SWITCHcert Security Report

January / February 2017

SWITCH

I. The Guardian going post-truth with WhatsApp story?

Since 1821, UK daily The Guardian has been synonymous with independent, reliable, liberal journalism for progressive, intellectual readers. The London-based imprint has been named National Newspaper of the Year at the British Press Awards four times. Its website theguardian.com has up to now been seen as a serious source of news, including news on IT security and privacy. However, in an exclusive on 13 January 2017, theguardian.com claimed that a back door in WhatsApp's end-to-end encryption, which had been thought infallible, allowed intelligence services to intercept messages. The Guardian referred, among other encryption and security experts, to the crpyto and security researcher Tobias Boelter of the University of California in Berkeley, who claims on his own blog «tobi.rocks» to have discovered the vulnerability back in April 2016 and reported it to Facebook. It was not fixed, and Boelter's blog entry of 13 January 2017 states that WhatsApp declared it to be a feature for rare transmission problems rather than a bug. Boelter, together with other researchers quoted in the Guardian article, sees this as proof that WhatsApp has deliberately left this loophole open as a back door for intelligence services.

«There is no WhatsApp backdoor,» said Moxie Marlinspike, crypto expert and co-author of the Signal encryption protocol used by WhatsApp, on the website whispersystems.org on the same day as the Guardian report. The story has been

making waves ever since. On the blog technosociology.com, Zeynep Tufekci, tech author and Associate Professor at the University of North Carolina, accused The Guardian of irresponsible reporting. She said the vast majority of encryption and security experts agree that the vulnerability is not a back door but a security feature that makes it easier to use WhatsApp on a daily basis to the extent that a negligible risk is acceptable. To underscore this claim, Tufekci attached the signatures of well over 50 experts to her entry. Other posts on security blogs and websites from Naked Security to techcrunch.com have echoed Tufekci's criticism and calls by various researchers for The Guardian to retract its article. The paper did respond, but merely by replacing the term «backdoor» in the headline with «vulnerability». Mohit Kumar, founder and CEO of the The Hacker News, argues that this entirely fair. He points out that security experts, WhatsApp and Facebook have all failed to deny that government agencies could potentially read WhatsApp messages.

This is where ZITiS, the German government's new central IT security body for law enforcement and intelligence, comes in. Its main job is to decrypt encrypted online communications from WhatsApp and other messaging services so that the authorities can read them. By 2022, some 400 people are expected to be working for it in Munich, paid for with the tax euros of the citizens it spies on. The location was probably chosen as favourable for recruiting the right people, given that a number of firms already based there specialise in government-sponsored Trojans and other surveillance software.

Read more here:

https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages
https://tobi.rocks/2017/01/whatsapp-vulnerability-bug-or-backdoor
https://whispersystems.org/blog/there-is-no-whatsapp-backdoor
http://technosociology.org/?page_id=1687
https://nakedsecurity.sophos.com/2017/01/16/whatsapp-backdoor-turns-out-to-be-known-design-feature
https://threatpost.com/why-whatsapps-backdoor-isnt-a-backdoor/123113
http://www.golem.de/news/sicherheitsbehoerde-zitis-soll-von-muenchen-aus-whatsapp-knacken-1701-125722.html

II. Fruitfly spyware lives long on Macs

Fruitfly is a type of spyware that was only recently discovered attempting to spy on Macs in biomedical research institutions but uses surprisingly old functions that predate OS X Yosemite. At least, this was the claim made by Thomas Reed, security researcher at Malwarebytes, in his company blog entry on 18 January 2017. Reed had found that the malware, dubbed Fruitfly by Apple, tries to create screenshots, access built-in or connected webcams and send hacked data to the attackers' servers. Once it has taken a bite of the Apple, it is also capable of controlling an infected Mac remotely. However, it is unclear how it infects them in the first place. What is clear is that it also includes Linux shell commands, meaning that it may have Linux variants that have not yet been discovered. Apple has now released a security patch to protect against Fruitfly.

Read more here:

https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code
https://www.heise.de/security/meldung/Fruitfly-Apple-Update-soll-Spionage-Software-blockieren-3603628.html
http://www.macnotes.de/2017/01/22/fruitfly-apple-vertreibt-update-gegen-spionage-malware
http://thehackernews.com/2017/01/mac-os-malware.html
http://www.giga.de/downloads/macos-sierra/news/fruitfly-macos-malware-blieb-anscheinend-jahrelang-unentdeckt

III. Good malware – FBI in absurdity trap

All the world's law enforcement agencies justify the use of state-sponsored malware with the argument that, as well as terrorists, drug dealers and violent criminals in general, it allows them to stop child abusers or at least bring them to justice. A current case in the US shows the sort of grotesque situation that can arise from this argumentation. A ring of suspected paedophiles uncovered using FBI malware had to be released because the FBI was unwilling to comply with the court's request to disclose the malware's source code. It had used the code to find the IP addresses of suspected paedophiles who had used the Playpen platform via the Tor network to share and trade images of abused children until the FBI closed it down. In all, 135 people were prosecuted. Some signed confessions, while others successfully argued that the evidence against them had been collected illegally. The court asked the FBI to disclose its source code in at least one case. Caught in the dilemma between

convicting a suspected criminal and continuing to use the malware, the FBI decided to protect its source code and thus stopped the prosecution.

The question remains as to how much sense it makes to use software to catch criminals if those criminals have to be set free again because the software would otherwise be rendered useless. This is the kind of logic only the authorities can grasp. According to gizmodo.com, they claim that their malware is not really malware because it is used by the good guys in a good cause.

Read more here:

http://www.golem.de/news/um-eigene-malware-zu-schuetzen-fbi-laesst-paedokriminellen-laufen-1701-125496.html
https://arstechnica.com/tech-policy/2017/01/feds-may-let-playpen-child-porn-suspect-go-to-keep-concealing-their-source-code
http://www.zeit.de/digital/datenschutz/2017-01/strafverfolgung-fbi-geheimer-tor-exploit-dilemma
http://gizmodo.com/the-fbi-says-its-malware-isn-t-malware-because-the-fbi-1783537208

IV. Star Wars on Twitter – sleeping Twitter botnet with over 350,000 bots discovered

Star Wars fans have always known that the Empire strikes back, even if it has seemed defeated for a long time. However, a Twitter botnet inactive since 2013 got the name Star Wars from those who discovered it for another reason. First things first: at the start of January 2017, Juan Echeverria and Shi Zou at University College London's Department of Computer Science published a research paper on arvix.org explaining how they had discovered a huge and currently inactive network of 356,957 bots that had infected the social network Twitter and could be reactivated at any time. While analysing English-language tweets, the two had noticed that 3,244 users where tweeting from the middle of the sea or from very sparsely populated areas. The fact that this group appeared in a surprising number of cases to be quoting lines and fragments of lines from Star Wars films led to the name «Star Wars botnet». On finding further common characteristics, the researchers programmed a classifier to look at tweets from some 14 million English-language users. It identified the 350,000-plus bots. Further observations led Echevarria and Shi to the conclusion that these must be part of a huge network. They suspected that this network had remained undiscovered because all of the bots had stopped tweeting on 14 July 2013. Given that this vast army of virtual storm troopers could be reactivated at any time, they note that

more work is needed on developing methods to detect Twitter botnets. May the Force be with them!

Read more here:

https://www.heise.de/newsticker/meldung/Forscher-entdecken-riesiges-Twitter-Botnetz-Star-Wars-3604196.html
https://arxiv.org/pdf/1701.02405v1.pdf
https://www.engadget.com/2017/01/23/twitter-botnet-quotes-star-wars-from-the-middle-of-the-sea
http://gizmodo.com/massive-twitter-bot-army-exposed-by-its-obsession-with-1791464124
http://digitalchew.com/2017/01/22/star-wars-twitter-bots

New SWITCH-CERT Security Blog entries

Background – malware: Usage of .ch domain names for spamming malware Tofsee stopped
https://securityblog.switch.ch/2016/12/22/tofsee-ch-domain-names-stopped/

Background – malware: A file that wasn't there
https://securityblog.switch.ch/2016/12/20/a-file-that-wasnt-there/

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