The Tetrade: Brazilian banking malware goes global

MALWARE DESCRIPTIONS 14 JUL 2020 15 minute read

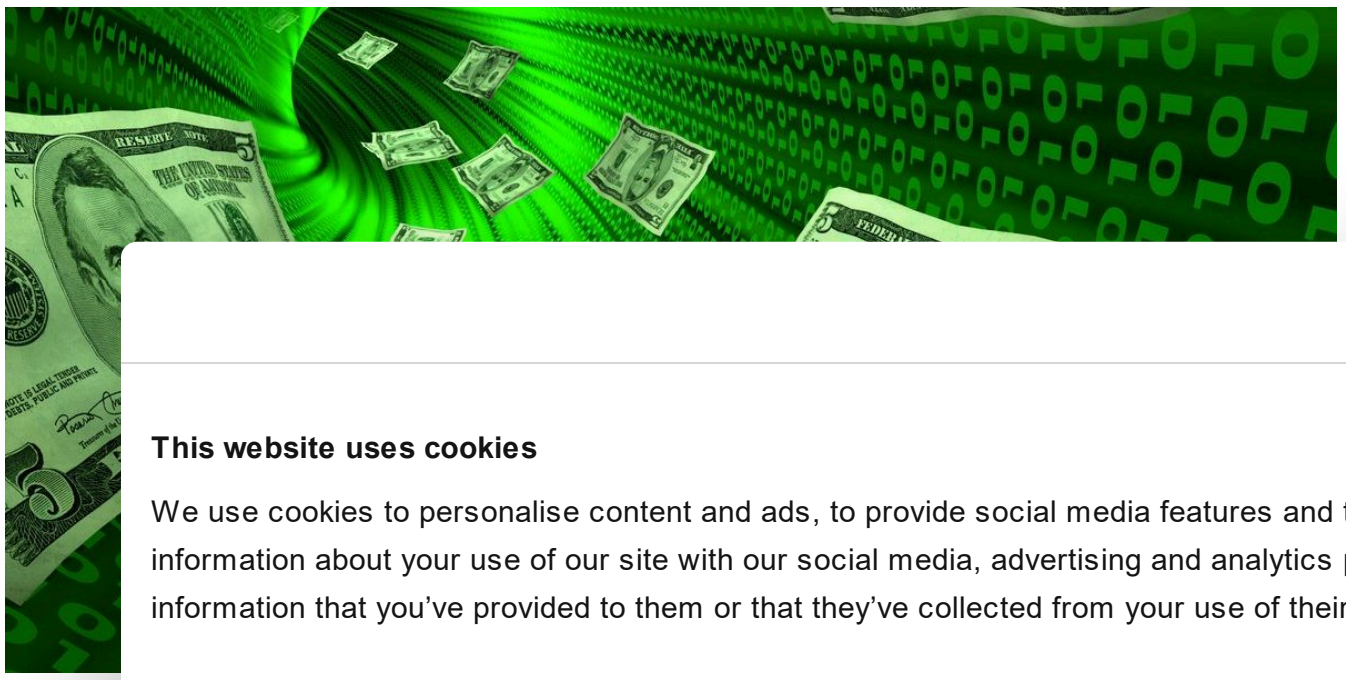


Table of Contents

// AU

Expert GRE

PC

Intro

Brazil is a
Brazilian
perpetra
have a s

local banks. But the time has come when they aggressively expand their attacks and operations abroad, targeting other countries and banks. The **Tetrade** is our designation for four large banking trojan families created, developed and spread by Brazilian crooks, but now on a global level.

Although this is not their first attempt – they tried, timidly, in 2011, using very basic trojans, with a low success rate – now the situation is completely different. Brazilian banking trojans have evolved greatly, with hackers adopting techniques for bypassing detection, creating highly modular and obfuscated malware, and using a very complex execution flow, which makes analysis a painful, tricky process.

At least since the year 2000, Brazilian banks have operated in a very hostile online environment full of fraud. Despite their early adoption of technologies aimed at protecting the customer, and deployment of plugins, tokens, e-tokens, two-factor authentication, CHIP and PIN credit cards, and other ways to safeguard their millions of clients, fraud is still ramping up, as the country still lacks proper legislation for punishing cybercriminals.

This article is a deep dive intended for a complete understanding of these four banking trojan families: **Guildma, Javali, Melcoz and Grandoreiro**, as they expand abroad, targeting users not just in Brazil, but in the wider Latin America and Europe.

These crooks are prepared to take on the world. Are the financial system and security analysts ready to deal with this persistent avalanche?

Guildma: full of tricks

Also known as	Astaroth
First seen	2015
Tricks	LOLBin and NTFS Alternate Data Streams (ADS), process hollowing, payloads hosted within YouTube and Facebook posts
Ready to steal data from victims living in...	Chile, Uruguay, Peru, Ecuador, Colombia, China, Europe. Confirmed victims in Brazil

The Guildma malware has been active since at least 2015, when it was targeting banking users exclusively from Brazil. From there on, it has been constantly updated, adding new targets, new features and stealthiness to its campaigns, and directing its attacks at other countries in Latin America. The group behind the attacks have shown a good knowledge of legitimate tools for performing a complex execution flow, pretending to hide themselves inside the host system and preventi

Recently
order to
highly m
sending
LNK; the
downloa

The malv
usage of
Streams
CloudFla
where th

From I

Guildma
attached
phishing
other regular corporate subjects, including the COVID-19 pandemic, but always with a corporate appearance.

Javascript executed in order to download a compressed LNK file

In order to download the additional modules, the malware uses the BITSAdmin tool, which this group has relied on for some years to avoid detection, since this is an allowlisted tool from the Windows operating system. By the end of September 2019, we started seeing a new version of Guildma malware being distributed that used a new technique for storing downloaded payloads in NTFS Alternate Data Streams in order to conceal their presence in the system.

```
c:\windows\system32\cmd.exe /c type "c:\users\public\Libraries\radm\koddsuffyi.gif" >
"c:\users\public\Libraries\radm\desktop.ini:koddsuffyi.gif" && erase
"c:\users\public\Libraries\radm\koddsuffyi.gif"
```

Downloaded payload being stored in desktop.ini's ADS

The usage of ADS helps to hide the file in the system, since it will not appear in Explorer, etc. In order to see the alternate data, you can use the "DIR" command, adding the switch "/R", which is specifically intended for to displaying alternate data streams.

Some of the anti-debugging/anti-emulation techniques used by the loader

This stage checks for debugging tools, virtual environments, known Windows product IDs commonly used by sandboxes, common usernames and certain disk serial numbers that are most likely associated with analyst environments detected earlier. If nothing like that is detected, the malware will decrypt the third stage and execute it by using the process

hollowing technique, commonly used by malware authors. In this version, the payloads are encrypted with the same XOR-based algorithm as the one used in previous versions, however in this latest version, the payload is encrypted twice, with different keys.

File content is encrypted twice using different keys

In order to execute the additional modules, the malware uses the process hollowing technique for hiding the malicious payload inside an allowlisted process, such as svchost.exe. The payloads are stored encrypted in the filesystem and decrypted in the memory as they are executed.

The final payload installed in the system will monitor user activities, such as opened websites and run applications and check if they are on the target list. When a target is detected, the module is executed, giving the criminals control over banking transactions.

This mod

- full c
- togg
- requ
- QR c
- requ

The atta
while av
machine

Youtul

After all
commun
versions
pages.

C2 information hosted on a YouTube page

The newer versions of Guildma found in 2020 are using an automated process to generate thousands of daily URLs, mostly abusing generic TLDs. Our systems have been catching more than 200 different URLs per day, such as:

01autogestor.ga	ghcco980m1zy9.org
04autogestor.ml	gurulea8.ml
0ff2mft71jarf.gq	k8cf0j5u.cf
2va6v.6pnc3461.ink	kaligodfrey.casa
4nk7h3s453b019.com.de	kfgkqnf5.cf
64pgrpyxpueoj.ga	nfiru.xyz
6pnc3461.ink	osieofcorizon.fun
6zs1njbw.ml	paiuew.bnorp.ml
7wpinibw	
84m4bl42	
909nu3d	
bantqr8rr	
evokgtis.	
g2ha14u2	

Our tele

Guildma: widespread globally

The intended targets of Guildma can be seen in the code: the malware is capable of stealing data from bank customers living in Chile, Uruguay, Peru, Ecuador, Colombia, China, Europe, and of course, Brazil. However, the code has been found in just one version of Guildma and has not been implemented in any of the newer versions.

FROM THE SAME AUTHORS

Grandoreiro, the global trojan with grandiose goals

Stealer here, stealer there, stealers everywhere!

Exotic SambaSpy is now dancing with Italian users

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Java

First seen

Tricks

Confirme

Javali ta
primarily
uses mu
or link to
Visual Ba
DLL side
and secu

The initial Microsoft Installer downloader contains an embedded custom action that triggers a Visual Basic Script. The script connects to a remote server and retrieves the second stage of the malware.

Using MSI's 'CustomAction' events to trigger the execution of the downloader VBS

The downloaded ZIP file package contains several files and a malicious payload that is capable of stealing financial information from the victim. A decompressed package commonly contains a large number of files including executables that are legit but vulnerable to DLL sideloading.

The contents of a typical Javali .ZIP package, including a 602 MB DLL file

The legitimate DLL that would be used in this case has the size of roughly 600 KB, but here we have an obfuscated library **that is over 600 MB**. The large size of the file is intended to hamper analysis and detection. In addition to that, file size limitations will prevent uploading to multiscanners like VirusTotal, etc. Once all empty sections have been removed from the library, the final payload is a binary of 27.5 MB...

After de
malware

Javali after deobfuscation: looking for Mexican bank customers

GDocs for malware

Once the library is called by one of the triggering events implemented in its code, it reads a configuration file from a shared **Google Document**. If it is not able to connect to the address, it uses a hardcoded one.

Configuration settings stored in a shared Google Document

The original configuration.

```
inicio{

"host":"7FF87EF610080973F065CAB4B5B0AA",

"porta":"0000"

}fim
```

The host
named I
started

Upon in-
Dependi
solutions
capture
find ope
monitore

The victi
demonst

Javali: focus on Brazil and Mexico

Javali is using allowlisted and signed binaries, Microsoft Installer files and DLL hijacking to infect victims en masse, all while targeting their efforts by country. This is achieved by controlling the means of distribution and sending phishing email only to those TLDs that the group is interested in. We can expect expansion mainly across Latin America.

Melcoz, a worldwide operator

First seen	2018 (worldwide) but active in Brazil for years
Tricks	DLL hijacking, AutoIt loaders, Bitcoin wallet stealing module
Confirmed victims in	Brazil, Chile, Mexico, Spain, Portugal

Melcoz is a banking trojan family developed by a group that has been active in Brazil for years, but at least since 2018, has expanded overseas. Their Eastern European partners heavily inspired the recent attacks. The new operations are professionally executed, scalable and persistent, creating various versions of the malware, with significant infrastructure improvements that enable cybercriminal groups in different countries to collaborate.

We found that the group has attacked assets in Chile since 2018 and more recently, in Mexico. Still, it is highly probable there are victims in other countries, as some of the targeted banks operate internationally. However, the attacks seem to be focused more on Latin American victims these days. As these groups speak different languages (Portuguese and Spanish), we believe that Brazilian cybercriminals are working with local groups of coders and mules to withdraw stolen money, managed by different operators, selling access to its infrastructure and malv
and CnC

Generall
DLLs usi
passwor
banking
wallet int

Yet Ar

Melcoz i
is availab
started
countrie
that con

Phishing email written in Spanish

Almost all of the analyzed MSI samples used some version of Advanced Installer with a VBS script appended to the CustomAction section, which makes the script run during the installation process. The script itself works as a downloader for additional files needed for loading the malware into the system, which are hosted separately as a ZIP package. We confirmed two different techniques used for distributing the Melcoz backdoor: the **AutoIt loader script** and **DLL Hijack**.

The official AutoIt3 interpreter comes as part of the AutoIt installation package, and it is used by the malware to execute the compiled script. The VBS script runs the AutoIt interpreter, passing the compiled script as an argument. Once executed, it loads the library, which was also passed as an argument to call a hardcoded exported function.

The code also has a timer that monitors content saved to the clipboard. Once a match is triggered, the malware checks if there is a Bitcoin wallet and then replaces it with the cybercriminal's wallet.

The attackers rely on a compromised legitimate server, as well as commercial servers they purchased. The compromised servers mostly host samples for attacking victims, whereas the commercial hosting is for C2 server communications. As mentioned earlier, different operators run different campaigns. This explains the different network infrastructures seen so far.

According to our telemetry, Melcoz samples have been detected in other Latin American countries and in Europe, mainly in Spain and Portugal.

Melcoz detections worldwide: focus on Brazil, Chile, Spain and Portugal

El Gran Grandoreiro

First seen

Tricks

Confirme

Just like
in Europ
installers
The malv
compute

We have
techniqu
Domain
one of th

It is still
that the
information collected during the analysis that showed many operators were involved.

While tracking of cybercrime campaigns that targeted Latin America, we found one interesting attack that was very similar to known Brazilian banking malware, but had distinctive features relating to the infection vector and the code itself. It was possible to identify two clusters of attacks, the first one targeting Brazilian banks and the second one aimed at other banks in Latin America and Europe. This is to be expected: many European banks have operations and branches in Latin America, so this is a natural next step for the cybercriminals.

The cluster targeting Brazil used hacked websites and Google Ads to drive users to download the malicious installer. The campaign targeting other countries used spear-phishing as the delivery method.

Lumma/Amadey: fake CAPTCHAs want to know if you're human

Grandoreiro, the global trojan with grandiose goals

Scam Information and Event Management

How the Necro Trojan infiltrated Google Play, again

Loki: a new private agent for the popular Mythic framework

The main module is in charge of monitoring all browser activity, looking for any actions related to online banking. As we analyzed the campaign, we identified two clusters of activity: the first one mainly focused on Brazilian targets and the second one focused more on international targets.

The code suggests that the campaign is being managed by various operators. The sample build specifies an operator ID, which will be used for select a C2 server to contact.

Code used to generate the URL based on the operator ID

The code above will calculate the path to a Google Sites page containing information about the C2 server to be used by the malware. The algorithm uses a key that is specific to the user as well as the current date, which means that the URL will change daily.

ID	Operator	Key	Date	Genera path
01	zemad	jkABCDEefghiHIa4567JKLMN3UVWpqrst2Z89PQRSTbuvwxyzXYFG01cdOlmno	16Mar0	zemadh
02	rici	jkABCDEefghFG01cdOlmnopqrst2Z89PQRiHIa4567JKLMN3UVWXYSTbuvwxyz	16Mar0	ricigms
03	breza	01cdOlmnopqrst2Z89PQRSTbuvwxjkABCDEefghiHIa4567JKLMN3UVWXYFGyz	16Mar0	brezasc
04	grl2	mDEefghiHIa4567JKLMNnopqrst2Z89PQRSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	grl25ns
05	rox2	567JKLMNnopqrst2Z89PQmDEefghiHIa4RSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	rox2rpfs
06	mrb	567JKLMNnopqrst2Z89PQmDEefghiHIa4RSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	mrbrpfs
07	ER	jkABCDEefghiHIa4567JKLMN3UVWXYFG01cdOlmnopqrst2Z89PQRSTbuvwxyz	16Mar0	erhjui3r

The generated path will then be contacted in order to get information about the C2 server to be used

The ope
operato
on the m

- requesting information needed for the banking transaction, such as an SMS token or QR code;
- allowing full remote access to the machine;
- blocking access to the bank website: this feature helps to prevent the victim from learning that funds were transferred from their account.

DGA and Google sites

The campaign uses commercial hosting sites in its attacks. In many cases, they use a very specific Web server named *HFS, or HTTP File Server* for hosting encrypted payloads. One can note a small change on the displayed page that helps to show "Infects" instead of "Hits" as used on the default page.

HFS used for hosting the encrypted payloads

Those hosting sites are disposable. Each is used for a short time before the operators move on to another server. We have seen Grandoreiro use DGA functions to generate a connection to a Google Sites page storing C2 information.

As for the victims, it is possible to confirm by analyzing samples that the campaign targets Brazil, Mexico, Spain and Portugal. However, it is highly possible that other countries are also victims since the targeted institutions have operations in other countries as well.

Conc

Guildma,
group/op
countries. They benefit from the fact that many banks operating in Brazil also have operations elsewhere in Latin America and Europe, making it easy to extend their attacks against customers of these financial institutions.

Brazilian crooks are rapidly creating an ecosystem of affiliates, recruiting cybercriminals to work with in other countries, adopting MaaS (malware-as-a-service) and quickly adding new techniques to their malware as a way to keep it relevant and financially attractive to their partners. They are certainly leading the creation of this type of threats in Latin America, mainly because they need local partners to manage the stolen money and to help with translation, as most of them are not native in Spanish. This professional approach draws a lot of inspiration from ZeuS, SpyEye and other big banking trojans of the past.

As a threat, these banking trojan families try to innovate by using DGA, encrypted payloads, process hollowing, DLL hijacking, a lot of LoLBins, fileless infections and other tricks as a way of obstructing analysis and detection. We believe that these threats will evolve to target more banks in more countries. We know they are not the only ones doing this, as other families of the same origin have already made a similar transition, possibly inspired by the success of their "competitors". This seems to be a trend among Brazilian malware developers that is here to stay.

We recommend that financial institutions watch these threats closely, while improving their authentication processes, boosting anti-fraud technology and threat intel data, and trying to understand and mitigate such risks. All the details, IoCs, Yara rules and hashes of these threats are available to the users of our Financial Threat Intel services.

MD5

Guildma
0219ef20ab2df29b9b29f8407cf74f1c
0931a26d44f0e7d70fda9ef86ee203f4

Javali
5ce1eb8065acad5b59288b5662936f5d
91b271e7bfe64566de562a8dd2145ac6

Melcoz
4194162fe30a3dca6d8568e72c71ed2d
aeaf7355604685d4d753d21902ff1c1c
c63b4eb3067d8cb5f2d576bc0777e87d

Grandoreiro
071d3d6
1b50b1e

BRAZI

MALWA

The T

Your em

Type y

Name *

Comment

// LATEST POSTS

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THR

04 SEP 20

Inside t the hum cybercr

ANNA PAVLO

PS

60 MIN

acklogs

// RE

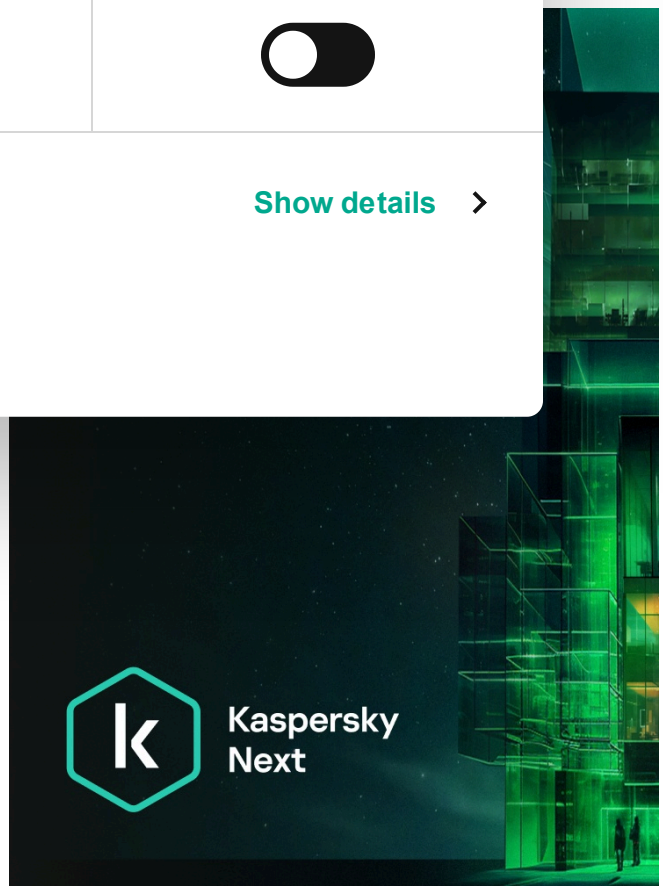
Beyond expansi

Kaspers activity: Africa, p

EastWi attacks Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.



// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at

the bottom of any e-mail sent to me for the purposes mentioned above.