Ghimob: a Tétrade threat actor moves to infect mobile devices

securelist.com/ghimob-tetrade-threat-mobile-devices/99228/

Authors

Expert GReAT

Guildma, a threat actor that is part of the Tétrade family of banking trojans, has been working on bringing in new techniques, creating new malware and targeting new victims. Recently, their new creation, the **Ghimob** banking trojan, has been a move toward infecting mobile devices, targeting financial apps from banks, fintechs, exchanges and cryptocurrencies in Brazil, Paraguay, Peru, Portugal, Germany, Angola and Mozambique.

Ghimob is a full-fledged spy in your pocket: once infection is completed, the hacker can access the infected device remotely, completing the fraudulent transaction with the victim's smartphone, so as to avoid machine identification, security measures implemented by financial institutions and all their antifraud behavioral systems. Even if the user has a screen lock pattern in place, Ghimob is able to record it and later replay it to unlock the device.

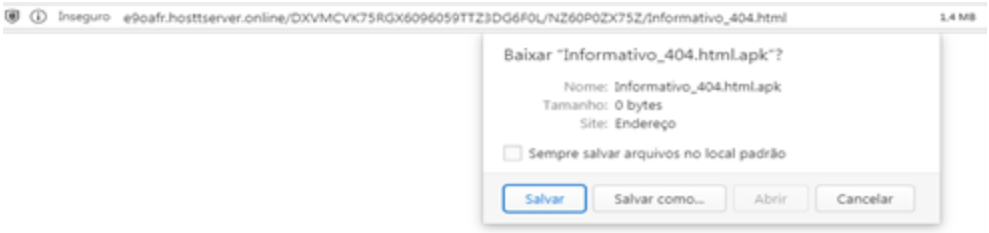
When the cybercriminal is ready to perform the transaction, they can insert a black screen as an overlay or open some website in full screen, so while the user looks at that screen, the criminal performs the transaction in the background by using the financial app running on the victim's smartphone that the user has opened or logged in to.

From a technical standpoint, **Ghimob** is also interesting in that it uses C2s with fallback protected by Cloudflare, hides its real C2 with DGA and employs several other tricks, posing as a strong competitor in this field. But yet, no sign of MaaS (malware-as-a-service). Compared to BRATA or Basbanke, another mobile banking trojan family originating in Brazil, **Ghimob** is far more advanced and richer in features, and has strong persistence.

Multiplatform financial attack

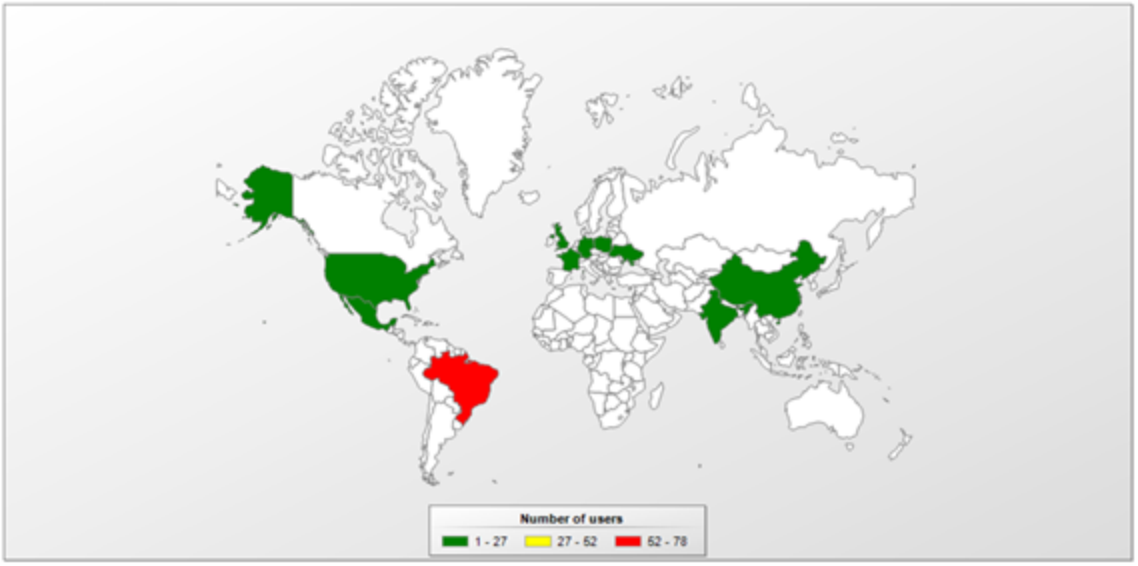
While monitoring a Guildma Windows malware campaign, we were able to find malicious URLs used for distributing both ZIP files for Windows boxes and APK files, all from the same URL. If the user-agent that clicked the malicious link is an Android-based browser, the file downloaded will be the Ghimob APK installer.

The APKs thus distributed are posing as installers of popular apps; they are not on Google Play but rather hosted in several malicious domains registered by Guildma operators. Once installed on the phone, the app will abuse Accessibility Mode to gain persistence, disable manual uninstallation and allow the banking trojan to capture data, manipulate screen content and provide full remote control to the fraudster: a very typical mobile RAT.



Same link, different files: ZIP for Windows, APK for Android

Our telemetry shows that all victims of the Ghimob mobile banking trojan are located in Brazil at the moment, but like all other Tétrade threat actors, Ghimob has big plans to expand abroad.



Ghimob detections: Brazil for now, but ready to expand abroad

To lure the victim into installing the malicious file, the email is written as if from a creditor and provides a link where the recipient could view more information, while the app itself pretends to be Google Defender, Google Docs, WhatsApp Updater, etc.

Prezado Cliente

Detectamos em nossos registros até presente data que encontra-se em aberto a fatura abaixo.
Solicitamos vossa especial atenção em verificar por qual motivo este título ainda nao foi pago,
antes das instruções automáticas de PROTESTO e SERASA do título.
Se já tenha sido pago, pedimos tambem nos comunicar.

FATURA: CWB-100991.5
EMISSÃO: 10/09/2020
VENCTO: 20/09/2020
VALOR: 227,32

Para sua conferencia e pagamento, segue abaixo os links para baixa-la.
Para faturas com mais de um CT-e, os arquivos XMLs e DACTEs estarão
compactados em formato .ZIP

Para download da fatura em PDF, acesse neste link

Para download do XML dos CT-e 's, acesse neste link

Para download do DACTE em PDF, acesse neste link

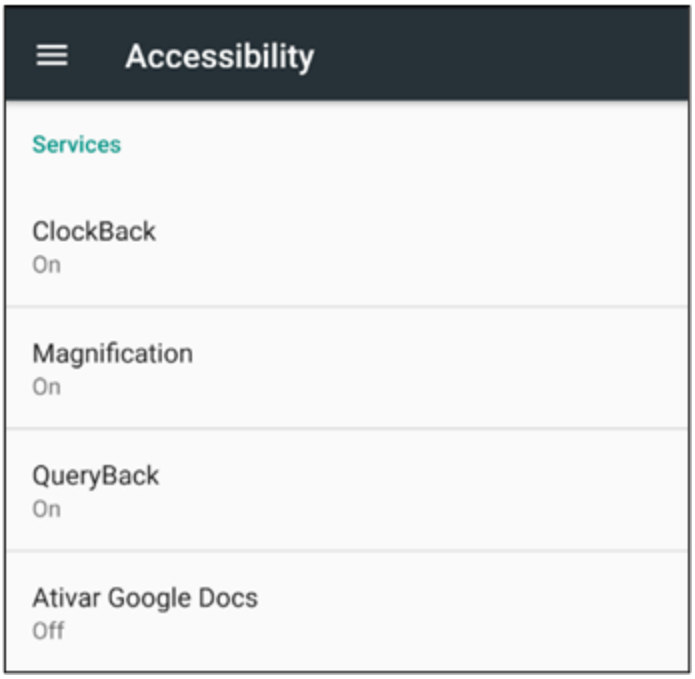
Caso necessite dirimir dúvidas, favor entrar em contato conosco o mais breve possível.
Estamos a sua disposição para ajudar.

A malicious message distributing the malware, written in Brazilian Portuguese

A persistent RAT in your pocket

As soon as the malware is launched, it tries to detect common emulators, checks for the presence of a debugger attached to the process and the manifest file, and also checks for a debuggable flag. If any of these are present, then the malware simply terminates itself.

Newer versions of the malware have moved the emulator names to an encrypted configuration file. If those previous checks are passed, the user is then presented with the default Android accessibility window, as the malware heavily relies on accessibility to work.



"Google Docs" is asking you to provide Accessibility permissions

Once infection is completed, the malware proceeds to send an infection notification message to its notification server. This includes the phone model, whether it has a screen lock activated and a list of all installed apps that the malware has as a target including version numbers. **Ghimob spies on 153 mobile apps**, mainly from banks, fintechs, cryptocurrencies and exchanges. By analyzing the malware, it is possible to see all the apps monitored and targeted by the RAT. These are mainly institutions in Brazil (where it watches 112 apps), but since Ghimob, like other Tétrade threat actors, has been moving toward expanding its operations, it also watches the system for cryptocurrency apps from different countries (thirteen apps) and international payment systems (nine apps). Also targeted are banks in Germany (five apps), Portugal (three apps), Perú (two apps), Paraguay (two apps), Angola and Mozambique (one app per country).

The malware also blocks the user from uninstalling it, restarting or shutting down the device. This is what happens when the user tries to remove Ghimob manually: video

Fallback C2s for complete remote control

Once installation is completed, Ghimob tries to hide its presence by hiding the icon from the app drawer. The malware will decrypt a list of hardcoded C2 providers from its configuration file and contact each in order to receive the real C2 address, a technique we call "fallback channels".

The C2 providers found are the same across all samples we analyzed, but the directory parameters of the request to obtain the real C2 vary among different samples, returning a different set of real C2 addresses. All of the communication is done via the HTTP/HTTPS protocol.

***Control Panel used by Ghimob for listing* infected victims**

Instead of recording the user screen via the MediaProjection API, like BRATA does, Ghimob sends accessibility-related information from the current active window, as can be seen below from the output of the “301” command returned from the C2. All the commands used by the RAT are described in our private report for customers of our Financial Threat Intel Portal.

```
1  Client:[TARGETED APP]
2  ID: xDROID_smg930a7.1.125_7206eee5b3775586310270_3.1
3  Data:Sep 24
4  2020 3:23:28 PM
5  Ref:unknown SAMSUNG-SM-G930A 7.1.1 25
6  KeySec:trueKeyLock:falseDevSec:trueDevLock:false
7  com.sysdroidxx.addons - v:3.1
8  Ativar Google Docs
9  ======================================
10 Link Conexao:hxxp://www.realcc.com
11 Senha de 8 digitos:12345678
12 Senha de 6 digitos:123456
13
14 ======================================
```

========== LOG GERAL ==========

==========

22{< x >}[com.android.launcher3]--[TEXTO:null]--[ID:com.android.launcher3:id/apps_list_view]--[DESCRICAO:null]--[CLASSE:android.support.v7.widget.RecyclerView]

22{< x >}[com.android.launcher3]--[TEXTO:null]--[ID:com.android.launcher3:id/apps_list_view]--[DESCRICAO:null]--[CLASSE:android.support.v7.widget.RecyclerView]

22{< x >}[com.android.launcher3]--[TEXTO:null]--[ID:com.android.launcher3:id/apps_list_view]--[DESCRICAO:null]--[CLASSE:android.support.v7.widget.RecyclerView]

16{< x >}[targeted app]--[TEXTO:]--[ID:null]--[DESCRICAO:Senha de 8 digitos]--[CLASSE:android.widget.EditText]

0{< >}[targeted app]--[TEXTO:null]--[ID:null]--[DESCRICAO:null]--[CLASSE:android.widget.FrameLayout]

1{< >}[targeted app]--[TEXTO:null]--[ID:null]--[DESCRICAO:null]--[CLASSE:android.widget.LinearLayout]

2{< >}[targeted app]--[TEXTO:null]--[ID:android:id/content]--[DESCRICAO:null]--[CLASSE:android.widget.FrameLayout]

3{< >}[targeted app]--[TEXTO:null]--[ID:null]--[DESCRICAO:null]--[CLASSE:android.widget.FrameLayout]

==========

========== SALDOS ==========

==========

[DESCRICAO: Rolando Lero Agencia: 111. Digito 6. Conta-corrente: 22222. Digito .7]--

[TEXTO:Account Rolando Lero]

[DESCRICAO:Agencia: 111. Digito 6. Conta-corrente: 22222. Digito .7]--[TEXTO:111-6 22222-7]

[DESCRICAO:Saldo disponivel

R$ 7000,00]--

[DESCRICAO:7000,00]--[TEXTO:R$ 7000,00]

[TEXTO:Saldo disponivel]

[DESCRICAO:Agendado ate 04/Out

R$ 6000,00]--

[DESCRICAO:6000,00]--[TEXTO:R$ 6000,00]

[TEXTO:Agendado ate 04/Out]

This is likely due to low Internet speeds in Brazil: sending text information from time to time consumes less bandwidth than sending a screen recording in real time, thus increasing the chances of successful fraud for the cybercriminal. While BRATA uses an overlay with a fake WebView to steal credentials, Ghimob does not need to do that, as it reads the fields directly from the target app through accessibility features. The following words in Portuguese are monitored: **saldo (balance), investimento (investment), empréstimo (lending), extrato (statement).**

Conclusions

It took some time for Brazilian crooks to decide to try their hand at creating a mobile banking trojan with a worldwide reach. First, we saw Basbanke, then BRATA, but both were heavily focused on the Brazilian market. In fact, Ghimob is the first Brazilian mobile banking trojan ready to expand and target financial institutions and their customers living in other countries. Our telemetry findings have confirmed victims in Brazil, but as we saw, the trojan is well prepared to steal credentials from banks, fintechs, exchanges, crypto-exchanges and credit cards from financial institutions operating in many countries, so it will naturally be an international expansion.

We believe this campaign could be related to the Guildma threat actor, a well-known Brazilian banking trojan, for several reasons, but mainly because they share the same infrastructure. It is also important to note that the protocol used in the mobile version is very similar to that used for the Windows version.

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 all of the risks that this new mobile RAT family poses. All the details, IoCs, MITRE ATT&CK Framework data, Yara rules and hashes relating to this threat are available to the users of our Financial Threat Intel services. Kaspersky products detect this family as **Trojan-Banker.AndroidOS.Ghimob**.

Indicators of Compromise

Reference hashes:
17d405af61ecc5d68b1328ba8d220e24
2b2752bfe7b22db70eb0e8d9ca64b415
3031f0424549a127c80a9ef4b2773f65
321432b9429ddf4edcf9040cf7acd0d8
3a7b89868bcf07f785e782b8f59d22f9
3aa0cb27d4cbada2effb525f2ee0e61e
3e6c5e42c0e06e6eaa03d3d890651619
4a7e75a8196622b340bedcfeefb34fff
4b3743373a10dad3c14ef107f80487c0
4f2cebc432ec0c4cf2f7c63357ef5a16

- Brazil
- Cryptocurrencies
- Financial malware
- Google Android
- Malware Technologies
- RAT Trojan
- Trojan Banker

Authors

GReAT

Ghimob: a Tétrade threat actor moves to infect mobile devices

---

Your email address will not be published. Required fields are marked *