SWITCH security report on the latest IT security and privacy trends

July/August 2021

I. Perhaps 1984 WAS like *1984* – a big blunder by Apple or simply brilliant advertising?

The year is 1949. In London, George Orwell publishes *Nineteen-Eighty-Four*, a dystopian vision of a future in which a totalitarian state watches over every moment of people's lives. When Apple introduced the Macintosh computer on 24 January 1984, it showed an ad spot which went down in the advertising hall of fame. The message: 'On January 24th, Apple Computer will introduce Macintosh. And you'll see why 1984 won't be like *1984*!' Ever since, Apple has always enjoyed a reputation among the tech giants as the 'good guy', as a protector and last line of defence guarding its users' privacy. Until 5 August 2021, anyway. That's when the Cupertino-based company published a white paper entitled *CSAM Detection*, laying out its plans to step up efforts to curb the dissemination and consumption of child pornography (child sexual abuse material). This is, without a doubt, an important and valid concern. International laws already require all storage service providers to investigate signs of child pornography content on their servers and report it to law enforcement agencies. Who could object to that?

However, what Apple is now rolling out with iOS 15 and iPad OS15 amounts to an original sin, transforming Apple from the self-proclaimed guardian of personal privacy into the company that opened the floodgates of human surveillance through IT devices and the Internet of Things. The iPhone and iPad scanning essentially involves bugging the systems running on all of the company's 'i' devices to constantly look for and report illegal content.

Human history in general and IT privacy in particular has led critics to fear that reportable content will soon expand beyond child pornography to include anything deemed 'conspicuous' on the grounds that it might deviate from the desired norm. Technically speaking, there is no end to the number of imaginable scenarios. The recent and still very current case of Pegasus shows just how eager governments are to collect surveillance data, which we will return to later.

Apple responded to the massive criticism from Edward Snowden and others on Twitter by noting that there are still complex data protections in place to ensure user privacy will remain protected.

So it is all the more embarrassing that over in California they still haven't succeeded in closing the security holes that make it possible for the government spyware known as Pegasus to spy on iPhones and iPads, just as they can on devices from Apple's competitors. So when the media then reports that the 'i' company itself is becoming Big Brother and monitoring its employees with bodycams to guard company secrets, those lines from the Robbie Williams song comes to mind: 'All that's left in any case is advertising space.'

Read more:

https://www.digitec.ch/de/page/apple-neuralhash-gegen-privatsphaere-die-buechse-der-pandora-wird-geoeffnet-20759

https://www.heise.de/meinung/Totalueberwachung-durch-die-Hintertuer-Apples-fataler-Suendenfall-6157251.html

https://www.tagesschau.de/ausland/apple-kritik-foto-funktion-kinderpornos-101.html

https://www.chip.de/news/Snowden-kritisiert-Apple-scharf_183756528.html

https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/

https://www.t-online.de/digital/sicherheit/id_90484688/pegasus-luecke-in-iphones-noch-immer-angreifbar.html

https://www.giga.de/news/apple-als-big-brother-mitarbeiter-sollen-body-cams-tragen/

https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life

II. Pegasus: what IT users can learn from the ancient Greeks

In the pantheon of Greek mythology, Pegasus was the winged horse whose heroic deeds included supplying two powerful weapons of destruction – thunder and lightning – to the mightiest of Greek gods, Zeus. Part of the dirty day-to-day surveillance work carried out by governments and intelligence agencies involves a piece of government spyware known as

Pegasus. The software used by many world leaders is a highly functional spying tool, extremely hard to detect and even harder to disable, and it helps them spy on and even track down their targets.

The software is made by the Israel-based NSO Group, whose ethos is reflected not only in the company's slogan of 'Cyber Intelligence for Global Security and Stability' but also in the name's similarity to NSA, the highly secretive intelligence agency in the United States. It seems quite naive to believe NSO's claims reassuring that Pegasus is intended exclusively to combat criminals and terrorists. This is decidedly not the case as confirmed by a list leaked to Amnesty International and the non-profit media organisation Forbidden Stories. The list contains more than 50,000 phone numbers of businesspeople, politicians, journalists, scholars, union leaders, prominent religious figures and government dignitaries, including cabinet members and heads of state. *The Guardian* also reported that Pegasus had apparently been used by a Mexican client to spy on and hunt down the reporter Cecilio Pineda Birto. A few weeks after his smartphone was infected with the NSO spyware, Pineda was found murdered – his phone was nowhere to be seen. NSO has denied playing any role whatsoever in Pineda's murder. However, the reporter had clearly been made a surveillance target along with 24 other Mexican journalists. With more than 15,000 phones under surveillance, Mexico is considered the biggest user of Pegasus, followed by Morocco and the United Arab Emirates, which have both used Pegasus some 10,000 times. To make matters worse, the government of one EU country also appears on the leaked NSO client list. To the surprise of no one, Hungary's intelligence agencies appear to have used Pegasus to systematically spy on 300 critics of Viktor Orbán since 2018.

One could say that Pegasus has transformed from a mythical figure into a murky – and in some cases deadly – player in real-world espionage. Another myth appears to be disintegrating as well – the superiority of native security mechanisms on iPhones and iPads. After all, they were left just as exposed to Pegasus attacks as Android devices. In late July, this prompted Matthew Green, a cryptologist and associate professor of IT security at Johns Hopkins University, to point out that Apple's iMessage service offered some 'really bad' attack vectors. There are growing complaints that the company is unable or unwilling to patch the security holes and is instead shipping devices with NeuralHash CSAM detection (see first section), setting the conditions for total surveillance via smartphone and tablet. It would appear that Pegasus has brought thunder and lightning to Cupertino as well.

Read more:

https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

https://www.dw.com/de/pegasus-skandal-kein-system-ist-sicher/a-58705194

https://www.heise.de/news/NSO-Skandal-100-Organisationen-fordern-Verkaufsstopp-fuer-Spyware-6149195.html

https://www.nzz.ch/international/pegasus-in-ungarn-ausspionierte-orban-kritiker-kein-dementi-ld.1636774?reduced=true https://www.heise.de/news/Pegasus-Sicherheitsforscher-fordert-Apple-zu-besserer-iPhone-Absicherung-auf-6144134.html

https://www.heise.de/meinung/Kommentar-Apple-setzt-die-falschen-Prioritaeten-6158007.html

III. The biggest hack in cryptocurrency history – finger-wagging or hacker vanity in its purest form?

Initial reports of a hack of colossal proportions blended fascination with horror – an unknown hacker made off with more than USD 600 million in various cryptocurrencies through a cyber-attack on Poly Network. The relatively low-profile company, which makes software for swapping data between different blockchains, particularly the transfer and conversion of various cryptocurrencies, was forced to report the incident to the public on 11 August via Twitter. The cybercriminals had discovered a serious security hole in the protocol and exploited it to replace the addresses of tens of thousands of customers with its own and redirect massive sums to its own accounts: USD 273 million in Ether from the Ethereum Blockchain, USD 253 million from the Binance Smart Chain and approximately USD 85 million from the Polygon network (for technical details, follow the link to SlowMist below).

Several hours after Poly Network's first tweet, the company posted a second tweet directed at the hackers, demanding that they return the loot and contact the company or face aggressive prosecution. Meanwhile, crypto-security researchers at Elliptic had reported that a large portion of the stolen money had been returned. Elliptic co-founder Tom Morrison explained that the sum was too large to launder without raising red flags. The transparency of blockchain technology was another reason.

Immediately after the hack was discovered, the crypto community had, in fact, started hunting for the thief or thieves and the loot. For example, the security firm SlowMist said that shortly after the second Poly tweet, the mailbox, IP and activity traces were identified on the hacker's smartphone. They were said to have carried out several currency conversion transactions, mainly on the Chinese crypto exchange Hoo. Additional information about the hacker was also shared with Poly Network, and disaster was ultimately averted.

The hacker has since returned nearly all of the loot but has not revealed his identity. On the contrary, he offered a personal reward to any hacker able to successfully identify him within a month.

He also turned down Poly Network's offer of USD 500,000 and immunity from prosecution for helping discover and close a grave security hole. Poly Network now refers to the hacker as 'Mr. White Hat', reflecting the company's belief that the hack was carried out with good intentions. The unidentified person with the white hat and black waistcoat had already announced in a three-page Q&A that he was not interested in money but rather in exposing vulnerabilities in the Poly Network software. Tom Robinson tweeted the Q&A. It came as a complete contrast to one of the hacker's previous tweets in which he expressed his regret that 'it would have been a billion hack if [he] had moved remaining shitcoins!' to his accounts in time. It will be interesting to see whether the mystery is ever solved.

Read more:

https://www.tagesschau.de/wirtschaft/finanzen/krypto-waehrung-diebstahl-hacker-angriff-ethereum-binance-polygon-101.html
https://blockchainwelt.de/poly-network-hack-mindestens-611-millionen-usd-wurden-gestohlen
https://bitcoinist.com/biggest-heist-in-defi-how-a-hacker-stole-600-million-from-poly-network
https://www.btc-echo.de/news/poly-network-hacker-zahlt-fast-alles-zurueck-und-teasert-mit-seiner-124042
https://www.tagesanzeiger.ch/hacker-erbeuten-ueber-600-millionen-dollar-aus-spass-rueckzahlung-laeuft-417830762835
https://www.manager-magazin.de/finanzen/geldanlage/poly-network-krypto-hacker-gibt-beute-zurueck-und-zitiert-martin-heidegger-a-4f8b2e0c-1f81-4212-bf01-aef637f5422a
https://slowmist.medium.com/the-root-cause-of-poly-network-being-hacked-ec2ee1b0c68f
https://www.youtube.com/watch?v=MfW7jUqLZ7Q
https://www.youtube.com/watch?v=O6M2JuIsCrQ

IV. In bed with Siri, Alexa and Uber – what is the privacy and data security situation for working from home?

During the exceptional situation of lockdown, many people got to experience what passes for a normal day for some of us: working from home. This has always been an alternative for many people. As society transformed from an industrial to a service-based economy, more and more companies have begun to outsource their telecommunications services, such as customer service or telemarketing, to specialist companies which have employees who provide these services from their own homes. In less wealthy countries, in particular, employees do not always have an office and often have to make do with a kitchen, children's room or bedroom.

This would not be fodder for Security Report if privacy and data security were not so relevant here as well. But these issues really began piling up once people started switching from purely phone-based service to the transmission of audio-visual content and two-way communication between smart devices and voice assistants. A few years back, for instance, we reported that 'Hello Barbie' was recording children's conversations with a smart doll and sending the data to the manufacturer, Mattel, which analysed the content and sent parents weekly bulletins on their child. Luckily, parents can disable this feature – an option unavailable to the employees of many companies.

NBC News reported in early August, for example, that big tech companies like Apple, Amazon and Uber have been outsourcing their customer service to tele-performance providers which are using camera(s), microphone(s) and AI-driven surveillance software to monitor staff working from home. NBC cited a leaked employment contract from a Colombian employee working for French call centre operator Teleperformance, which works as part of Apple's service team. The contract states that the company is allowed to use the aforementioned technologies to monitor the woman while she is working from home, regardless of the room in which the workspace is located. While Apple has dismissed the report as false, an Amazon spokeswoman stated that the company had not sought to carry out 'any additional' surveillance of employees working from home. The fact that Amazon keeps a close eye on its employees is nothing new: its delivery vehicles are fitted with four HD cameras to monitor the traffic situation, driver conduct and the delivery of the packages.

As the number of networked surveillance devices increases, so does the risk that devices – often poorly encrypted – will create a wide-open door for hackers to invade the privacy of naive users. For example, the Mississippi-based news platform WMC5 reported that the Amazon Ring camera used by two parents to monitor their child's room had been hacked to play songs for their eight-year-old daughter and talk to her. The parents admitted that they had indeed neglected to enable two-factor authentication, which would have made it more difficult for the hackers to gain access to the system. The vice.com IT blog Motherboard also covered the incident and reported on other spying attacks using Amazon Ring in other states. Motherboard warned that its own research on the dark web had turned up multiple forums in which cybercriminals were found discussing the best ways to hack Ring cameras.

Amazon, which makes Ring, responded to the incident by urging all users to enable two-factor authentication instead of using Ring's 'Shared users' feature to log in, to use strong passwords and to change them regularly.

Even 72 years after the release of Orwell's *1984*, the issue of security versus privacy is as relevant as ever.

Read more:

https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227

https://www.golem.de/news/apple-amazon-uber-callcenter-ueberwachen-angestellte-mit-kameras-im-homeoffice-2108-158804.html

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05_de.pdf

https://futurezone.at/digital-life/hacker-spionieren-mit-kameras-von-amazon-ring-kinderzimmer-aus/400703223

This SWITCH security report was written by Dieter Brecheis and Frank Herberg.

The SWITCH security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH assumes no liability for the content or opinions presented in the security report nor for the correctness thereof.