SWITCH-CERT report on the latest IT security and privacy trends

November/December 2017

SWITCH

I. Dresscode for apps in the Google Play Store: malicious

«Mobile first» – the strategy of offering new services primarily for mobile device users and only secondarily developing them for desktop computers – is increasingly being adopted by cybercriminals. Recently the Google Play Store was once again a target for their activities, raising alarm in security circles. Since April 2016, the store has hosted hundreds of apps masquerading as regular games or as video or phone utility apps which in fact transmit malware known as «Dresscode». Dresscode is used for various malicious purposes: to gain access to networks and steal data, to illicitly use a device in a botnet in order to distribute other malware, spam or DDoS attacks, or to penetrate home networks via routers, where it infects other devices or manipulates smart devices in the Internet of Things.

The most recent example is «Update WhatsApp». For normal users of the store, this fake version of WhatsApp was indistinguishable from the real one. With its logo and look and feel, it was the spitting image of the original. To avoid detection, the developers simply added the Unicode %C2%Ao to the address of the WhatsApp developer ID, which couldn't be seen in the Play Store. The fake app also remained

invisible on the user's device, where a «blank icon» was installed. Even if it seems the app was «only» used to bring its developers advertising revenue, it could also be used to introduce malware to devices.

On the one hand, this shows the lengths that Google, as the operator of the store, must go to just to check the apps it offers, let alone vouch for them – a truly monumental task given the 3.3 million apps currently available in the Google Play Store. This means that cybercriminals can repeatedly launch malicious apps, implant malware or – the latest trend – mine cryptocoins.

The article from «welivesecurity.com» linked below describes the multi-tiered architecture and encryption of these malware apps and shows just how sophisticated the methods used by developers of Trojans for mobile banking, for example, can be.

The sloppy work of API developers Twilio is a completely different matter. Its programming interface (REST-API) leaves access data for apps completely unprotected and opens a gateway for attackers to read contents in their entirety. Security researchers from Appthority discovered the vulnerability in the Twilio API and established that more than 680 apps for both iOS (56%) and Android (44%) were affected.

This leaves the question of what users can do to protect themselves from this kind of malicious app, or how they can get rid of it should worse come to worst. In this event, welivesecurity.com recommends a three-phase procedure:

1) Deactivate admin rights for secretly installed payloads (e.g. Trojans)
   Go to **Settings** > (**General**) > **Security** > **Device Administrators** and search for *Adobe Flash Player*, *Adobe Update* or *Android Update*.
2) De-install the payload
   Go to **Settings** > (**General**) > **Application Manager/Apps** and search for the relevant app (*Adobe Flash Player*, *Adobe Update* or *Android Update*)
3) De-install the app obtained from the store
   Same navigation as point 2, but for other apps. Search for these names: MEX Tools, Clear Android, Cleaner for Android, World News, WORLD NEWS, World News PRO, Игровые Автоматы Слоты Онлайн or Слоты Онлайн Клуб Игровые Автоматы.

Of course, it is better not to download malicious apps from the store in the first place. However, as neither Google nor Apple are in a position to offer sufficient protection from malware apps (despite what they might claim), users have little recourse but to check the ratings and study the comments to find out more about the app. But that doesn't always help, either – the fake WhatsApp app had a 4-star rating and more than 6,000 comments.

Read more:

http://www.zdnet.com/article/fake-whatsapp-app-fooled-million-android-users-on-google-play-did-you-fall-for-it
https://uk.norton.com/internetsecurity-emerging-threats-hundreds-of-android-apps-containing-dresscode-malware-hiding-in-google-play-store.html
https://www.heise.de/security/meldung/Eavesdropper-Entwickler-Schludrigkeit-gefaehrdet-hunderte-Apps-3887665.html
https://www.welivesecurity.com/2017/11/15/multi-stage-malware-sneaks-google-play/

II. Quad9 – does it offer a data protection-friendly alternative to Google DNS?

That Google knows more about us than we know ourselves is a widespread aphorism with a kernel of truth. That's because just about everything we do on the Internet begins with a query for the IP address of a domain. Before we call up a website, send an email or load a program, a request for the relevant IP address is sent to the Domain Name System (DNS). Because the DNS has to know where to send this data, the user's own IP address is disclosed. This combination of sender data and query content is the stuff of marketing and profiling dreams. As a result, this data is a sought-after (and expensive) commodity. With its public DNS network, Google has secured itself increasingly large slices of this cake in recent years. By using Google DNS, Internet providers can save plenty of money on setting up their own infrastructure. Users «pay» for this by disclosing their own data to Google – a business model which is business as usual for Google.

Now there is an alternative to Google DNS, with a number of security and TLS encryption features designed to prevent third parties from accessing data: Quad9. The name refers to the address 9.9.9.9, which the founder-organisers IBM, PCH (Packet Clearing House) and GCA (Global Cyber Alliance) are positioning against Google's 8.8.8.8. With a present tally of 100 servers, Quad9 is aiming to offer a data protection-

friendly alternative, which the operators claim will not collect personal data or market click behaviour data. The service is financed by donations and public sector contributions.

To ensure privacy and provide protection against cybercriminality, queries can be encrypted via TLS and answered along the short route of the PCH's DNS Anycast network, which reduces the time in which attacks might occur. However, it should be pointed out that «DNS over TLS» (RFC7858) currently requires installation of a stub resolver, «stuby», or local implementation of an «Unbound DNS Resolver with DNS Forwarding». The validation of DNSSEC-signed domains prevents phishing and can make state-implemented DNS blockades visible. And when it comes to security, Quad9 can offer both SMEs and private users something they could previously only get from larger companies: filtering of DNS traffic to thwart cyber attacks. To achieve this, the security alerts and lists from 18 other filter services are integrated into Quad9, along with the DNS filter from the security service IBM X-Force.

Now, you might think that sounds too good to be true. In his blog, IT security and privacy expert Mike Kuketz points out that IBM, one of the big players in big data, is heavily involved in Quad9, and that the GCA is supported by security forces such as the New York and London police, which co-finance Quad9.

For the sake of completeness, it should be mentioned that the most secure measure when it comes to privacy and data protection is to run your own DNS resolver. As well as better response times, local resolvers also have the advantage that they usually supply better results from CDNs (content delivery network).

Read more:

https://www.heise.de/newsticker/meldung/Quad9-Datenschutzfreundliche-Alternative-zum-Google-DNS-3890741.html
https://quad9.net/#/about
https://www.kuketz-blog.de/quad9-datenschutzfreundliche-alternative-zum-google-dns

III. Uber's customer and driver data on a highway to the Dark Net

In his talks and his book «Übermorgen – eine Zeitreise in die Zukunft» («The Day After Tomorrow – A Journey to the Future»), Swiss Internet pioneer Jörg Eugster coined the term «weggeubert» («Uber-ed away») to describe companies and industries

that are unable to withstand digital disruption. We may now need to add one if not two new definitions for this term. That's because in late November it became known that data relating to 50 million passengers and 7 million drivers was stolen in a hacker attack on the car service – it was «Uber-ed away» in other words. An embarrassed Uber was not only forced to admit that the data theft had taken place, but that it had occurred in October 2016 and the company had paid the hackers USD 100,000 in exchange for assurance that the data would be deleted. Evidently the company, which has been plagued by various scandals for some time now, didn't wish to alarm the stock exchange or jeopardise imminent transactions with major investors. It therefore covered up the affair – or «Uber-ed it away». At least that was the sense conveyed by the taxi service's refusal to release the information – it informed potential investor Softbank first and didn't go public until three weeks later.

It was at this point that the State Prosecutor of New York, as well as data protection authorities from a number of countries, launched investigations into Uber. This only increased after Uber's payment to the data thieves failed to result in the promised deletion of the data, or copy cats entered the picture. Online news service thedailybeast.com reported numerous instances of fake emails from sender noreply@uberapp.com, in which Uber apologised for the hack and prompted passengers to change their passwords. The senders were even bold enough to offer the «security advice» that users should change their passwords for all their other online accounts «to avoid further damage».

In an interview in bazonline.ch, Professor Hannes Lubich from the University of Applied Sciences and Arts Northwestern Switzerland indicated that the number of known data thefts will increase in the future. Lubich, who was previously involved in the set-up and operation of the SWITCH-CERT security centre, fears this will be the case for two reasons. On the one hand, hackers can win big with low risk. On the other, new European data protection guidelines have increased pressure on companies, institutions and individuals targeted by hackers to report data theft straight away instead of Ubering it away.

Read more:

https://www.nzz.ch/wirtschaft/cyber-attacke-auf-uber-daten-von-57-millionen-kunden-erbeutet-ld.1331053
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach
https://www.heise.de/newsticker/meldung/Datenklau-Uber-informierte-erst-potenziellen-Investor-Nutzer-blieben-im-Dunkeln-3901025.html

https://www.thedailybeast.com/hackers-are-using-ubers-57-million-account-data-breach-to-steal-passwords
https://bazonline.ch/digital/mobil/Die-Zahl-der-DatenDiebstaehle-wird-ansteigen/story/27945022

IV. An earful of espionage: when headphones become listening devices

Disobedient children are often told: «open your ears!». SPEAK(a)R, a new form of spyware, relays this message on to the computer and turns its fitted (passive) headphones or speakers into microphones. In mid-August, four security researchers at the Ben-Gurion University»s Cyber Security Research Center presented SPEAK(a)R at the Usenix Workshop on Offensive Technologies (Woot ´17) in Vancouver. In the paper quoted below, they provide a detailed explanation of how the task assignment of connections can be changed with a normal audio chip. So any hacker who manages to access the computer could simply redefine headphones or speakers attached to connection sockets as microphones and record voice signals within a radius of nine metres. And the user would be none the wiser, because SPEAK(a)R can temporarily reverse the signal again to enable normal audio playback when required.

In any case, the virtual bug in the ear only works with small, non-amplified audio devices which are connected to the computer via cable. Active speakers and headphones in which the computer output signal first runs through an amplifier, or Bluetooth devices, cannot be repurposed as listening devices. That»s because both amplifiers and the Bluetooth protocol only allow sonic signals to travel through the ether in one direction.

Read (and hear) more at:

http://derstandard.at/2000063472070/Forscher-Kopfhoerer-koennen-zu-Wanze-umfunktioniert-werden
https://www.usenix.org/system/files/conference/woot17/woot17-paper-guri.pdf
https://www.youtube.com/watch?v=ez3o8aIZCDM
https://m.heise.de/security/meldung/Malware-kann-Kopfhoerer-zur-Abhoerwanze-machen-3818074.html

This SWITCH-CERT security report was written by Dieter Brecheis and Michael Fuchs.