SWITCHcert Security Report

May 2014

SWITCH

I. Android to scan installed apps continually in future – fake virus scanner popular on Google's app store

Devices running Google's mobile operating system Android are to scan continually for malicious apps in future by regularly checking all installed programs for unusual behaviour using the «Verify apps» function. This is referred to as on-device monitoring. Up to now, this type of security scan has only been carried out once when an app is installed – and even then only if it did not come from Google's own app store. Google will release an update making the «Verify apps» function available to all users with Android 2.3 or higher.

The company should definitely push ahead with the rollout without delay. Analysts from FireEye recently discovered that malicious apps on Android devices can secretly attack other installed apps by exploiting their permissions, for example to manipulate user-defined links. One possible scenario is that the mobile banking icon on your smartphone, rather than linking to the correct app, might instead open a manipulated phishing version. This would allow hackers to collect users' details, the analysts warn. They were able to place an app that does exactly that in Google's Play Store without any difficulty.

Anyone wishing to protect their Android device with additional apps should choose carefully, however, since Google recently had to remove a completely ineffectual supposed virus scanner from the store. The security experts at Android Police exposed the fake security app, saying, «The only thing that it does is change from an 'X' image to a 'check' image after a single tap. »

They added that it was «disheartening» that such an obviously fraudulent program could find its way to the top of the paid apps chart on the Play Store. In an interview with the UK's Guardian newspaper, the developer said that the whole thing was a «foolish mistake» with no malicious intent. However, this useless app is not alone. Google now intends to compensate thousands of defrauded users.

Read more here:
http://officialandroid.blogspot.ch/2014/04/expanding-googles-security-services-for.html
http://www.fireeye.com/blog/technical/2014/04/occupy_your_icons_silently_on_android.html
http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/

II. US authority shuts door on net neutrality

In future, those who can afford it will be able to distribute their data packets faster on the Internet than their competitors. The US supervisory authority, the Federal Communications Commission (FCC), has laid the foundations for this to happen.
If the FCC has its way, there will be «fast lanes» for data packets on the last mile to the customer. This amounts to a de facto abolition of net neutrality, one of the very cornerstones of the Internet. The principle has hitherto been that all information is given equal priority, i.e. no one has «right of way» over others.

FCC Chairman Tom Wheeler claims that net neutrality and web fast lanes can coexist peacefully. He says that Internet service providers would be allowed to demand payment for them but not to sign exclusive deals. «Commercially reasonable» offers to rent these fast lanes would also have to be made to rival operators. The IT news portal Futurezone comments that this would still result in insurmountable hurdles for startups.

Internet pioneers, online activists and many who played an important role in the growth of the World Wide Web believe that this will pave the way towards a two-tier Internet. Craig Aaron, CEO of Freepress.net, is clear on this point: «With this proposal, the FCC is aiding and abetting the largest ISPs in their efforts to destroy the open Internet.» Michael Weinberg, Vice President of Public Knowledge, puts it this way: «The FCC is inviting ISPs to pick winners and losers online. The very essence of a 'commercial reasonableness' standard is discrimination. [...] This is not net neutrality.»

The FCC will formally vote on the new rules on 15 May. They may yet be changed, and in any case they would only apply in the US, but they could set a precedent for Europe to follow.

Further information:
http://futurezone.at/netzpolitik/offenes-internet-in-den-usa-vor-dem-ende/62.192.252
https://netzpolitik.org/2014/netzneutralitaet-in-den-usa-fcc-erlaubt-wirtschaftlich-angemessenene-zerstoerung-des-internets/
http://www.freepress.net/press-release/106177/fcc-proposal-payola-internet-would-end-net-neutrality
http://www.publicknowledge.org/news-blog/press-release/public-knowledge-statement-on-updated-net-neutrality-rules
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/netzneutralitaet-was-die-plaene-der-amerikanischen-fcc-bedeuten-12908307.html

III. Heartbleed leads to frustration and hope for open-source developers

The Heartbleed security loophole appears to have been just what was needed to raise awareness of the difficulties with some key open-source software such as OpenSSL. Companies, governments and individuals have been using free open-source programs for years without a thought for the fact that their continued development costs money.

A bug in the OpenSSL cryptographic software library, which is used throughout the Internet, meant that hackers could for two years theoretically steal secret keys, passwords and other data from affected systems. «Heartbleed is a rare bug,» says cryptography expert Matt Blaze, «a failure in a crypto library that leaks data beyond what it's protecting. So worse than no crypto at all.»
The bug was caused by a volunteer OpenSSL developer and remained undiscovered for two years.

It has now been rectified, and Internet services that were potentially under threat – including many leading names – have installed the update and taken precautions. Nevertheless, a bitter aftertaste remains: in a press release, the newly formed Core Infrastructure Initiative (CII) criticises the fact that the computer industry is increasingly reliant on open-source code, but hardly anyone wants to take responsibility for its development and funding. The CII has been set up by the Linux Foundation in response to Heartbleed and aims to provide financial support to vital open-source projects such as OpenSSL.

Steve Marquess, who describes himself as the OpenSSL Software Foundation's «money guy», is also critical of these double standards. He claims that the project is a long way short of having the money, time and people needed to maintain such as complex and critical software product. He points out that companies and governments around the world have taken the free use of OpenSSL for granted. In view of this doggedly frustrating situation, he says, «the mystery is not that a few overworked volunteers missed this bug; the mystery is why it hasn't happened more often».

At any rate, Heartbleed has succeeded in sparking some action: Cisco, Dell, Facebook, NetApp, IBM, Google and many other large corporations have now committed to donating at least USD 100,000 each to the CII over the next three years.

More on this subject:
http://www.golem.de/news/openssl-wichtige-fragen-und-antworten-zu-heartbleed-1404-105740.html
http://www.zeit.de/digital/internet/2014-04/openssl-heartbleed-core-infrastructure-initiative
http://veridicalsystems.com/blog/of-money-responsibility-and-pride/
http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel

IV. Dropbox targeting global expansion with help from Condoleezza Rice

#DropDropbox is the Twitter hashtag under which a protest against the cloud storage service Dropbox has been gaining ground since the start of April. Many incensed users, both private and commercial, are threatening to cancel their accounts, calling for a

boycott or voicing strong criticism. This follows the announcement by Dropbox's CEO Drew Houston that Dr Condoleezza Rice will sit on its Board of Directors.
As Secretary of State and National Security Advisor in George W. Bush's administration, Dr Rice was responsible for the very increase in government surveillance that made the NSA spying scandal possible in the first place. She currently runs a consulting firm together with two other former government officials.

At a time when users and companies worldwide are concerned about the close links between tech firms and the government in the US, industry insiders are not impressed by Rice's appointment to the Board. IT media around the globe are viewing it as a big PR mistake and a threat to data protection.
Houston attempted to quell the backlash on the company's blog: «Dr Rice understands our stance on these issues and fully supports our commitments to our users.» He claims that someone like the former Secretary of State is exactly what Dropbox needs to bring data protection and security issues forward.
It remains to be seen whether this will be the case with such a polarising figurehead.

Read more here:
https://blog.dropbox.com/2014/04/our-commitment-to-your-rights-and-privacy/
http://www.drop-dropbox.com/
https://news.ycombinator.com/item?id=7566069
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/datenspeicherdienst-dropbox-nutzer-empoert-ueber-berufung-von-condoleezza-rice-12891125.html

The Clipboard: Interesting Presentations, Articles and Videos

The Federal Council adopted the National Strategy for the Protection of Switzerland against Cyber Risks in June 2012. The strategy comprises 16 measures, broken down into seven spheres of action, to be put in place by 2017. A 30-page annual report is now available detailing the progress made with these measures.

http://www.news.admin.ch/NSBSubscriber/message/attachments/34670.pdf

How long does a user account remain valid in a Microsoft Active Directory after it is disabled or deactivated? Up to 10 hours, say the experts at Aorato, who have carried out extensive research into the Kerberos authentication protocol.

http://www.aorato.com/blog/windows-authentication-flaw-allows-deleteddisabled-accounts-access-corporate-data/

The SWITCHcert Security Report was written by Katja Locker and Frank Herberg.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.