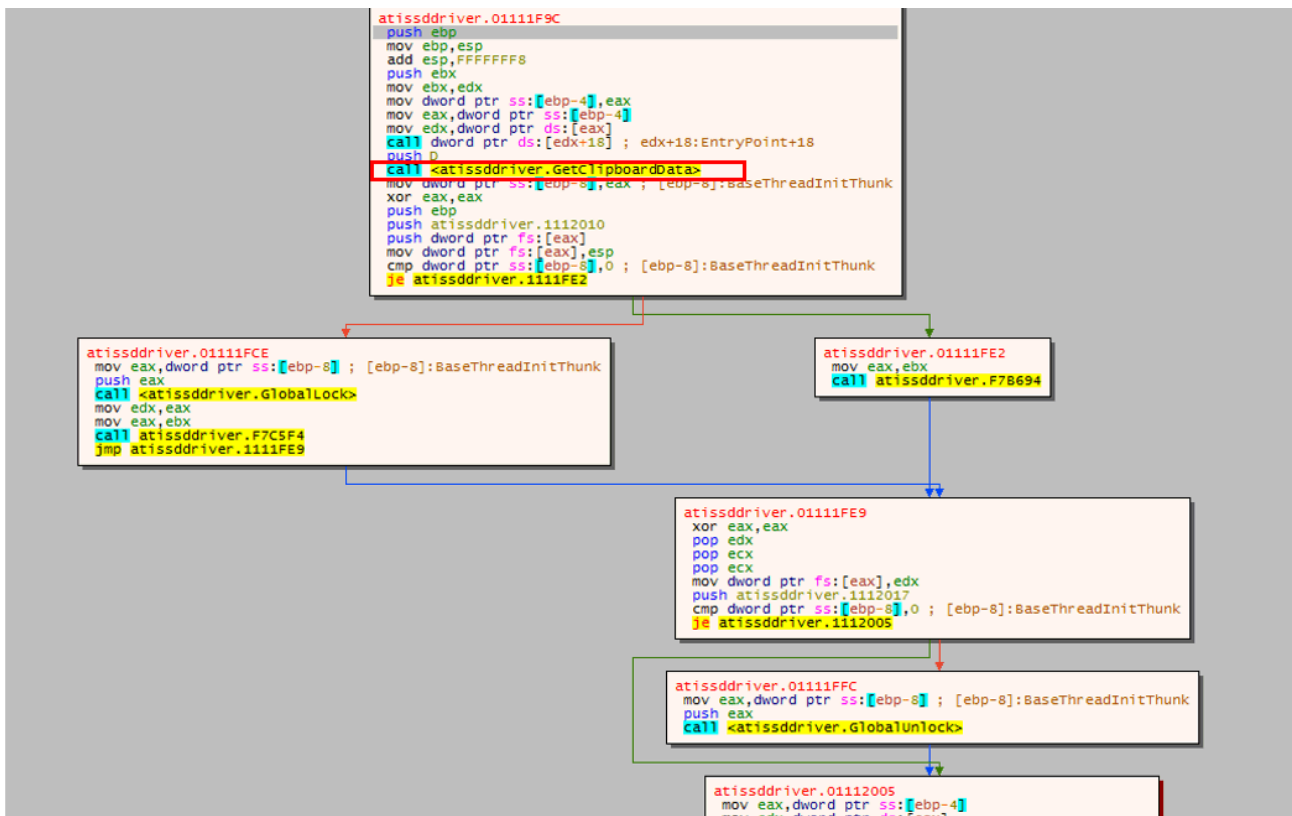
In terms of the core functionality, some Grandoreiro samples check whether the following programs are installed:

- CHROME.EXE;
- MSEDGE.EXE;
- FIREFOX.EXE;

- IEXPLORE.EXE;
- OUTLOOK.EXE;
- OPERA.EXE;
- BRAVE.EXE;
- CHROMIUM.EXE;
- AVASTBROWSER.EXE;
- VeraCrypt;
- Nortonvpn;
- Adobe;
- OneDrive;
- Dropbox.

If any of these is present on the system, the malware stores their names to further monitor user activity in them.

Grandoreiro also checks for crypto wallets installed on the infected machine. The malware includes a clipboard replacer for crypto wallets, monitoring the user’s clipboard activity and replacing the clipboard data with the threat actor keys.



Clipboard replacer

2024 campaigns

During a certain period of time in February 2024, a few days after the announcement of the arrest of some of the gang’s operators in Brazil, we observed a significant increase in emails detected by spam traps. There was a notable prevalence of Grandoreiro-themed messages masquerading as Mexican CFDI communications. Mexican CFDI, short for “Comprobante Fiscal Digital por Internet” is an electronic invoicing system administered by the Mexican Tax Authority

(SAT — Servicio de Administración Tributaria). It facilitates the creation, transmission, and storage of digital tax documents, mandatory for businesses in Mexico to record transactions for tax purposes.

In our investigation, we have acquired 48 samples associated not only with this instance but also with various other campaigns.

Notably, this new campaign added a new sandbox detection mechanism, namely a CAPTCHA before the execution of the main payload, as a way to avoid the automatic analysis used by some companies:



Grandoreiro anti-sandbox CAPTCHA

It is worth noting that in the 2024 Grandoreiro campaigns, the new sandbox evasion code has been implemented in the downloader. Although the main sample still has anti-sandbox functionality too, if a sandbox is detected, it is simply not downloaded. Besides that, the new version also added detection of many tools to its arsenal, aiming to avoid analysis. Here is whole list of analysis tools detected by the newest versions:

regmon.exe	hopper.exe	nessusd.exe	OmniPeek.exe
procmon.exe	jd-gui.exe	PacketSled.exe	netmon.exe
filemon.exe	canvas.exe	prtg.exe	colasoft.exe
Wireshark.exe	pebrowsepro.exe	cain.exe	netwitness.exe
ProcessHacker.exe	gdb.exe	NetworkAnalyzerPro.exe	netscanpro.exe
PCHunter64.exe	scylla.exe	OmniPeek.exe	packetanalyzer.exe

PCHunter32.exe	volatility.exe	netmon.exe	packettotal.exe
JoeTrace.exe	cffexplorer.exe	colasoft.exe	tshark.exe
ollydbg.exe	angr.exe	netwitness.exe	windump.exe
ida.exe	pestudio.exe	netscanpro.exe	PRTG Probe.exe
x64dbg.exe	die.exe	packetanalyzer.exe	NetFlowAnalyzer.exe
cheatengine.exe	ethereal.exe	packettotal.exe	SWJobEngineWorker2x64.exe
ollyice.exe	Capsa.exe	tshark.exe	NetPerfMonService.exe
fiddler.exe	tcpdump.exe	windump.exe	SolarWinds.DataProcessor.exe
devenv.exe	NetworkMiner.exe	PRTG Probe.exe	ettercap.exe
radare2.exe	smartsniff.exe	NetFlowAnalyzer.exe	apimonitor.exe
ghidra.exe	snort.exe	SWJobEngineWorker2x64.exe	apimonitor-x64.exe
frida.exe	pcap.exe	NetPerfMonService.exe	apimonitor-x32.exe
binaryninja.exe	SolarWinds.NetPerfMon.exe	SolarWinds.DataProcessor.exe	x32dbg.exe
cutter.exe	nmap.exe	ettercap.exe	x64dbg.exe
scylla.exe	apimonitor.exe	PCHunter64.exe	x96dbg.exe
volatility.exe	apimonitor-x64.exe	PCHunter32.exe	fakenet.exe
cffexplorer.exe	apimonitor-x32.exe	JoeTrace.exe	hexworkshop.exe
angr.exe	x32dbg.exe	ollydbg.exe	Dbgview.exe
pestudio.exe	x64dbg.exe	ida.exe	sysexp.exe
die.exe	x96dbg.exe	x64dbg.exe	vmtoolsd.exe
ethereal.exe	fakenet.exe	cheatengine.exe	dotPeek.exe
Capsa.exe	hexworkshop.exe	ollyice.exe	procexp64.exe
tcpdump.exe	Dbgview.exe	fiddler.exe	procexp64a.exe
NetworkMiner.exe	sysexp.exe	devenv.exe	procexp.exe
smartsniff.exe	vmtoolsd.exe	radare2.exe	cheatengine.exe
snort.exe	dotPeek.exe	ghidra.exe	ollyice.exe
pcap.exe	procexp64.exe	frida.exe	pebrowsepro.exe
cain.exe	procexp64a.exe	binaryninja.exe	gdb.exe

nmap.exe	procexp.exe	cutter.exe	Wireshark.exe
nessusd.exe	regmon.exe	hopper.exe	ProcessHacker.exe
PacketSled.exe	procmon.exe	jd-gui.exe	SolarWinds.NetPerfMon.exe
prtg.exe	filemon.exe	canvas.exe	NetworkAnalyzerPro.exe

These are some RAT features that we found in this version:

- Auto-update feature allows newer versions of the malware to be deployed to the victim’s machine;
- Sandbox/AV detection, still present in the main module, which includes more tools than previous versions;
- Keylogger feature;
- Ability to select country for listing victims;
- Banking security solutions detection;
- Checking geolocation information to ensure it runs in the target country;
- Monitoring Outlook emails for specific keywords;
- Ability to use Outlook to send spam emails.

In terms of static analysis protection, in 2024 versions, Grandoreiro has implemented enhanced encryption measures. Departing from its previous reliance on commonly shared encryption algorithms found in other malware, Grandoreiro has now adopted a multi-layered encryption approach. The decryption process in the newer versions is the following. Initially, the string undergoes deobfuscation through a simple replacement algorithm. Following this, Grandoreiro employs the encryption algorithm based on XOR and conditional subtraction typically utilized by Brazilian malware; however, it differs from them by incorporating a lengthy, 140759-byte string instead of smaller magic strings we saw in 2022 and 2023 samples. Subsequently, the decrypted string undergoes base64 decoding before being subjected to decryption via the AES-256 algorithm. Notably, the AES key and IV are encrypted within Grandoreiro’s code. Upon completion of all these steps, the decrypted string is successfully recovered.

```

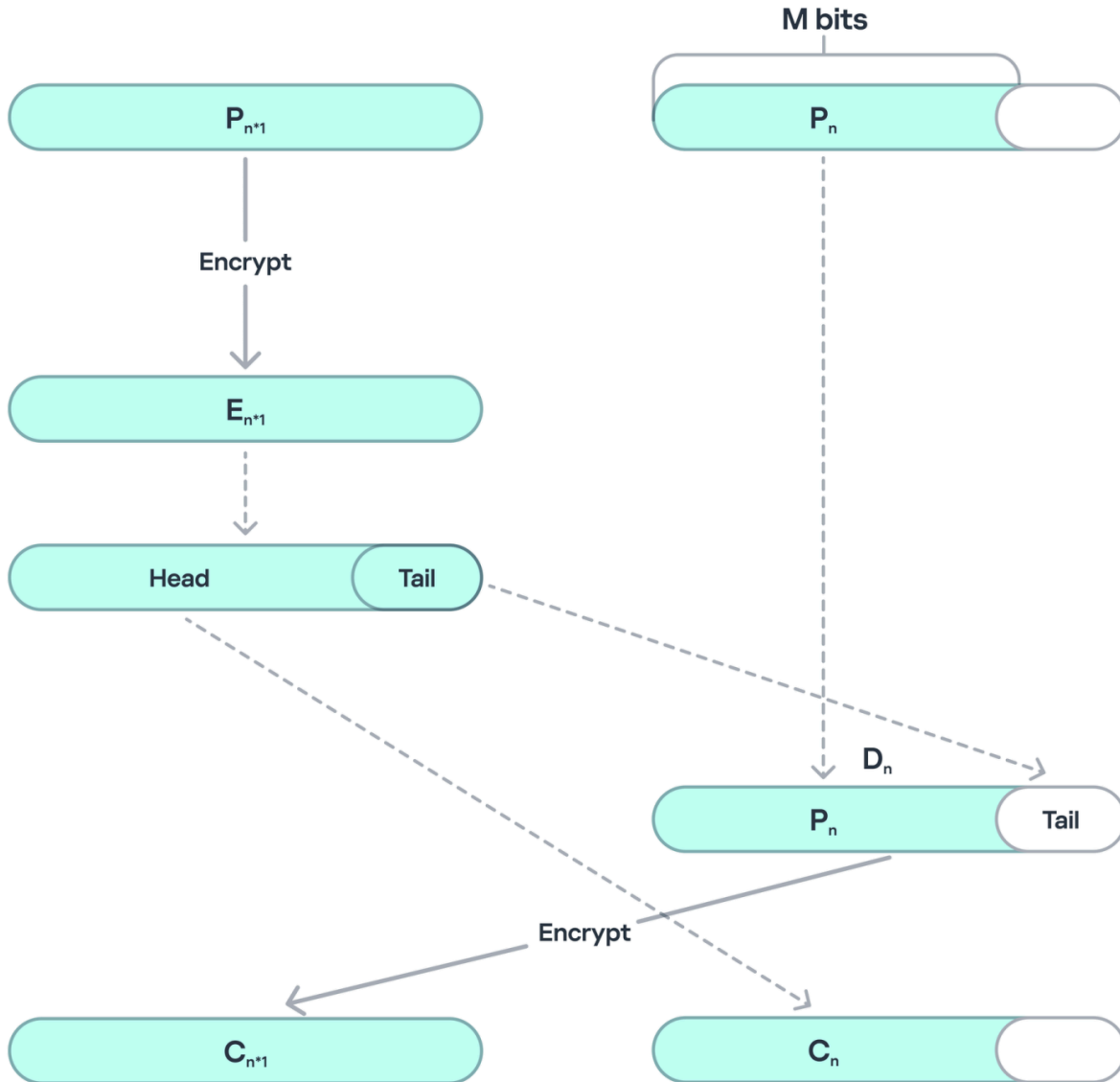
mov     eax, 1
call   GetEncryptedString
mov     ecx, dword ptr [ebp+hCrypto+4]
xor     edx, edx
xor     eax, eax
call   DecryptStr      0D05E92D4901D4F4D637CC56D8449836 - AES KEY
mov     edx, dword ptr [ebp+hCrypto+4]
lea     eax, [ebp+var_10]
mov     ecx, 0
call   System_@LStrFromUStr
lea     eax, [ebp+hCrypto]
push   eax             ; hCrypto
lea     edx, [ebp+var_5C]
mov     eax, 2
call   GetEncryptedString
mov     ecx, [ebp+var_5C]
xor     edx, edx
xor     eax, eax
call   DecryptStr      60D43123100873EB070779F956DF4FD078 -> decrypted = 038989CD7BB390E4 - AES IV

```

Grandoreiro AES key and IV

In newer samples, Grandoreiro upgraded yet again the encryption algorithm using AES with CTS, or [Ciphertext Stealing](#), a specialized encryption mode used when the plaintext is not a multiple of the block size, which in this case is the 128-bit (16-byte) block size used by AES. Unlike more common padding schemes, such as PKCS#7, where the final block is

padding with extra bytes to ensure it fits a full block, CTS operates without padding. Instead, it manipulates the final partial block of data by encrypting the last full block and XORing its output with the partial block. This allows encryption of any arbitrary-length input without adding extra padding bytes, preserving the original size of the data.



ECB Encryption Steps for CTS

In the case of Grandoreiro, the malware's encryption routine does not add standard padding to incomplete blocks of data. Their main goal is to complicate analysis: it takes time to figure out that CTS was used, and then more time to implement decryption in this mode, which makes the extraction and obfuscation of strings more complicated. This marks the first time this particular method has been observed in a malware sample.

As the threat actors continue to evolve their techniques, changing the encryption in every iteration of the malware, the use of CTS in malware may signal a shift toward more advanced encryption practices.

Local versions: old meets new

In a recent campaign, our analysis has revealed the existence of an older variant of the malware that utilizes legacy encryption keys, outdated algorithms, and a simplified structure, but which runs in parallel to the campaign using the new code. This variant targets fewer banks — about 30 financial institutions, mainly from Mexico. This analysis clearly indicates that another developer, likely with access to older source code, is conducting new campaigns using the legacy version of the malware.

How they steal your money

Operators behind Grandoreiro are equipped with a wide variety of remote commands, including an option to lock the user screen and present a custom image (overlay) to ask the victim for extra information. These are usually OTPs (one-time passwords), transaction passwords or tokens received by SMS, sent by financial institutions.

A new tactic that we have discovered in the most recent versions found in July 2024 and later suggests that the malware is capturing user input patterns, particularly **mouse movements**, to bypass machine learning-based security systems. Two specific strings found in the malware — “GRAVAR_POR_5S_VELOCIDADE_MOUSE_CLIENETE_MEDIA” (“Record for 5 seconds the client’s average mouse speed”) and “Medição iniciada, aguarde 5 segundos!” (“Measurement started, please wait 5 seconds!”) — indicate that Grandoreiro is monitoring and recording the user’s mouse activity over a short period. This behavior appears to be an attempt to mimic legitimate user interactions in order to evade detection by anti-fraud systems and security solutions that rely on behavioral analytics. Modern cybersecurity tools, especially those powered by machine learning algorithms, analyze user’s behavior to distinguish between human users and bots or automated malware scripts. By capturing and possibly replaying these natural mouse movement patterns, Grandoreiro could trick these systems into identifying the activity as legitimate, thus bypassing certain security controls.

This discovery highlights the continuous evolution of malware like Grandoreiro, where attackers are increasingly incorporating tactics designed to counter modern security solutions that rely on behavioral biometrics and machine learning.

To perform the cash-out in the victim’s account, Grandoreiro operators’ options are to transfer money to the account of local money mules, using transfer apps, buy cryptocurrency or gift cards, or even going to an ATM. Usually, they search for money mules in Telegram channels, paying \$200 to \$500 USD per day:

PROCURO QUEM TEM

1º PRECISO DE PESSOAS QUE TENHA O APP DA [REDACTED] COM HISTÓRICO DE MOVIMENTAÇÕES EM USD ou EURO

2º CASO VOCÊ TENHA, E QUEIRA GANHAR UMA RENDA EXTRA, ME CHAME INBOX!

3º NÃO PRECISA INVESTIR NADA!
NÃO PRECISA TER NENHUM SALDO!
NÃO QUERO ACESSO DE NADA OK!

CHAME INBOX!

Você que faz a utilização do [REDACTED] e gostaria de ganhar extra de 200\$ a 500\$ Dólares no dia me chame Dinheiro na hora sem investimento totalmente Gratuito e seguro ✓

📢 + Informações me chama no particular , início imediato! 🏃☁️

4:32 AM

Grandoreiro operator looking for money mules

Infrastructure

The newest Grandoreiro version uses 3 Domain Generation Algorithms (DGAs), generating valid domains for command and control (C2) communications. The algorithm uses the current daytime to select strings of predefined lists and concatenates them with a magic key to create the final domain.

By dynamically generating unique domain names based on various input data, the algorithm complicates traditional domain-based blocking strategies. This adaptability allows the malicious actors to maintain persistent command-and-control communications, even when specific domains are identified and blacklisted, requiring security solutions to base their protection not on a fixed list of domains, but on an algorithm for generating them.

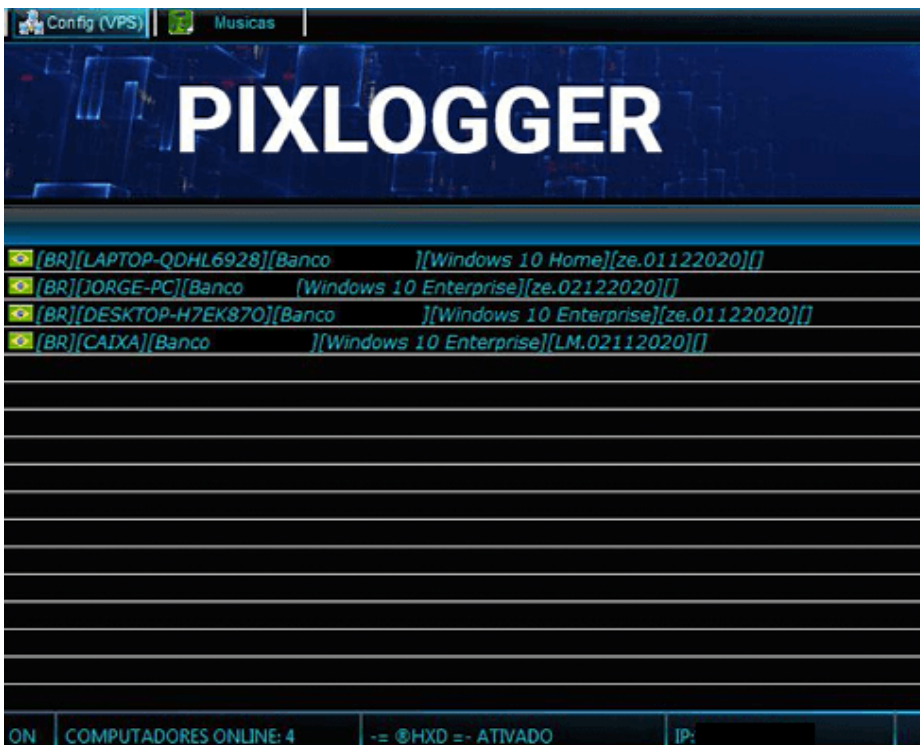
Since early 2022, Grandoreiro leverages a known Delphi component shared among different malware families named RealThinClient SDK to remotely access victim machines and perform fraudulent actions. This SDK is a flexible and modular framework for building reliable and scalable Windows HTTP/HTTPS applications with Delphi. By using RealThinClient SDK, the program can handle thousands of active connections in an efficient multithreaded manner.

```
POST http://[REDACTED]/Srdgate?ACTION=HELLO&ID=NEW
POST http://[REDACTED]/Srdgate?ACTION=START&ID=B5B722DEF44848B3B4E1996792159F80
POST http://[REDACTED]/Srdgate?ID=B5B722DEF44848B3B4E1996792159F80
POST http://[REDACTED]/Srdgate?ID=B5B722DEF44848B3B4E1996792159F80
```

Grandoreiro C2 Communication

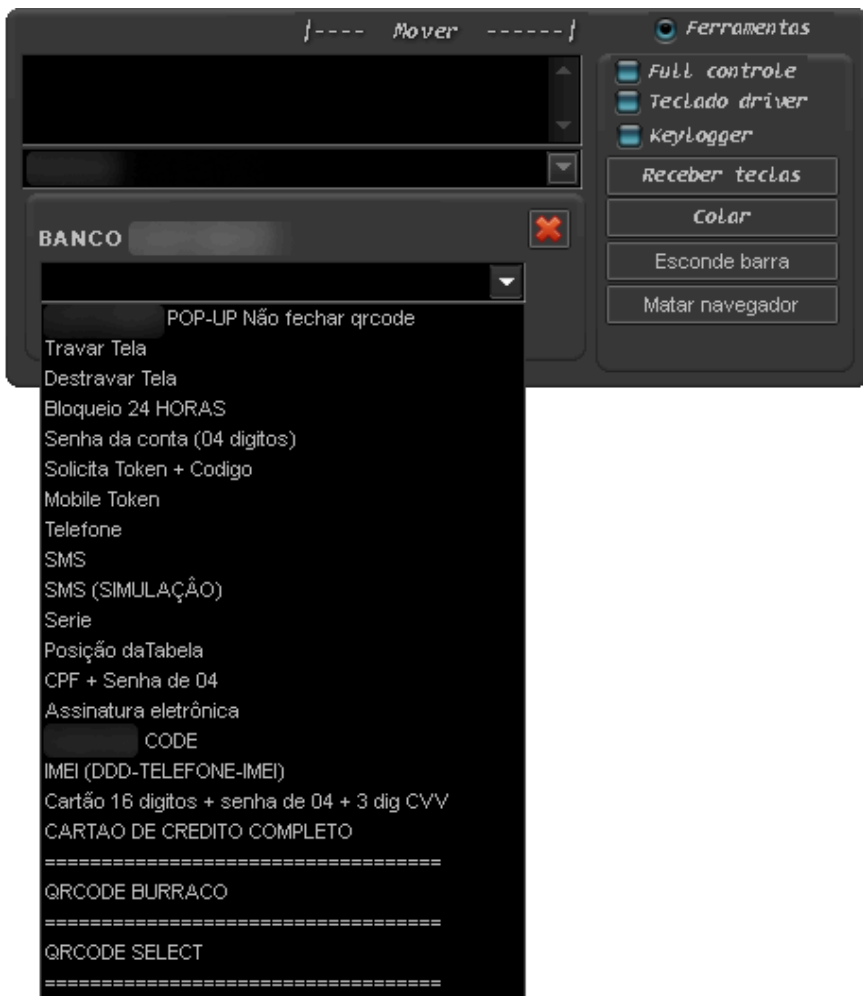
Operator tool

Grandoreiro’s Operator is the tool that allows the cybercriminal to remotely access and control the victim’s machine. It’s a Delphi-based software that lists its victims whenever they start browsing a targeted financial institution website.



Grandoreiro’s Operator tool

Once the cybercriminal chooses a victim to operate on, they will be presented with the following screen, seen in the image below, which allows many commands to be executed and visualizes the victim’s desktop.



Grandoreiro’s Operator commands

Cloud VPS

One overlooked feature of the Grandoreiro malware is what is called “Cloud VPS” by the attackers — it allows cybercriminals to set up a gateway computer between the victim’s machine and the malware operator, thus hiding the cybercriminal’s real IP address.

This is also used by them to make investigation harder, as the first thing noted is the gateway’s IP address. When requesting a seizure, an investigator just finds the gateway module. Meanwhile, the criminal has already set up a new gateway somewhere else and new victims connect to the new one through its DGA.



Grandoreiro Cloud VPS

Victims and targets

The Grandoreiro banking trojan is primed to steal the credentials accounts for 1,700 financial institutions, located in 45 countries and territories. After decrypting the strings of the malware, we can see the targeted banks listed separated by countries/territories. This doesn't mean that Grandoreiro will target a specific bank from the list; it means it is ready to steal credentials and act, if there is a local partner or money mule who can operationalize and complete the action. The banks targeted by Grandoreiro are located in Algeria, Angola, Antigua and Barbuda, Argentina, Australia, Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cayman Islands, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, Ethiopia, France, Ghana, Haiti, Honduras, India, Ivory Coast, Kenya, Malta, Mexico, Mozambique, New Zealand, Nigeria, Panama, Paraguay, Peru, Philippines, Poland, Portugal, South Africa, Spain, Switzerland, Tanzania, Uganda, United Kingdom, Uruguay, USA, and Venezuela. It's important to note that the list of targeted banks and institutions tend to slightly change from one version to another.

From January to October 2024, our solutions blocked more than 150,000 infections impacting more than 30,000 users worldwide, a clear sign the group is still very active. According to our telemetry, the countries most affected by Grandoreiro infections are Mexico, Brazil, Spain, and Argentina, among many others.

Conclusion

We understand how difficult it is to eradicate a malware family, but it is possible to impede their operation with the cooperation of law enforcement agencies and the private sector — modern financial cybercrime can and must be fought.

Brazilian banking trojans are already an international threat; they're filling the gaps left by Eastern European gangs who have migrated into ransomware. We know that in some countries, internet banking is declining on desktops, forcing Grandoreiro to target companies and government entities who are still using operating in that way.

The threat actors behind the Grandoreiro banking malware are continuously evolving their tactics and malware to successfully carry out attacks against their targets and evade security solutions. Kaspersky continues to cooperate with INTERPOL and other agencies around the world to fight the Grandoreiro threat among internet banking users.

This threat is detected by Kaspersky products as **HEUR:Trojan-Banker.Win32.Grandoreiro**, **Trojan-Downloader.OLE2.Grandoreiro**, **Trojan.PDF.Grandoreiro** and **Trojan-Downloader.Win32.Grandoreiro**.

For more information, please contact: crimewareintel@kaspersky.com

Indicators of Compromise

Host based

[f0243296c6988a3bce24f95035ab4885dd2ea25752751c8fb44da2b23daf24a4555856076fad10b2c0c155161fb9384b49355fd0d152862e9c8e3ca3bbc55eb043eec7f0fecf58c71a9446f56def0240150de04cb34fdc5fd131e342fe4df638b979d79be32d99824ee31a43deccdb18](#)

Source: <https://securelist.com/grandoreiro-banking-trojan/114257/>