Bizarro banking Trojan expands its attacks to Europe

By GReAT

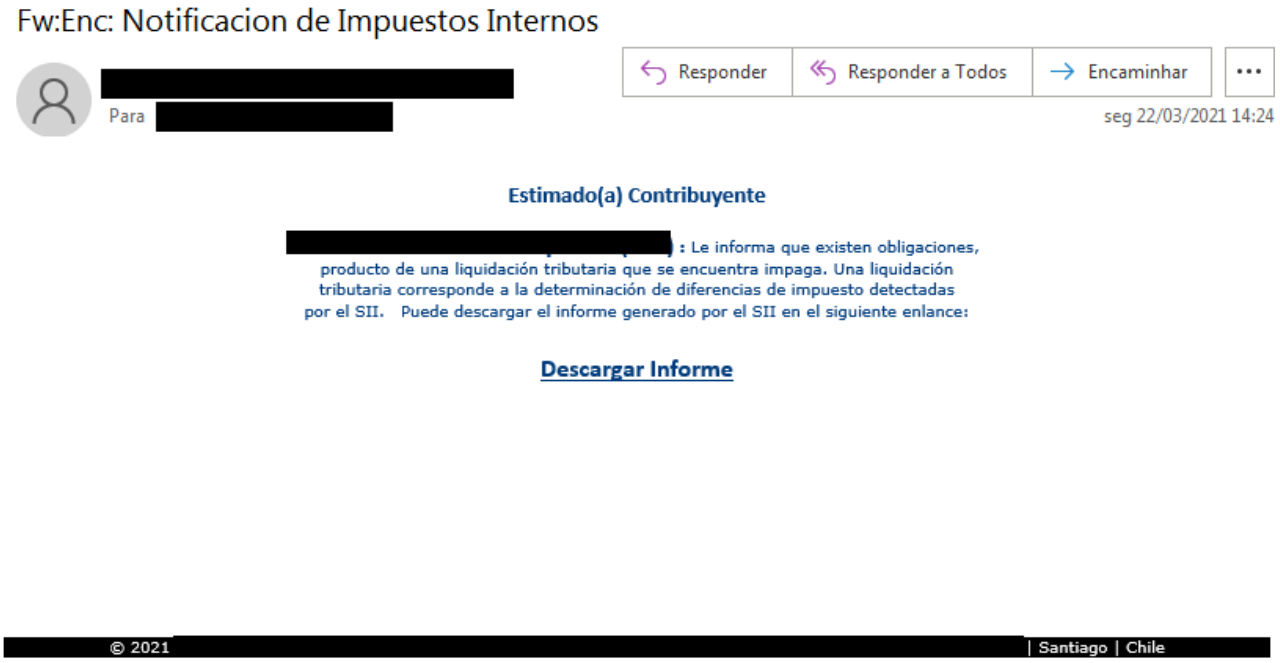
Published: 2021-05-17 · Archived: 2026-04-02 11:37:31 UTC

Bizarro is yet another banking Trojan family originating from Brazil that is now found in other regions of the world. We have seen users being targeted in **Spain, Portugal, France and Italy. Attempts have now been made to steal credentials from customers of 70 banks from different European and South American countries.** Following in the footsteps of Tetrade, Bizarro is using affiliates or recruiting money mules to operationalize their attacks, cashing out or simply to helping with transfers. In this article we analyse the technical features of the Trojan's components, giving a detailed overview of obfuscation techniques, the infection process and subsequent functions, as well as the social engineering tactics used by the cybercriminals to convince their victims to give away their personal online banking details.

Bizarro has x64 modules and is able to trick users into entering two-factor authentication codes in fake pop-ups. It may also use social engineering to convince victims to download a smartphone app. The group behind Bizzaro uses servers hosted on Azure and Amazon (AWS) and compromised WordPress servers to store the malware and collect telemetry.

Bizarreland

Bizarro is distributed via MSI packages downloaded by victims from links in spam emails. Once launched, Bizarro downloads a ZIP archive from a compromised website. While writing this article, we saw hacked WordPress, Amazon and Azure servers used for storing archives. The MSI installer has two embedded links – which one is chosen depends on the victim's processor architecture.



Typical malicious message sent by Bizarro operators

The downloaded ZIP archive contains the following files:

- A malicious DLL written in Delphi;
- A legitimate executable that is an AutoHotkey script runner (in some samples AutoIt is used instead of AutoHotkey);
- A small script that calls an exported function from the malicious DLL.

The DLL exports a function that contains the malicious code. The malware developers have used obfuscation to complicate code analysis. The code of the exported functions have been removed by the protector. The bytes that belong to the exported functions are restored by the DLL entry point function at runtime. This entry point function is heavily obfuscated. The tricks used to complicate analysis consist of constant unfolding and junk code insertion. As for the malware developers, they are constantly improving the protection of the binaries. In earlier versions of Bizarro, only the entry point function was protected, while in more recent samples the protector is also used to obscure calls of the imported API functions.

When Bizarro starts, it first kills all the browser processes to terminate any existing sessions with online banking websites. When a user restarts the browsers, they will be forced to re-enter the bank account credentials, which will be captured by the malware. Another step Bizarro takes in order to get as many credentials as possible is to disable autocomplete in a browser.

Bizarro gathers the following information about the system on which it is running:

- Computer name;
- Operating system version;
- Default browser name;
- Installed antivirus software name.

Bizarro uses the '**Mozilla/4.0 (compatible;MSIE 6.0; Windows NT 5.0′** user agent while sending the POST request. This user agent has typos: there should be a space symbol after the **compatible;** substring and the closing bracket is missing. Our research shows that this mistake has not been fixed in the latest versions. After that, Bizarro creates an empty file in the *%userprofile%* directory, thus marking the system as infected. The name of the file is the name of the script runner (AutoIt or AutoHotKey) with the .jkl extension appended to it.

Having sent the data to the telemetry server, Bizarro initializes the screen capturing module. It loads the **magnification.dll** library and gets the address of the deprecated **MagSetImageScalingCallback** API function. With its help, the Trojan can capture the screen of a user and also constantly monitor the system clipboard, looking for a Bitcoin wallet address. If it finds one, it is replaced with a wallet belonging to the malware developers.

The backdoor is the core component of Bizarro: it contains more than 100 commands and allows the attackers to steal online banking account credentials. Most of the commands are used to display fake pop-up messages to users. The core component of the backdoor doesn't start until Bizarro detects a connection to one of the hardcoded online banking systems. The malware does this by enumerating all the windows, collecting their names. Whitespace characters, letters with accents (such as ñ or á) and non-letter symbols such as dashes are removed

from the window name strings. If a window name matches one of the hardcoded strings, the backdoor continues starting up.

The first thing the backdoor does is remove the DNS cache by executing the *ipconfig /flushdns* command. This is done in order to prevent connecting to a blocked IP. After that, the malware resolves the domain name to an IP address, creates a socket and binds it to the resolved address. If the connection was successful, it creates the **%userprofile%\bizarro.txt** file.

The Backdoor and its C2

The commands that Bizarro receives from its C2 can be divided into the following categories:

- **Commands that allow the C2 operators to get data about the victim and manage the connection status**

  The <|**PT**|> command sends the environment information to the C2: Bizarro's version, OS name, computer name, Bizarro's unique identifier, installed antivirus software and the codename used for the bank that has been accessed. The codenames are bank names written in leetspeak.

- **Commands that allow attackers to control the files located on the victim's hard drive**

  The <|**DownloadFile**|> command downloads files to the victim's computer, while the <|**UploadFile**|> command allows attackers to fetch files from the client machine. The <|**Folder**|> and <|**File**|> commands allow the attackers to search for folders and files which have a given mask.

- **Commands that allow attackers to control the user's mouse and keyboard**

  The <|**SuaykRJ**|> command performs a left mouse button click at the designated location. The <|**SuaykJI**|> command performs a double click at the given location, while the <|**IXjzwtR**|> command performs a right mouse button click. The <|**ztUjzwtR**|> command moves the mouse to a designated location. The syntax of these three commands is <|**command name**|>**x coordinate**<|>**y coordinate**<<|.

  Bizarro can also manipulate the user's keyboard (what the user actually types) with the help of the **carmena** command.

- **Commands that allow the attackers to control the backdoor operation, shut down, restart or destroy the operating system and limit the functionality of Windows**

  The **LkingWajuGhkzwu** command shuts the backdoor down, while the **vkbAlcvtlY** command drops a BAT file in the working directory. The batch script is responsible for deleting the malware from disk.

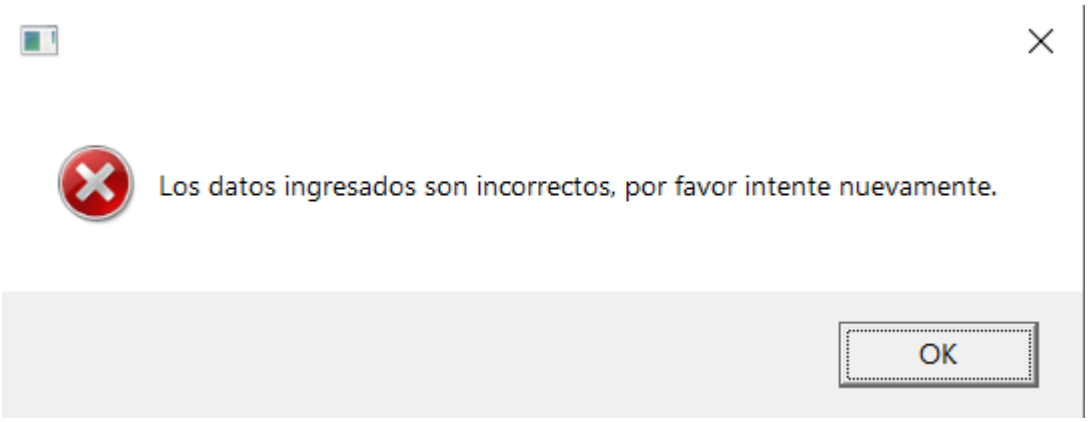
- **Commands that log keystrokes**

  Bizarro supports two commands that are responsible for keylogging. The **COZUMEL** command starts the logging process, while the **COZUMARIA** command stops it.

- **Commands that perform social engineering attacks**

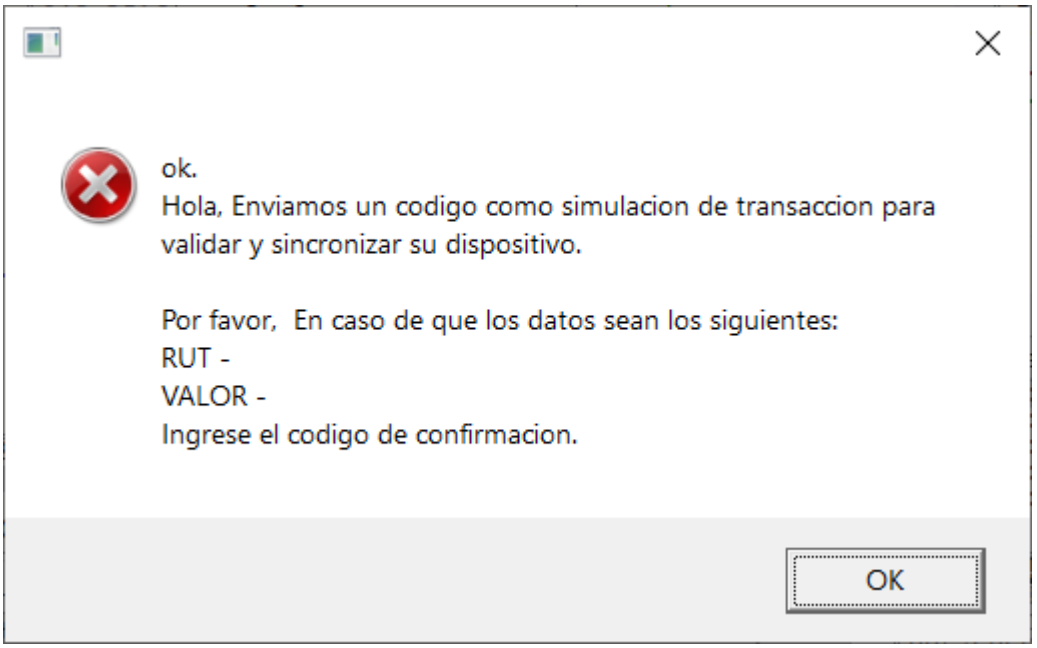
These commands display various messages that trick users into giving attackers access to the bank account. The type of messages displayed vary from simple message boxes to well-designed windows with bank logs on them.

We will first describe commands that show Windows message boxes. The **dkxqdpdv** command displays an error message with the text: *"Los datos ingresados son incorrectos, por favor intente nuevamente."* (English: *"The data entered is incorrect, please try again."*)



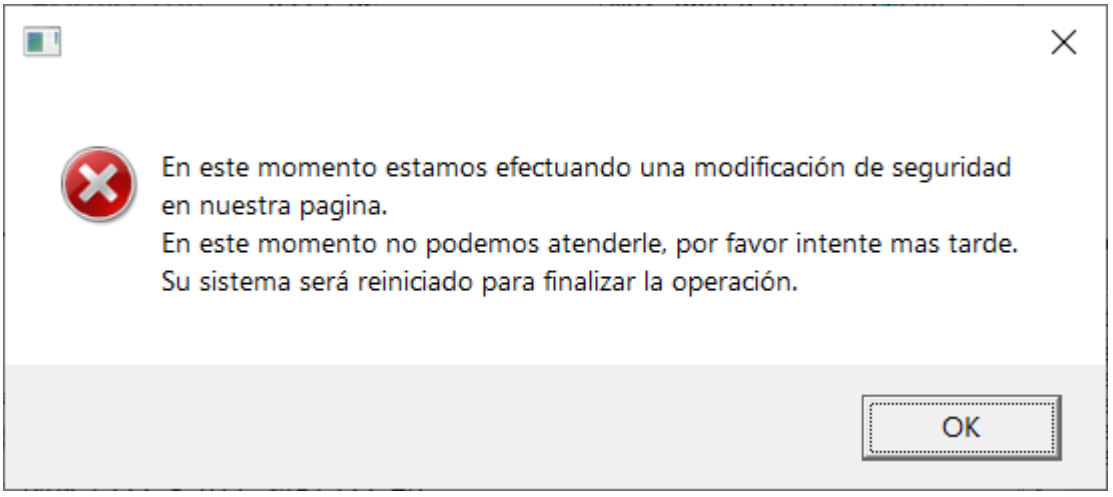
Bizarro shows a message telling the user to enter the requested data again

The **vanessa** command displays an error message which tells the user to enter confirmation information. To further convince the user that all operations are legitimate, the malware displays the RUT (Rol Único Tributario, a Chilean ID number) and the value that was supplied earlier. The message has the following text:



Error message asking the user to enter a confirmation code

The **LMAimwc** command displays another error message. This time it tells the user that their computer needs to be restarted in order to finish a security-related operation. Bizarro displays the following text:



Error message telling the user that the operating system will be restarted

The most interesting messages that Bizarro displays are those that try to mimic online banking systems. To display such messages, Bizarro needs to download a JPEG image that contains the bank logo and instructions the victim needs to follow. These images are stored in the user profile directory in an encrypted form. Before an image is used in a message, it is decrypted with a multi-byte XOR algorithm. As the messages are downloaded from the C2 server, they can be found only on the victims' machines.

The first type of custom messages that Bizarro may show are messages that freeze the victim's machine, thus allowing the attackers to gain some time. When a command to display a message like this is received, the taskbar is hidden, the screen is greyed out and the message itself is displayed. While the message is shown, the user is unable to close it or open Task Manager. The message itself tells the user either that the system is compromised and thus needs to be updated or that security and browser performance components are being installed. This type of message also contains a progress bar that changes over time.

The images below show what these messages look like on the screens of victims, with messages written in Spanish:

Bizarro blocking a bank login page and telling the user that security updates are being installed

The following two messages try to convince the victim that their system is compromised. In most of them, Bizarro tells the user not to worry about any transactions that occur during the “security update” as they are only confirming the identity of the client. This makes clients feel more confident about approving all the transactions requested by the attackers.

Messages telling the user that their system is compromised

Bizarro also tries to lure victims into sending two-factor authentication codes to the attackers. Another interesting feature we have seen entails an attempt to convince the victim to install a malicious app on their smartphone. It uses the following windows to determine the type of mobile operating system:

Bizarro asks the user to choose the operating system of their smartphone

If the victim chooses Android, the C2 server will send a link with a malicious application to the client. The client will make a QR code out of it with the help of the Google Charts API. It sends a request with the following arguments:

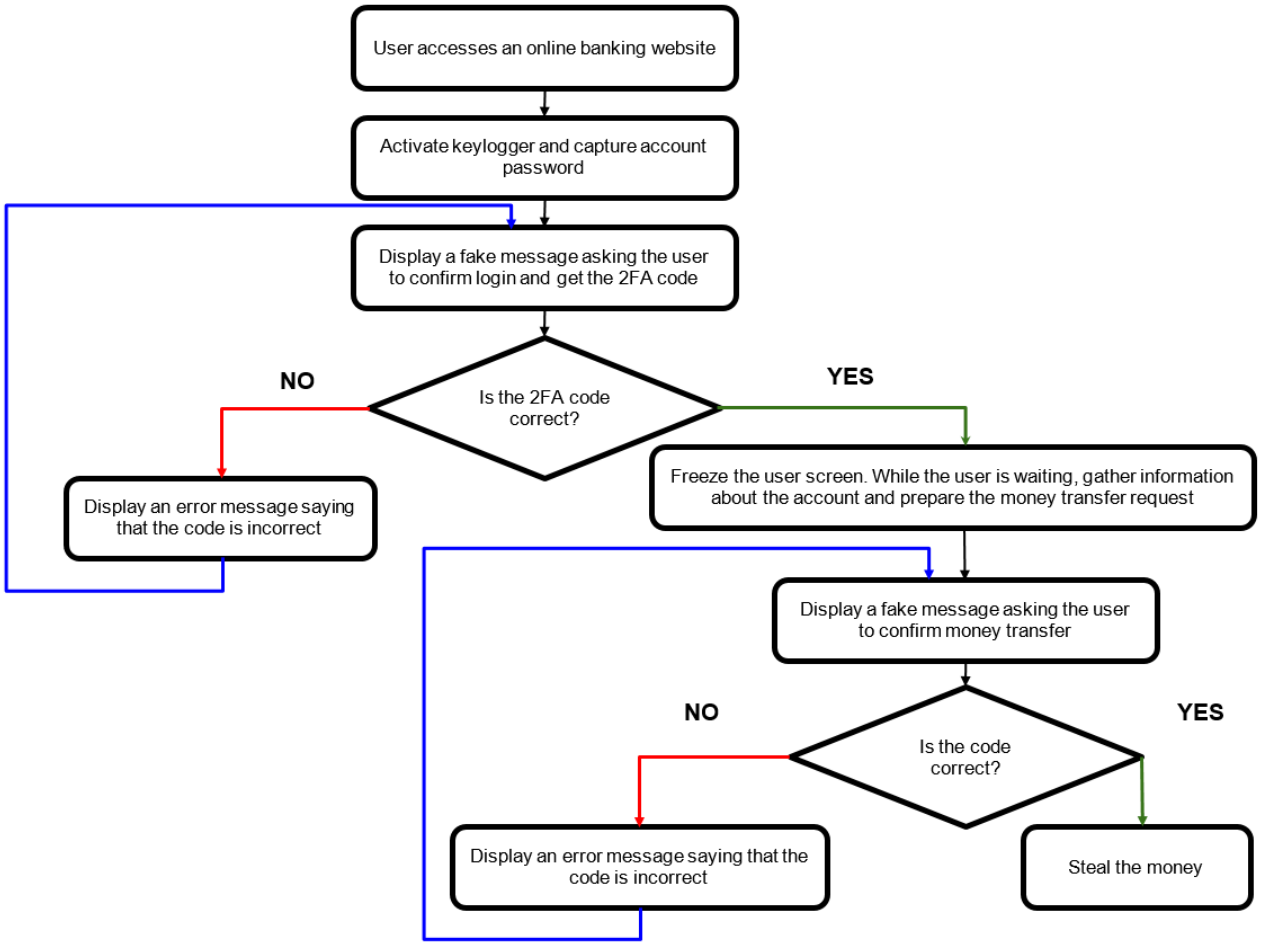
```
http://chart.apis.google.com/chart?chs=<QR code width>x<QR code height>&cht=qr&chld=<error correction level>&chl=<link to the application>
```

The obtained QR code is then shown in a window with the following text:

Bizarro asking the user to scan the QR code

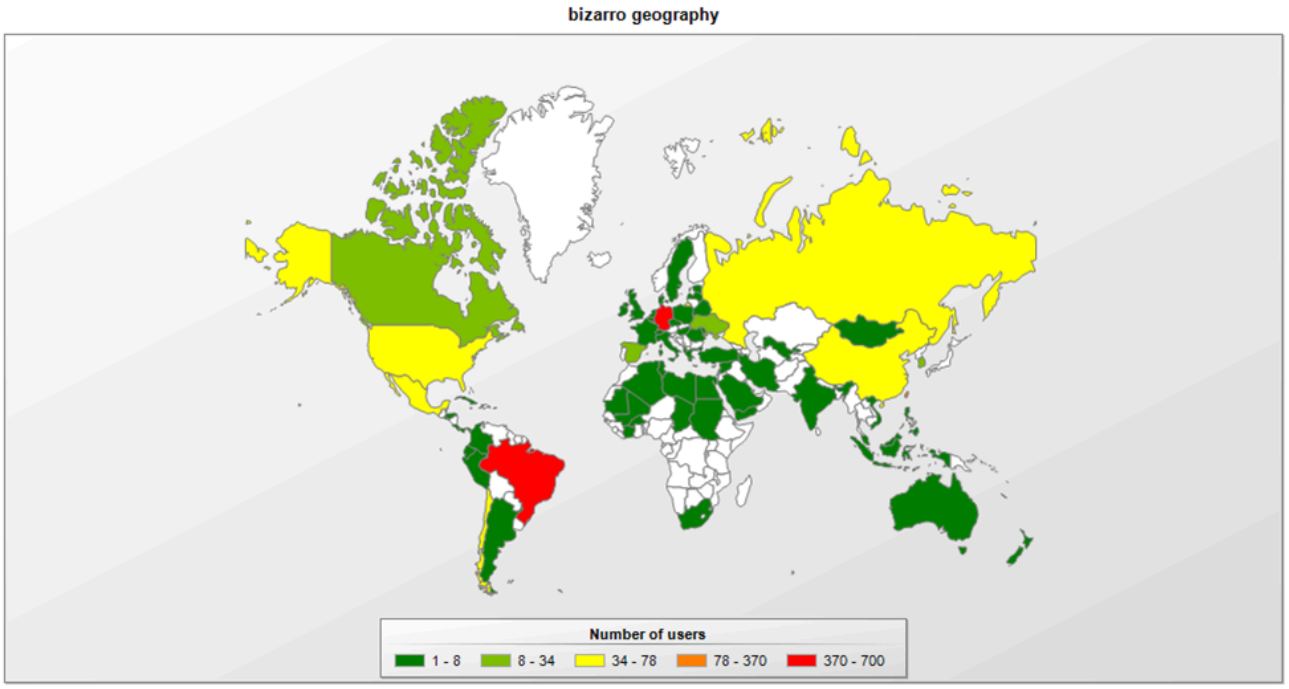
Attack scenario

With the help of the commands that the Bizarro developers have included in the Trojan, adversaries may stage an attack with the following scenario:



Infection scheme used by Bizarro

According to the list of supported banks, the threat actor behind Bizarro is targeting clients of various banks from Europe and South America. Based on our telemetry, we've seen victims of Bizarro in different countries, including Brazil, Argentina, Chile, Germany, Spain, Portugal, France and Italy. These statistics again prove the fact that Bizarro's operators have expanded their interest from Brazil to other countries in South America and Europe.

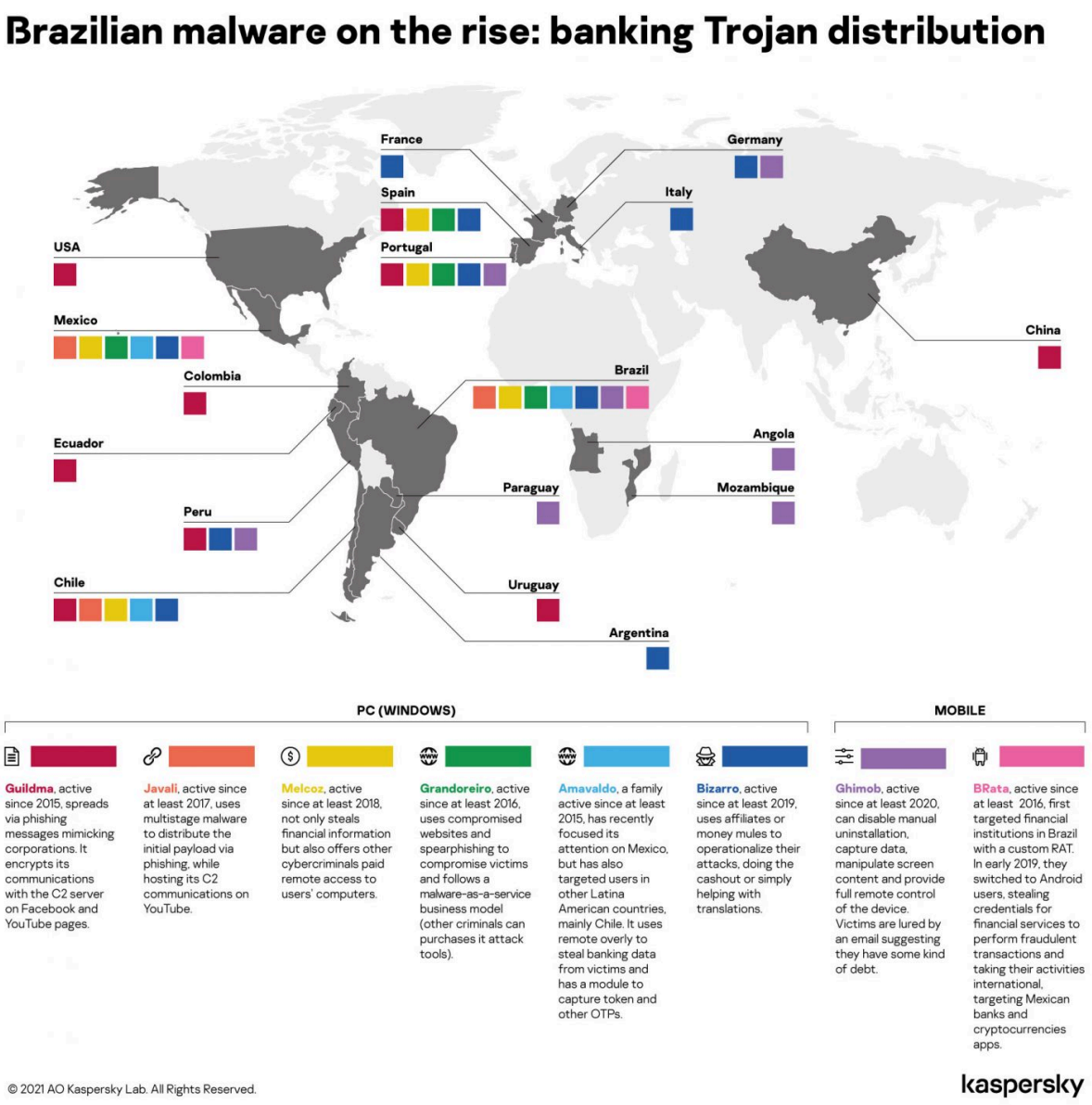


Distribution of Bizarro detections in the last 12 months

Conclusion

We've recently seen several banking Trojans from South America (such as Guildma, Javali, Melcoz, Grandoreiro and Amavaldo) expanding their operations to other regions, mainly Europe. Bizarro is yet another example of this. The threat actors behind this campaign are adopting various technical methods to complicate malware analysis and detection, as well as social engineering tricks that can help convince victims to provide personal data related to their online banking accounts.

Kaspersky products detect this family as **Trojan-Banker.Win32.Bizarro** or **Trojan-Banker.Win64.Bizarro**. All the details, IoCs, MITRE ATT&CK Framework data, Yara rules and hashes relating to this threat are available to users of our Financial Threat Intel services. To learn more about threat hunting and malware analysis from Kaspersky's GReAT experts, check out http://xtraining.kaspersky.com



Indicators of compromise

Reference MD5 hashes

e6c337d504b2d7d80d706899d964ab45
daf028ddae0edbd3d7946bb26cf05fbf
5184776f72962859b704f7cc370460ea
73472698fe41df730682977c8e751a3e
7a1ce2f8f714367f92a31da1519a3de3
0403d605e6418cbdf8e946736d1497ad
d6e4236aaade8c90366966d59e735568
a083d5ff976347f1cd5ba1d9e3a7a4b3

b0d0990beefa11c9a78c701e2aa46f87
38003677bfaa1c6729f7fa00da5c9109
