

Fully equipped Spying Android RAT from Brazil: BRATA

SL securelist.com/spying-android-rat-from-brazil-brata/92775/



[Malware descriptions](#)

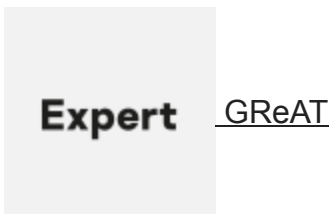
[Malware descriptions](#)

29 Aug 2019

minute read



Authors



“BRATA” is a new Android remote access tool malware family. We used this code name based on its description – “Brazilian RAT Android”. It exclusively targets victims in Brazil: however, theoretically it could also be used to attack any other Android user if the cybercriminals behind it want to. It has been widespread since January 2019, primarily hosted in the Google Play store, but also found in alternative unofficial Android app stores. For the malware to function correctly, it requires at least Android Lollipop 5.0 version.

The cybercriminals behind BRATA use few infection vectors. For example, they use push notifications on compromised websites; and also spread it using messages delivered via WhatsApp or SMS, and sponsored links in Google searches.

The first samples we found in the wild date to January and February 2019, while so far over 20 different variants have appeared in the Google Play Store, the majority of these pose as an update to the popular instant messaging application WhatsApp. The CVE-2019-3568 WhatsApp patch is one of the topics abused by BRATA threat actor. Once a victim’s device is infected, “BRATA” enables its keylogging feature, enhancing it with real-time streaming functionality. It uses Android’s Accessibility Service feature to interact with other applications installed on the user’s device.

```

private static void b(final Context context) {
    if (a == null) {
        Builder builder = new Builder(context);
        builder.setTitle("Atenção");
        StringBuilder stringBuilder = new StringBuilder();
        stringBuilder.append("Para continuar você precisa ativar o serviço de acessibilidade em <b>Serviços > ");
        stringBuilder.append(context.getString(2131427358));
        stringBuilder.append("</b> na próxima janela.");
        builder.setMessage(Html.fromHtml(stringBuilder.toString()));
        builder.setCancelable(false);
        builder.setNeutralButton("Continuar", new OnClickListener() {
            public void onClick(DialogInterface dialogInterface, int i) {
                Intent intent = new Intent("android.settings.ACCESSIBILITY_SETTINGS");
                intent.addFlags(268435456);
                intent.addFlags(32768);
                intent.addFlags(8388608);
                context.startActivity(intent);
            }
        });
        a = builder.create();
    }
    a.show();
}

```

COMMAND	DESCRIPTION
Start/Stop Streaming	Capture and send user's screen output in real-time.
Turn Off/Fake Turn Off	Can be used to turn off the screen or give the user the impression that the screen is off while performing actions in the background.
Device Information	Retrieves Android system information, logged user and their registered Google accounts, but missing permissions to properly execute the malware, and hardware information.
Request Unlock/Unlock Device	Request the user to unlock the device or perform a remote unlock.
Start Activity	Launch any application installed with a set of parameters sent via a JSON data file.
Send Text	Send a string of text to input data in textboxes.
Launch/Uninstall	Launch any particular application or uninstall the malware and remove traces of infection.

It is worth mentioning that the infamous fake WhatsApp update registered over 10,000 downloads in the official Google Play Store, reaching up to 500 victims per day.

Kaspersky products detect this family as "HEUR:Backdoor.AndroidOS.Brata"

In general, we always recommend carefully review permissions any app is requesting on the device. It is also essential to install an excellent up-to-date anti-malware solution with real-time protection enabled.

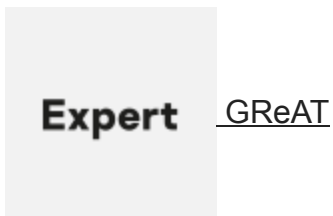
Reference md5 hashes:

- 1d8cf2c9c12bf82bf3618becfec34ff7
- 4203e31024d009c55cb8b1d7a4e28064
- 4b99fb9de0e31004525f99c8a8ea6e46

To get a complete list of IoCs along with YARA rules, please visit Kaspersky Threat Intelligence Portal <https://tip.kaspersky.com/>

- [Brazil](#)
- [Google Android](#)
- [Malware Descriptions](#)
- [Mobile Malware](#)
- [RAT Trojan](#)

Authors



Fully equipped Spying Android RAT from Brazil: BRATA

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

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm

GReAT Ideas. Green Tea Edition

17 Jun 2020, 1:00pm

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

26 Aug 2020, 2:00pm

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

22 Jul 2020, 2:00pm

GReAT Ideas. Powered by SAS: threat hunting and new techniques

From the same authors



The Verizon 2022 DBIR



Evaluation of cyber activities and the threat landscape in Ukraine



New ransomware trends in 2022



APT trends report Q1 2022

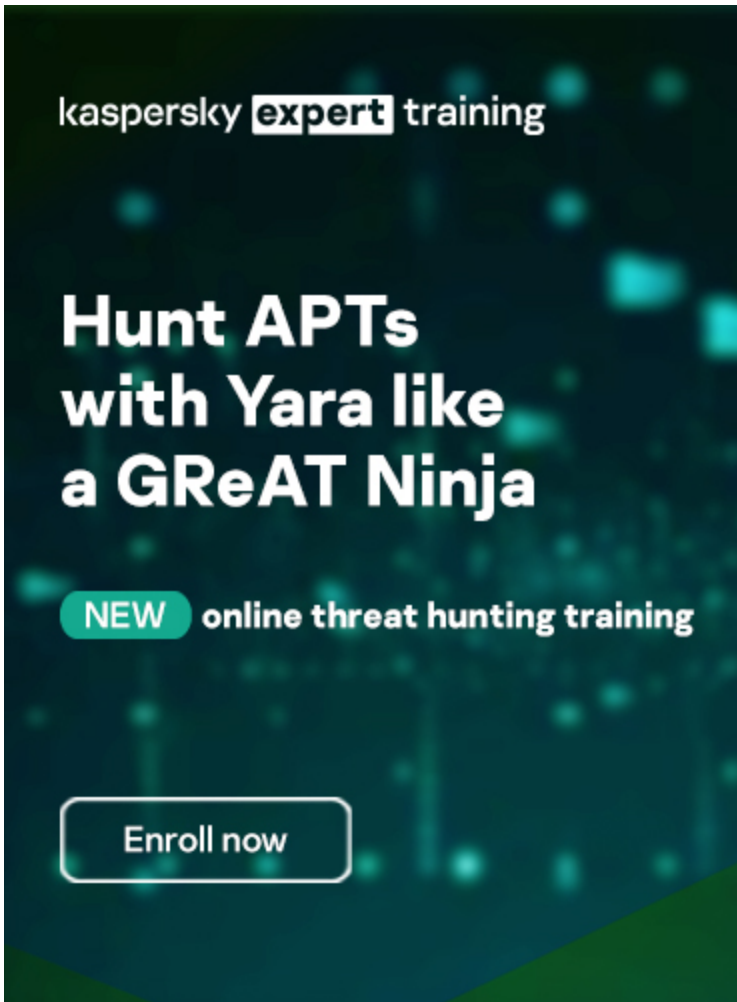


A Bad Luck BlackCat

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-



Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

A promotional banner for Kaspersky Expert Training. The background is a vibrant green with teal triangular accents in the corners. The text is in a clean, sans-serif font. At the top left, it says "kaspersky expert training" where "expert" is in a black box. The main headline reads "Improve threat hunting & reversing skills with GReAT experts". At the bottom, there is a white button with a black border that says "Learn more".

kaspersky **expert** training

**Improve threat
hunting & reversing
skills with GReAT
experts**

Learn more

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-

kaspersky **expert** training

Improve threat hunting & reversing skills with GReAT experts

[Learn more](#)