SWITCHcert Security Report

October 2015

SWITCH

I. XcodeGhost and Stagefright hit industry heavyweights Apple and Google and pose questions

Security researchers at Zimperium zLabs discovered seven vulnerabilities in Android's Stagefright multimedia interface at the end of July. They allowed attackers to use a text message or video to block devices running Android versions below 5.0 – an estimated 80% of all Android mobile devices – completely or even use them as bugs. Google initially responded to Zimperium's warnings only with a general announcement that it would introduce a regular monthly patch day. The zLabs staff then published a working exploit at the start of September so as to step up the pressure on Google to eliminate the loopholes. The first security updates have since been made available, but Zimperium's researchers have already discovered a new weakness in Stagefright 2.0 that makes it possible to deliver malware to a device with the aid of MP3 or MP4 files.

Security firm Palo Alto Networks found even more holes in apps from Apple's App Store. Chinese developers in particular had substituted Apple's original Xcode development environment with a compromised version created by Chinese hackers. It is currently hard to gauge how many apps are infected in total. When XcodeGhost was first discovered, 39 was the number mentioned, but security experts at FireEye claim

that it could be more than 4,000. Since this includes some very popular apps such as WeChat, it is likely to affect several million users. This has damaged confidence in the security of the App Store from Cupertino, which has up to now been seen as exemplary. Apple has informed all developers about the vulnerabilities and asked them to update their apps using the original Xcode. It says that all of the apps concerned that it knows about and have not been updated have been removed from the App Store, and new apps containing XcodeGhost are blocked.

Compared with the scope of Stagefright and XcodeGhost, the – successful – attempts to hack the lock screens of iOS and Android devices almost pale into insignificance. Nevertheless, they are further grounds to believe that mobile security still needs improving.

Read more here:

http://www.nzz.ch/digital/stagefright-exploit-zimperium-zlabs-ld.1896
http://www.spiegel.de/netzwelt/gadgets/android-neue-gefahr-durch-sicherheitsluecke-stagefright-2-0-a-1055865.html
http://www.heise.de/security/meldung/Malware-in-Apples-App-Store-Wie-XcodeGhost-funktioniert-2824035.html
http://www.darknet.org.uk/2015/09/xcodeghost-ios-trojan-infected-over-4000-apps
http://www.theregister.co.uk/2015/09/23/xcodeghost_analysis
http://www.nzz.ch/sperrbildschirm-siri-ios-9-austricksen-ld.2138
http://www.golem.de/news/nach-malware-infektion-apple-raeumt-den-app-store-auf-1509-116473.html

II. BÜPF, NDG and government Trojans – debate on sense, senselessness, costs and risks of state surveillance enters next round

August's Security Report contained a detailed account of the affair surrounding the Swiss authorities' purchase of the «Galileo» government Trojan from Italian firm Hacking Team. Even after it emerged that the Trojan, which cost over half a million Swiss francs, could not actually be used because the provider itself had been hacked and that Hacking Team's clients apart from Switzerland include various dictators, rogue states and people with links to the eastern European Mafia, government circles still seem convinced that they acted correctly in procuring Galileo. In addition to the above concerns, however, critics of the use of government Trojans point out that state-sponsored hacking literally throws the door wide open to cybercriminals without

bringing any tangible benefits. They say that the Hacking Team hack proves the bad guys have access to the same software as the people who want to use it to stop them and that many Trojans – Galileo included – are designed such that the data they capture are easy to fake and thus have no value as evidence.

In adopting the Federal Act on the Surveillance of Post and Telecommunications (BÜPF) on 17 June 2015, the National Council has now given the green light in principle for government Trojans to be used in Switzerland. In parallel with this, the new Intelligence Service Act (NDG) also gives Swiss spy agencies much greater powers to listen in on, intercept and store communication data and content. Rainer J. Schweizer, a professor of public law, believes that this legislative package marks a fundamental paradigm shift that will ultimately curtail media freedom to a considerable degree.

Critics of both BÜPF and NDG have launched an initiative to hold a referendum on abolishing the NDG. Berner Zeitung also sees a referendum as desirable in view of the experience with personal dossiers, since a «yes» to the new legislation would cast aside doubts over the legitimacy of the Federal Intelligence Service.

It remains to be seen whether privacy will remain a right worth protecting in future or, in the words of Gottlieb Duttweiler Institute futurologist Karin Frick, whether it will be overstated in political debate and the media but eroded in the interests of convenience.

Read more here:

http://www.computerworld.ch/news/it-branche/artikel/zuercher-regierungsrat-nimmt-stellung-zum-staatstrojaner-von-reue-keine-spur-68658
http://www.computerworld.ch/news/politik-gesellschaft/artikel/falscher-staatstrojaner-kapo-zueri-wird-lukrative-ware-fuer-cyberkriminelle-68790
https://www.digitale-gesellschaft.ch/2015/06/08/offener-brief-zum-ndg
http://www.tagesanzeiger.ch/schweiz/standard/Wir-schaffen-da-eine-geheime-Staatsgewalt/story/21297019
http://www.nzz.ch/schweiz/aktuelle-themen/gegner-des-nachrichtendienstgesetzes-lancieren-referendum-1.18620992
http://folio.nzz.ch/2015/oktober/haendler-ohne-waren
http://www.bernerzeitung.ch/schweiz/volksentscheid-zum-nachrichtendienstgesetz-wuenschenswert/story/16492264

III. Privacy B2B – growing number of attacks on SMEs and critical infrastructure

While many individuals appear increasingly uninterested in protecting their own privacy, more and more organisations are claiming that privacy is essential to their survival. Companies and operators of critical infrastructure such as power stations, electricity grids, authorities, hospitals etc. are facing a growing onslaught of ever more malicious cyberattacks. These destroy or compromise control systems, fish out communication details that could be used by rival firms to scupper a takeover bid, and steal information on prototypes, clients, corporate strategies and more.

Experts are increasingly pointing out that cyberattacks are no longer directed solely at the big names but also target small and medium-sized enterprises, for instance to undermine their online presence or Google score. Besides IT and security experts, major consulting firms including KPMG are now also giving warnings about the steady growth in networked products and cluster risks concerning attacks on whole areas of infrastructure like power supply. German legislators responded in mid-June 2015 with a new law on IT security that stipulates new requirements in terms of measures to avert cyberattacks and to report them when they happen. The extent of demand in this field is illustrated by a «honeypot» case in Sonntagszeitung, where a simulated hydroelectric power station server recorded several serious attacks in the space of just three weeks: «One hacker from Vietnam attempted to crash the whole system; two attackers from the US and one from Romania [...] faked a fault in the fictitious plant that could have caused a pump to cut out suddenly.»

Read more here:

http://www.zeit.de/digital/2015-09/industrie-hacker-sicherheit-digitalisierung
http://www.faz.net/aktuell/wirtschaft/unternehmen/der-schaden-durch-hackerangriffe-wird-immer-groesser-13331689-p2.html
https://home.kpmg.com/de/de/home/themen/2014/08/industrie-4-0-wie-hacker-in-industrie-it-eindringen.html
http://www.computerwoche.de/a/security-konzepte-im-praxis-check,3211303
http://www.trendmicro.de/media/wp/industrie-4-und-die-sicherheit-whitepaper-de.pdf
http://www.computerwoche.de/a/bundestag-beschliesst-das-it-sicherheitsgesetz,3210652
http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051
http://blog.kpmg.ch/cyberangriffe-auf-schweizer-wasserkraftwerke-was-man-darueber-wissen-sollte

IV. Fingerprints of at least 5.6 million US federal employees stolen – who cares?

We covered the cyberattacks on the US Office for Personnel Management (OPM), in which personal details and security reports concerning over 21 million federal employees were stolen, back in August. It has now been revealed that a huge number of fingerprints fell into the cybercriminals' hands. Whereas a figure of 1.1 million was originally quoted, the official number is now 5.6 million. As well as unlocking personal mobile phones, these fingerprints might be used for access to federal facilities. The OPM published a statement at the end of September attempting to play down the threat posed by this theft, but the consequences of biometric data theft can be grave. One person who thinks so is Alan Woodward, computer scientist at Surrey University and security advisor to Europol: «If [people] can actually steal something that is unique, like fingerprints, and somebody is relying upon it, then it's just going to cause a nightmare – it really is». Once again, we must note that biometric «passwords», once stolen, are very hard to replace.

Read more here:

https://netzpolitik.org/2015/opm-hack-noch-mehr-fingerabdruecke-von-us-bediensteten-betroffen
http://www.zdnet.com/article/the-opm-breach-deepens-5-6-million-federal-employees-fingerprints-stolen
https://www.opm.gov/news/releases/2015/09/cyber-statement-923
http://www.bankinfosecurity.com/stolen-opm-fingerprints-whats-risk-a-8548
https://www.ccc.de/de/updates/2008/schaubles-finger

V. DIY 007 – Deep Sweep project spies on satellite communications

It is somewhat reminiscent of the «Spy vs. Spy» cartoons from the glory days of MAD magazine: the self-styled Critical Engineering Working Group led by media artist Julian Oliver has developed a probe laden with high-tech equipment to capture high-altitude radio transmissions and visualise them on zeigma.com. Oliver hopes that the probe will find radio signals between military drones and satellites, even though he knows that they are encrypted. He explained to WIRED magazine that the main idea is to supply information on radio chatter at high altitudes that earthbound amateur radio

enthusiasts cannot receive. The first attempt yielded no data, however, and the second saw the probe reach an altitude of only 10 km, far short of the 24-30 km target. The project still has some way to go – literally.

Read more here:

http://www.heise.de/make/meldung/Hacker-starten-Stratosphaerenballon-um-Drohnen-Funk-mitzuschneiden-2823100.html
http://zeigma.com/deepsweep
http://www.wired.com/2015/09/balloon-spy-probe-deep-sweep
https://criticalengineering.org/projects/deep-sweep
http://www.20min.ch/digital/news/story/Hacker-spionieren-mit-Ballon-Militaer-Drohnen-aus-30099780

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.