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

July/August 2018

SWITCH

I. An own goal and serious foul: Spanish football league's app turns 10 million users into involuntarily spies

The Spanish football league, 'La Liga', scored a major own goal when the football federation's official app activated the microphone and GPS module during live broadcasts of football matches to find out whether any public screenings were taking place near the respective smartphones. To show matches, venues such as restaurants, petrol stations or campsites need to purchase a special pay TV licence from the league. If they screen a match without a licence, the league can take legal action, justified by the fact that illegal broadcasting in public spaces costs the game an estimated EUR 150 million in licensing revenue each year. However, spying in the service of the league's business interests without the knowledge of the users of the app amounts to a serious foul – not in the eyes of a referee but, instead, according to the new General Data Protection Regulation (GDPR).

Before coming into effect, there was a clause buried in the pages of the terms and conditions, which stated that the app uses the microphone for 'audience analyses'. The latest GDPR-compliant and much briefer data protection policy now states explicitly that the app is used to discover unlicensed broadcasts of the league's matches – scoring an own goal!

And the Spanish Football Federation's very inquisitive app is by no means unique in the sports world. The official app of sports broadcaster Eurosport, for instance, contacts various servers in the background and sends the location of the Android mobile device to 18 different parties. Our security report (including the last edition) has also periodically covered the topic of microphone spying on internet devices with GPS modules. And the Open Web Application Security Project (OWASP) has included these spying attacks on its list of more than 60 vulnerabilities.

Anyone who wants to prevent exposing their data has no other option than to disable the camera, microphone and geolocation services in the system settings (at least when the device is idle) or to completely remove from the device any apps suspected of spying.

Read more:

https://www.heise.de/newsticker/meldung/Spanien-App-der-Fussball-Liga-sucht-uebers-Mikro-unlizenzierte-Uebertragungen-4075636.html

https://www.blick.ch/news/ausland/handy-mik-sucht-nach-illegalen-uebertragungen-spanische-liga-spioniert-fussball-fans-aus-id8483984.html

https://www.golem.de/news/dsgvo-la-liga-app-ueberwacht-umfeld-per-mikrofon-1806-134887.html

https://www.owasp.org/index.php/Category:Vulnerability

II. Amazon Rekognition – useful security and convenience tool or total surveillance for pennies?

For some, facial recognition is a useful primary method for simplifying identification and authentication, better meeting security requirements and tracking down criminals more effectively, for example. For others, it heralds the end of our individual sovereignty over our information and is a one-way street to a total surveillance state. Because Amazon Rekognition can do far more than 'just' recognise faces, it is no surprise that opinions differ greatly on the subject.

By its own account, it can also recognise thousands of objects (e.g. bikes, phones, buildings) and settings (e.g. car parks, beaches, cities), including the activities taking place in the frame, such as refuelling a car or delivering a package. It is an AI program developed with deep learning technologies that were designed to analyse billions of images and videos each day. Amazon's advertising slogan for the product is 'Recognize one face among a million others'.

To find out just how pervasive this software-based detection is in all domains of life and for countless applications, refer to Amazon's AWS website. Civil rights organisations see the user instructions for the software as a 'manual for authoritarian surveillance'. Amazon's detractors are suspicious that Rekognition has been designed in such a way that plainly makes it a candidate for 'misuse by governments'.

Those who wish to remain anonymous on the social web and block facial recognition and image-based search should read the mimikama.at article cited below. The article describes how Canadian researchers from the University of Toronto are using artificial intelligence to pit two rival neural networks against each other: one that is constantly refining its facial recognition abilities and the other aiming to undermine just that. This sort of AI arms race has brought about the development of a nearly invisible filter that can be overlaid on images to not only disable facial recognition but also block automatic image search processes.

Read more:

https://www.nzz.ch/digital/das-gesicht-ist-das-ticket-ld.1410493
https://www.welt.de/regionales/bayern/article177883974/Gesichtserkennung-Muenchner-Polizei-setzt-jetzt-Super-Recogniser-ein.html
http://www.spiegel.de/netzwelt/netzpolitik/singapur-will-gesichtserkennung-testen-kameras-an-strassenlaternen-a-1202769.html
https://aws.amazon.com/en/rekognition
https://meedia.de/2018/04/26/datenschuetzer-caspar-die-technik-der-gesichtserkennung-birgt-unabsehbare-risiken-fuer-die-gesellschaft
https://www.tagesschau.de/ausland/amazon-gesichtserkennung-rekognition-101.html
https://eu.usatoday.com/story/tech/2018/07/09/orlando-police-decide-keep-testing-amazon-facial-recognition-program/768507002
https://www.mimikama.at/allgemein/filter-schuetzt-user

III. An underestimated risk: the number of malware attacks on smartphones and tablets is exploding

Up 54% from 2016 to 2017 and 240% since 2014 – figures an entrepreneur could only dream of. For many smartphone and tablet users, on the other hand, it is a nightmare, as the 54% jump is the increase in new types of malware for mobile devices. The 240% figure reflects a steep upward trend in the number of attacks on smartphones and tablets. Most of these are low-hanging fruit for hackers, because unlike laptop and

desktop PCs, many Android and iOS devices are very poorly guarded against attacks. Mobile security experts have found that around 24,000 malicious apps are blocked each day before they can land on smartphones and tablets – 1,000 per hour! Over 27,000 new types of malware for mobile devices were identified in 2017 alone! And even if a lot more of them were developed for Android devices, iPhones are just as desirable as targets. Add to this that, as users entrust more and more tasks to their devices, the more lucrative attacks become for hackers. The reason for this is that mobile devices are the key to the lives of users, their friends and all of the people and institutions that become interlinked via the device: Personal data, online banking logins, controls for smart environments like cars and homes, and even the workplace – both private and company networks fall prey to spying and phishing or can sometimes be used for the most outrageous break-ins or theft, including industrial espionage and sabotage.

The article cited below describes six main types of mobile malware. It also discusses how this malware finds its way onto devices in the first place. To protect their devices, users should follow the rules below:

- Only download apps from official provider stores.
- After installing, immediately check which rights have been granted to the app. Proceed with caution when the requested rights have no obvious relation to the function of the app (for instance, when an app used to keep track of your weight requests access to the camera and geolocation services or even your address book).
- Always keep your operating system and browser up-to-date.
- Avoid wifi networks from unknown operators and instead use official hotspot providers or reputable services offered by hotels or other providers.
- Set up a virtual private network (VPN) to encrypt your own network communications.

Read more:

https://www.heise.de/security/solutions/telekom/malware-angriffe-auf-smartphones-die-unterschaetzte-gefahr/?source=nat_teas

IV. Phishing with the stars: scammers take advantage of our celebrity obsession and the crypto craze to cause harm to users

Celebrity advertising is more effective than ever in 2018. Tennis aces, football heroes, music, web and business stars make millions because people want to be like them and buy the products endorsed by their idols. So it was really only a matter of time before cyber criminals latched onto the same idea and launched some extra glitzy phishing attacks.

For example, an article that recently appeared on bluewin.ch discussed just how clever scammers on Twitter were in pretending to be Elon Musk and draining crypto currencies from the accounts of unsuspecting users. Using a similar account name (elohnmusk), they started a Twitter dialogue, posing as the real Tesla founder. After a few deceptively real-looking tweets, they announced an impromptu marketing campaign that promised the payout of Ethereum and Bitcoin if users click a link and then pay a small 'verification fee' with crypto currency.

The victims of such criminal mischief are not just the users but also the celebrities themselves, whose credibility is massively undermined by such fraud.

Read more:

https://www.bluewin.ch/de/digital/betrueger-phishen-ueber-elon-musks-twitter-account-nach-bitcoins-124106.html

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