BIZCOMMUNITY

What's *really* chewing up your data

By Leigh Andrews

13 Nov 2018

"I never subscribed for that, now all my data is gone!" It's a common call centre complaint, and also the basis of a highlight of the AfricaCom 20/20 track: The keynote address by Dimitris Maniatis, head of Secure-D at Upstream, who revealed the scary reality of smartphone data fraud.

Cybersecurity has long been seen as the Achilles heel of digital transformation, and Maniatis fast painted a picture of the darker side of the web, with a tightened focus for mobile operators.

You just need to turn to social media for an idea of how hidden malware depletes subscribers' data and triggers further fraudulent charges.

What's on the AfricaCom 20/20 agenda?

2 Oct 2018

Maniatis said the situation is only set to get worse, with smartphone adoption in Africa as well as the popularity of mobile transactions ever-growing. Unfortunately, Upstream data shows that almost 85% of those mobile transactions on the continent are fraudulent.

In fact, much of carrier billing is driven by malware and further incentivised by ad fraud, which impacts on end consumer.

> *"You see the charges on your device, then you complain online, as most of those R2/day subscription charges are for something you didn't actively sign up for. The subscriber doesn't know how it happened, but the operator is usually in the dark, too."*

Maniatis says the answer is **mobile malware**.

It's not going anywhere either, as it's incentivised by mobile ad spend. Nulltx confirms that Google went so far as to delist over 700,000 fraudulent apps from their Play store last year.

16 hours of work = 1Gb of data?

Emerging market consumers are still being hit the hardest. Maniatis explained, a data point is the hours of work needed to be done on minimal wage by the average consumer to earn 1GB data. In SA it is close to 16 hours, whereas it's usually just two to three hours in the US. #Datafeesmustfall

#BizTrends2018: Competition Commission's inquiry into data costs finalised in 2018

Burton Phillips 8 Jan 2018

There are still thousands of malicious applications to be wary of out there, and others that subscribe you to further digital services in the background, but Maniatis pointed out that the malware isn't always something you were tricked into downloading by an app – **malware-infected devices** are also causing data disappearance.

Maniatis says the malware sometimes sits preinstalled on your handset, ready to deplete data before you've even subscribed.

The mobile malware triple threat

You may see it as an idle app, but it's secretly downloading ad campaign content, which counts as ad fraud. This makes it a triple threat:

Your **personal info** can be leaked to servers outside the country, while **depleting your data allowance** and also adding **fraudulent charges** to airtime.

The customer gets angry and contacts their mobile data provider. If they can't track the disappearing data, this leads to higher customer churn as they're seen as 'stealing data', even though the third-party software is usually the culprit.

What to expect at AfricaCom 2018

13 Nov 2018

See above for more on what to expect from AfricaCom 2018, and follow the latest updates on KNectAfrica and the #AfricaCom2018 hashtag.

ABOUT LEIGH ANDREWS

Leigh Andrews AKA the #MilkshakeQueen, is former Editor-in-Chief: Marketing & Media at Bizcommunity.com, with a passion for issues of diversity, inclusion and equality, and of course, gourmet food and drinks! She can be reached on Twitter at @Leigh_Andrews.

- #Loeries2020: Behavioural economics as creativity, but not as we know it... - 24 Nov 2020
- #DI2020: Ignite your inner activist - representation through illustration - 27 Feb 2020
- #DI2020: How Sho Madjozi brought traditional Tsonga *xibelani* into 2020 - 27 Feb 2020
- #DI2020: Silver jubilee shines with Department of Audacious Projects launch - 26 Feb 2020
- #BehindtheSelfie with... Qingqile 'WingWing' Mdlulwa, CCO at The Whole Idea - 26 Feb 2020

View my profile and articles...