THE SAS CON

The enemy in your pocket: large-scale SIM swap fraud

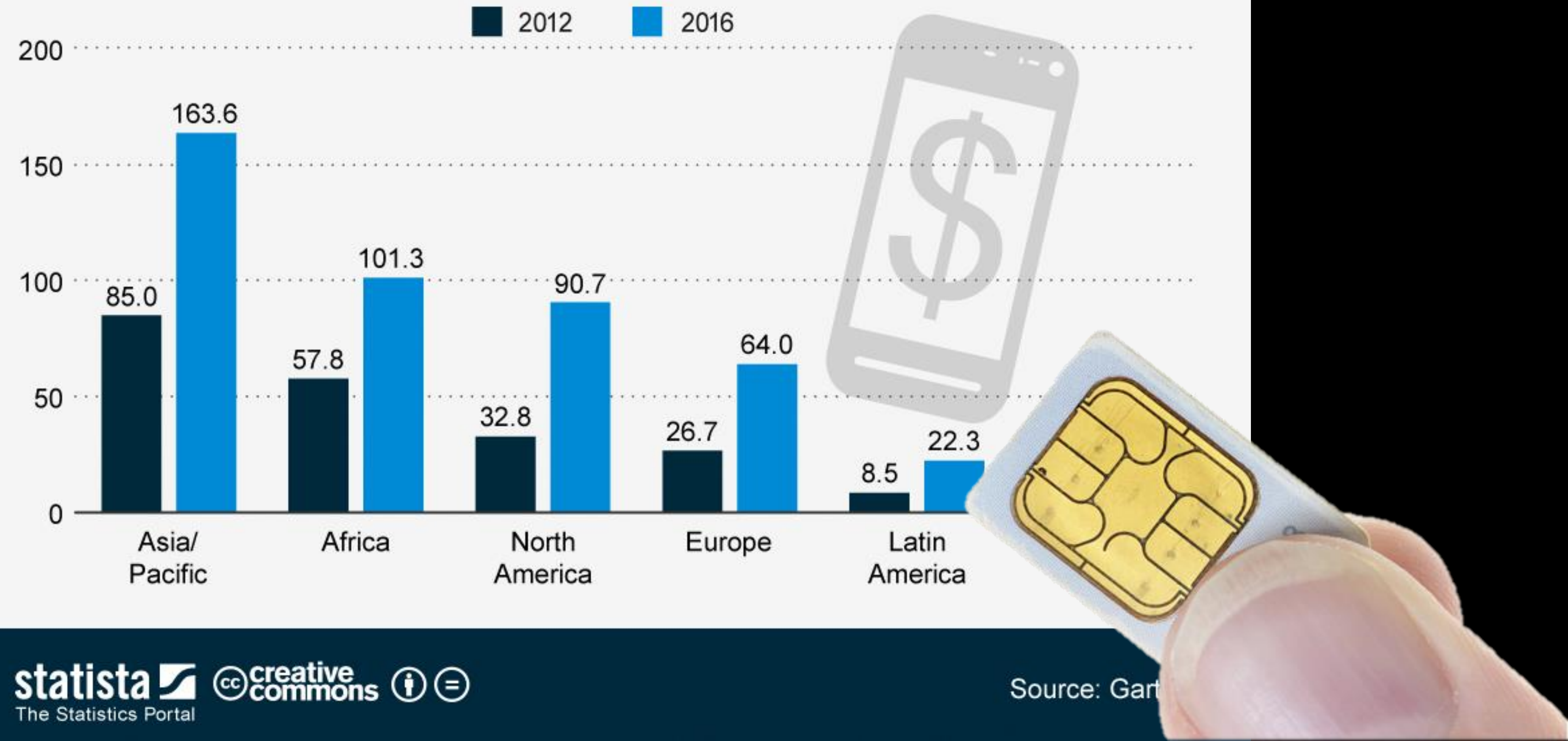
Andre Tenreiro and Fabio Assolini

CERT Mozambique and Kaspersky Lab

Mobile Payments: huge in Africa

Africa and Asia Are Embracing Mobile Payments

Forecast: mobile payment users (in millions)



statista The Statistics Portal

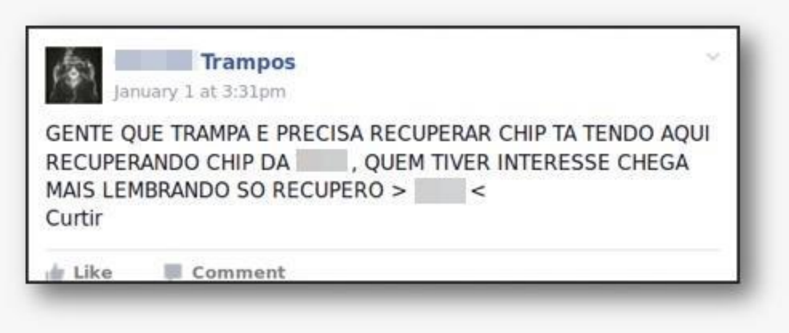
Source: Gart

How?

No Service
9:41 AM
50%
9:41
Saturday, Sept 10
This iPhone has been deactivated.
Please contact your provider.

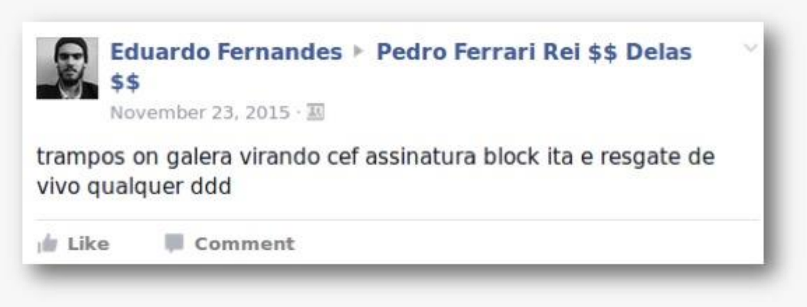
Social engineering, bribery, corruption, insiders, phishing, malware, RATs, etc…

“SIM Swap as a Service”



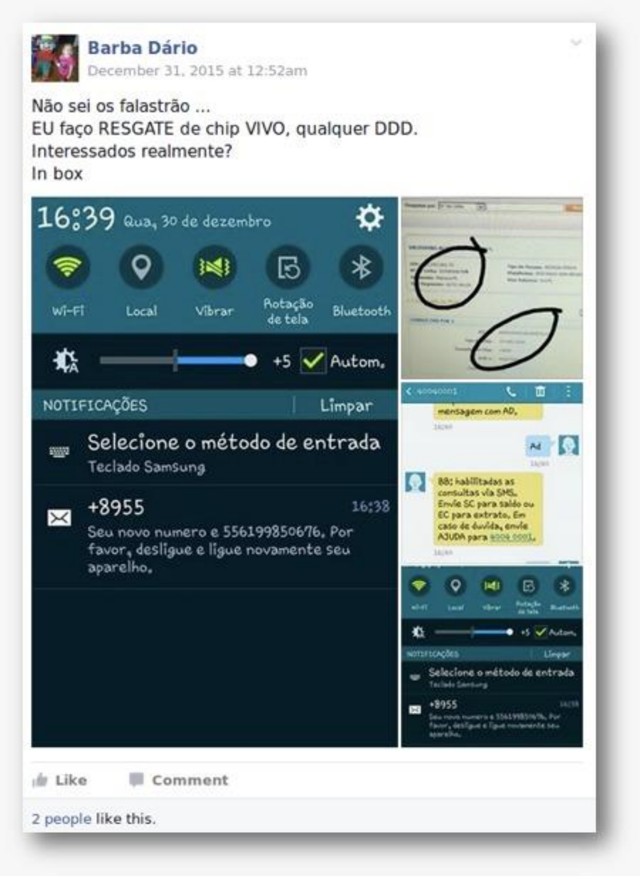
[redacted] Trampos
January 1 at 3:31pm

GENTE QUE TRAMPA E PRECISA RECUPERAR CHIP TA TENDO AQUI RECUPERANDO CHIP DA [redacted] , QUEM TIVER INTERESSE CHEGA MAIS LEMBRANDO SO RECUPERO > [redacted] <
Curtir



Eduardo Fernandes ▸ Pedro Ferrari Rei $$ Delas $$
November 23, 2015 ·

trampos on galera virando cef assinatura block ita e resgate de vivo qualquer ddd



Barba Dário
December 31, 2015 at 12:52am

Não sei os falastrão ...
EU faço RESGATE de chip VIVO, qualquer DDD.
Interessados realmente?
In box

16:39 Qua, 30 de dezembro

Selecione o método de entrada
Teclado Samsung

+8955 16:38
Seu novo numero e 5561998506676, Por favor, desligue e ligue novamente seu aparelho.

mensagem com AD,

Ad

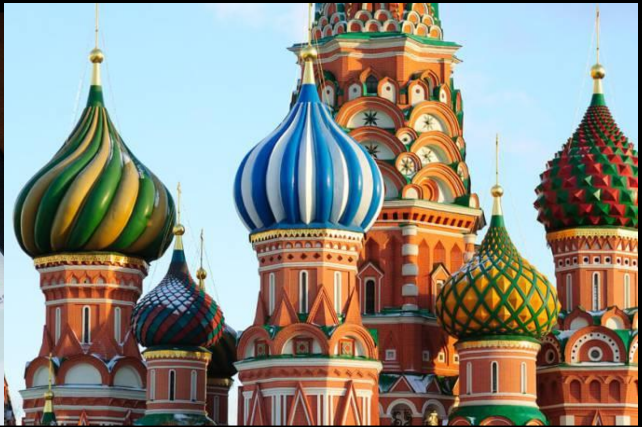
BB: habilitadas as consultas via SMS. Envie SC para saldo ou EC para extrato. Em caso de dúvida, envie AJUDA para 4004 0001.

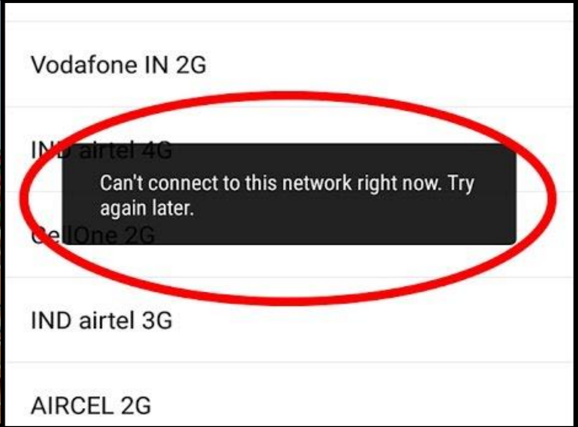
2 people like this.

Each SIM card $10 to $40

Falling victim #metoo

truecaller
Made in Sweden
Truecaller: Caller ID, SMS spam blocking & Dialer
True Software Scandinavia AB
INSTALL





Vodafone IN 2G

IND airtel 4G

Can't connect to this network right now. Try again later.

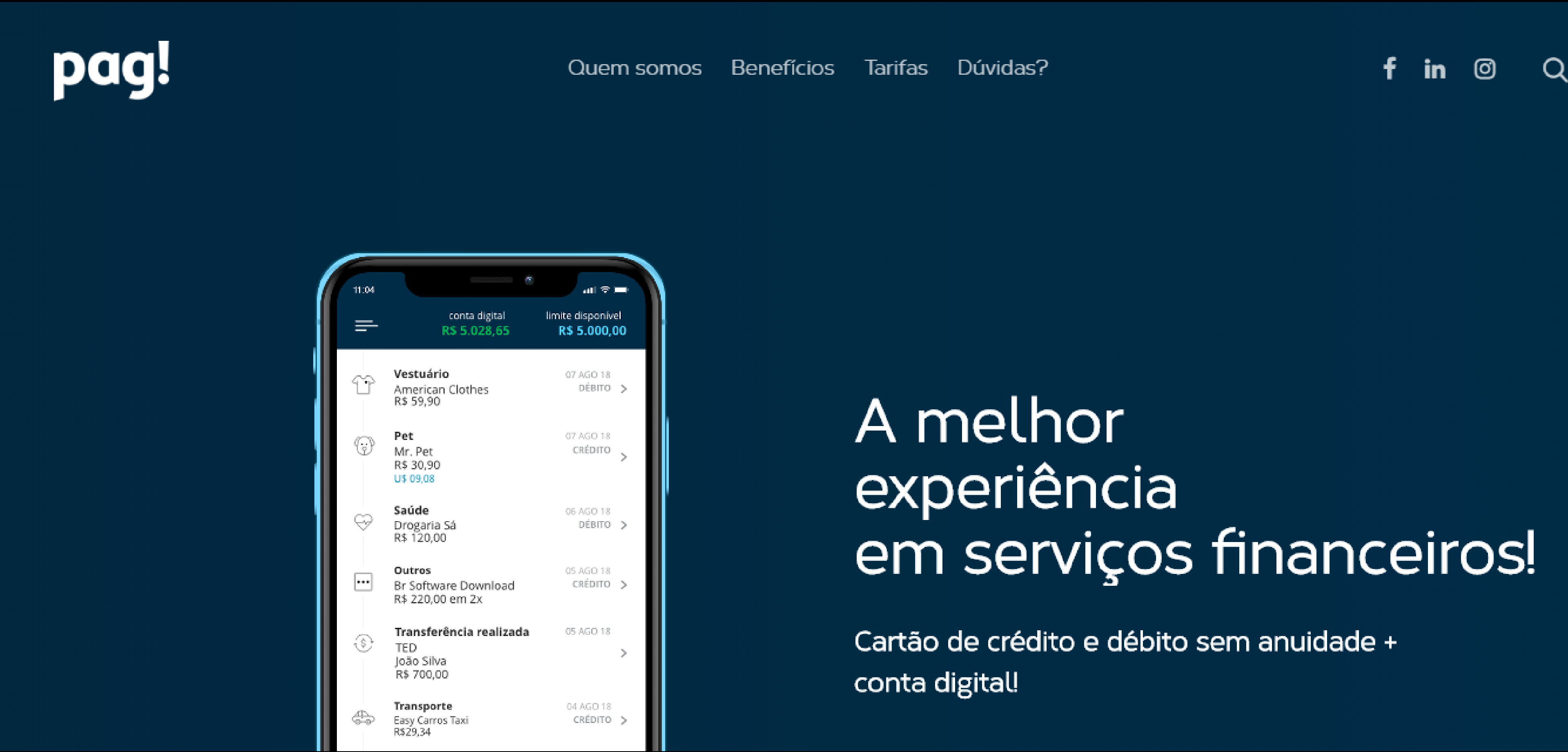
CellOne 2G

IND airtel 3G

AIRCEL 2G

Your number: TrueCaller, in a data leakage (sometimes from carriers) e-mail signature, your LinkedIn, your wife's phone, etc...

Brazil: extortion, WhatsApp, fintechs



conta digital
R$ 5.028,65

limite disponível
R$ 5.000,00

Vestuário American Clothes R$ 59,90	07 AGO 18 DÉBITO
Pet Mr. Pet R$ 30,90 U$ 09,08	07 AGO 18 CRÉDITO
Saúde Drogaria Sá R$ 120,00	06 AGO 18 DÉBITO
Outros Br Software Download R$ 220,00 em 2x	05 AGO 18 CRÉDITO
Transferência realizada TED João Silva R$ 700,00	05 AGO 18
Transporte Easy Carros Taxi R$29,34	04 AGO 18 CRÉDITO

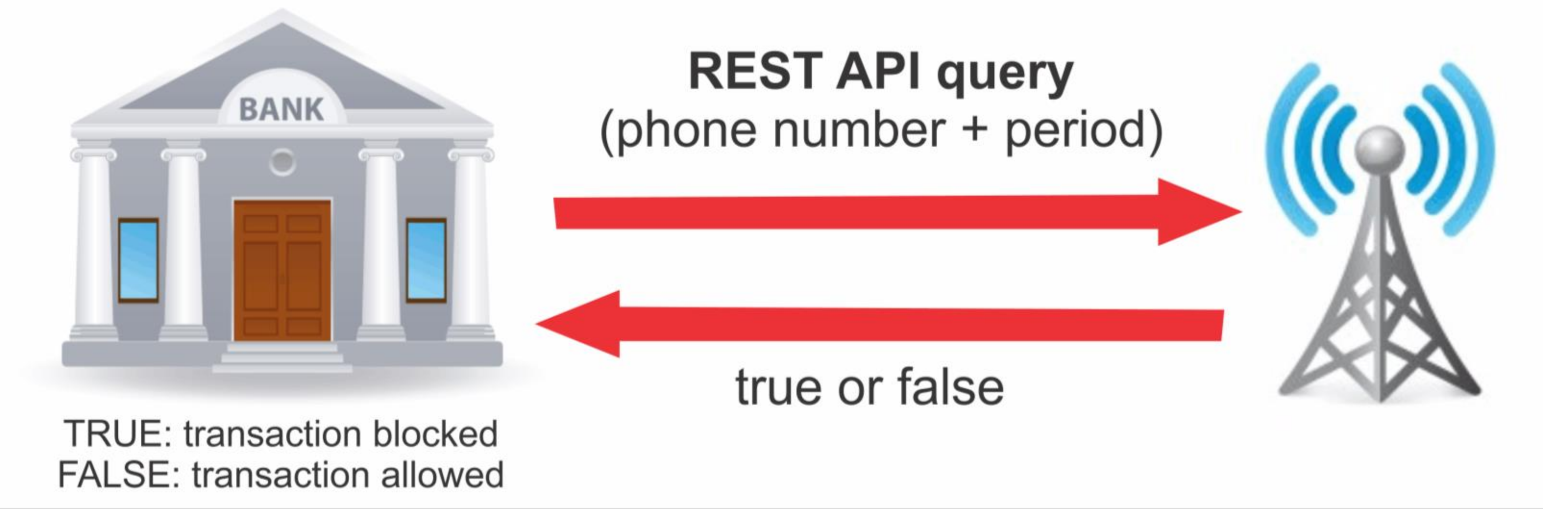
A melhor
experiência
em serviços financeiros!

Cartão de crédito e débito sem anuidade +
conta digital!

Mozambique: bribery, banks and a solution

One case: $50,000

Mozambique: platform workflow



1. The banks are connected to different mobile operators through a VPN connection so that all traffic is secure.
2. The online banking system conducts a REST API query to the respective mobile operator giving the mobile number (MSISDN) and the period (24-72 hours) as arguments.
3. The mobile operator simply returns in real time: True or False.
4. If the query is False, the bank allows the transaction as normal. If True, the bank blocks the transaction and may request additional steps to verify the transaction.

Conclusion: don’t be a victim

Carriers: Strength the processes

Banks: let OTPs via SMS die, please! In app basead OTPs are welcome!

Internet: voice password recovery? No, please!

You: 2FAs everywhere, including WhatsApp

Today: SS7? Hello spy agencies!

Future: hello e-sim and biometrics!

More details on Securelist.com tomorrow

#TheSAS2019

Obrigado!
Thank You!
谢谢

André Tenreiro and Fabio Assolini

CERT-MZ and Kaspersky Lab