SWITCHcert Security Report

December 2014

I. No «Land of the Free» in sight: NSA allowed to continue gathering data, BND puts forward EUR 300 million wish list

There were long faces in the US Senate after the USA Freedom Act fell two votes short of a majority at the end of November. The Act, supported by a broad coalition of Democrats, some more liberally minded Republicans, civil rights organisations, tech firms including Apple, Google, Microsoft and Yahoo as well as President Barack Obama, would have banned the National Security Agency (NSA) from continuing to gather phone call data on a massive scale. Opponents of the Act were against domestic phone call records being stored by the phone companies rather than the NSA, which would have needed a court order to get access to them. Their main argument was the emergence of new terrorist threats such as the group calling itself Islamic State. The USA Freedom Act was seen as the lowest common denominator in a reform intended to overhaul secret service powers in the wake of Edward Snowden's revelations.

Germany's foreign intelligence service BND is also entirely unmoved by such reform initiatives. Even while it was defending itself before the German parliamentary NSA inquiry, it presented a wish list totalling EUR 300 million (on top of its normal budget of almost EUR 560 million) to the Budget Committee – just in time for Christmas. In the BND's own words, the list is intended to bring it «up to speed with its partners in cyberspace». ZEIT ONLINE described the plans making up the Strategic Technology

Initiative in an article on 13 November. The list stretches from government-sponsored Trojans to real-time analysis of streaming data and a project with the technocratic title «Protection against Identification through Image Manipulation / Falsification». What this actually refers to is software that automatically cheats facial recognition systems. At least the BND has not lost its sense of humour.

Read more here:

http://www.nzz.ch/international/amerika/nsa-darf-weiter-ungebremst-daten-sammeln-1.18428311

https://netzpolitik.org/2014/usa-freedom-act-sogar-das-kleinstmoegliche-geheimdienst-refoermchen-faellt-durch

https://www.eff.org/deeplinks/2014/11/usa-freedom-act-week-whats-come-and-what-you-need-know

http://www.zeit.de/digital/internet/2014-11/bnd-bundesnachrichtendienst-ueberwachung-ausbau

https://netzpolitik.org/2014/kein-steuergeld-fuer-grundrechtsbruch-morgen-frueh-vorm-reichstag-gegen-etat-erhoehung-fuer-bnd-demonstrieren

http://www.golem.de/news/geheimdienst-bnd-moechte-sich-vor-gesichtserkennung-schuetzen-1411-110631.html

II. Censorship culture in the UK

«In our view, [the principle of filtering out illegal content with network blocks] represents a step backwards in the fight against illegal Internet content. We believe that creating an infrastructure to block and filter Internet content is not only counterproductive with regard to combating and removing illegal content, it also opens the door to a culture of censorship that undermines the fundamental principles of transparency and the rule of law.» This was the criticism eco, the German association of Internet service providers, levelled against the UK's increasingly commonplace network blocks. In addition to the «porn filter», a new button was recently added for reporting terrorist or extremist propaganda. The system currently blocks 23,000 websites in the UK, including sites dealing with nudity, sex education, dating, gambling, violence, extremist and terrorist political content, anorexia and eating disorders, suicide, alcohol, smoking, chat rooms, esoteric material and tools to circumvent network blocks. The blocks have also affected – at least temporarily – open-source websites such as Linuxtracker, pages posted by the news aggregator Reddit and the online magazine TorrentFreak because they allegedly enable peer-to-peer file sharing. Critics see this as a sign that child protection and the war on terror are being used as an excuse to censor any form of undesirable content.

Read more here:

http://www.theguardian.com/technology/2014/nov/14/isps-filter-extremist-material-internet

http://www.golem.de/news/ofcom-briten-schalten-den-pornofilter-ab-1407-108079.html

https://www.eco.de/2014/news/eco-britische-netzsperren-sind-rueckschritt-in-der-bekaempfung-illegaler-internetinhalte.html

http://www.bbc.com/news/technology-30052211

III. The new PR: how parties, companies and organisations manipulate web chat to propagate opinions

«We Make Opinions» is the tagline of Austrian PR agency Modern Mind Marketing. The magazine «Datum», also Austrian, recently revealed how this is done. It starts with setting up tens of thousands of fake accounts and hiring freelance posters who use these accounts to post comments online (not from the agency's offices, naturally, since the IP addresses could be traced) that show clients in a positive light and discredit critics or at least contradict their criticisms. According to the Datum report, practices the Russian secret service has been accused of using during the Ukraine crisis have also been adopted by leading clients like the Austrian People's Party (ÖVP), the state-run rail operator ÖBB, Bank Austria, TUI Austria, pharmaceuticals firm Bayer Austria and others from outside the German-language area such as UK company Paysafecard. The existence of these trolls is old news since the attacks on Wikipedia in 2013 came to light, but the extent of their manipulation nevertheless raised a few eyebrows. Austria's PR ethics commission was severely critical of these tactics.

The Broadway Hotel in the UK seaside resort of Blackpool proved that there are other ways to make money through opinion-forming posts. Its terms and conditions state that anyone posting a negative review of the hotel will be fined GBP 100 (about CHF 150).

Read more here:

http://www.datum.at/artikel/die-netzfluesterer

http://www.heise.de/newsticker/meldung/Putins-Trolle-schwemmen-die-Online-Foren-2221297.html http://futurezone.at/digital-life/so-manipulieren-firmentrolle-online-foren/95.363.385

http://www.lunzer-kommunikation.at/imageschaden-fuer-die-imagemacher.html

http://futurezone.at/digital-life/auf-tripadvisor-schlecht-bewertet-hotel-verlangt-gebuehr/97.967.200

IV. Regin and the Detekt-ives: new software finds known government Trojans – Symantec discovers a new one

No, our headline is not a misprint. «Detekt» is the name of a new tool that scans Windows computers for state-sponsored malware. It was developed by Claudio Guarnieri, a world-leading expert in government Trojans. Four civil rights organisations are supporting the publication of the open-source software, and the source code is available on GitHub. The list of malware that Detekt can identify reads like a Who's Who of government Trojans: BlackShades RAT, DarkComet RAT, FinFisher FinSpy, Gh0st RA, HackingTeam RCS, ShadowTech RAT, XtremeRAT and njRAT.

«Regin» will probably have to be added to the list soon. This is the name given by its discoverers at Symantec to a backdoor Trojan that has been in use since 2008 but appeared in what experts have termed a «most sophisticated» new form in 2013. It has been compared to StuxNet, Flame and Duqu. This version uses all manner of tricks to cover up not only its presence on infected machines, but also the fact that it has stolen data. The website The Intercept reported at the end of November that the NSA in the US and GCHQ in the UK were using Regin to spy on the EU, among other things. The main targets, however, are thought to be companies (primarily infrastructure operators), authorities and private individuals in Saudi Arabia and Russia.

Read more here:

https://netzpolitik.org/2014/detekt-anti-viren-scanner-fuer-staatstrojaner-veroeffentlicht

https://github.com/botherder/detekt

https://digitalegesellschaft.de/2014/11/software-gegen-staatstrojaner-veroeffentlicht

http://www.inside-it.ch/articles/38402

https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq

http://www.pcwelt.de/news/Regin___neuer_Super-Trojaner_spionierte_viele_Jahre_unentdeckt-Stuxnet-_und_Duqu-Nachfolger-9005597.html

http://www.spiegel.de/netzwelt/netzpolitik/trojaner-regin-ist-ein-werkzeug-von-nsa-und-gchq-a-1004950.html

V. Generali cheaper: lower premiums in exchange for personal information

In October's Security Report, we mentioned insurers offering cheaper car insurance to customers who installed «black box» recorders and suggested the possibility that they might also grant other discounts in exchange for information on health, fitness and lifestyle from smart home devices or wearables. Generali has now announced that it will do precisely this in the next 12 to 18 months. Customers will have to use an app to prove that they attend regular check-ups and get plenty of exercise to stay fit. If they do this, they will benefit from reduced premiums, vouchers and free gifts. Generali says that it will carry out spot checks on the data provided. It remains to be seen what sort of impact the first Bluetooth-enabled toothbrush with its own app, launched this August, will have on dental insurance costs or children's pocket money.

Read more here:

http://www.zeit.de/digital/2014-11/versicherung-generali-fitness-daten-sammeln

http://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generali-modell-wir-werden-manipulierbar-und-unfrei-1.2232147

http://www.faz.net/aktuell/technik-motor/umwelt-technik/zahnbuerste-oral-b-pro-7000-bluetooth-fuer-weisse-zaehne-13079480.html

The Clipboard: Interesting Presentations, Articles and Videos

Writing on the SANS InfoSec forum, Xavier Mertens outlines a simple way to detect potentially harmful new devices automatically on the Net using Arpwatch, Nmap and OSSEC:

https://isc.sans.edu/forums/diary/Guest+diary+Detecting+Suspicious+Devices+On-The-Fly/18993/

Google hijacking study – In November, Google provided an update on account hijacking and what can be done to stop it:

http://googleonlinesecurity.blogspot.ch/2014/11/behind-enemy-lines-in-our-war-against.html

http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf

ICMP and ICMPv6 redirects as an attack vector are nothing new, but Zimperium Mobile Security Labs reports that a more sophisticated form is now widespread in the mobile space:

http://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/

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

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.