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

March/April 2018

SWITCH

I. The dark side of the Data Force: Facebook, Cambridge Analytica, and the pressing question of who is using whose data for what

Star Wars in reverse: the Empire might have struck back, but this time the rebels are the bad guys. As tech giants – with Facebook at the top of the list, but also Google with its Google News and YouTube services, and Amazon with Netflix and Amazon Prime – transform into a new generation of media companies, many traditional media outlets are facing an existential threat. Now a whistleblower and traditional investigative journalists from the Observer, the New York Times and British TV broadcaster Channel 4 have created a serious crisis for Facebook and Alexander Nix, who has been ousted from his position as CEO of the data analytics firm Cambridge Analytica. The scandal surrounds the revelation that the data of around 87 million Facebook users was taken from the company without authorisation and used illegitimately for campaign purposes during the last US presidential election and, most likely, the Brexit referendum in the UK as well. These unfolding events are likely to be one of the biggest stories of the century. This is a completely unprecedented case of misconduct in both quantitative and qualitative terms – grave intervention in democratic elections by manipulators and their henchmen and women (Steve Bannon in particular, as well as Robert and Rebekah Mercer), both domestic and foreign, and in a form never thought possible.

Even worse are Alexander Nix's boasts of having orchestrated both virtual and physical extortion in order to influence elections.

All of these events are relevant to our daily lives, but they also resemble something of a horror series set in our Big Data society, indeed as hair-raising, dubious and surreal as the scripts for *House of Cards*, *Breaking Bad* and *Homeland* fused with the Seldon Plan from Isaac Asimov's *Foundation* sci-fi trilogy (1942-1950). Not a day goes by without major coverage of the scandal in the media. *The Guardian*, heise.de, netzpolitik.org and *Die Zeit* have published their own stories, which are well worth reading (see links below).

Once again, Facebook founder and CEO Mark Zuckerberg feigns contrition when confronted with the accusation that his company neglected to protect the data of its users. What complicates the matter this time, however, is that Cambridge Analytica's misconduct was made possible in the first place by this very lack of oversight. Now Zuckerberg will not only have to answer to the European Commission, but has also been summoned for questioning by a British parliamentary committee and the US Senate's Commerce and Judiciary committees. Google co-founder Larry Page and Twitter CEO Jack Dorsey are also set to testify before the committee. It appears that this has shaken up the managers of other tech giants as well. That includes Brian Acton, co-founder of the WhatsApp messenger service – which was bought out by Facebook in 2014 for 16 billion dollars – who publicly campaigned for Facebook users to delete their accounts (#deletefacebook). Prior to that, Tesla CEO Elon Musk had already deleted the Facebook accounts of his two companies, Tesla and Space-X. Even celebrities like Jim Carrey are selling their Facebook shares, deleting their accounts and encouraging their fans to do the same.

Facebook could also come under fire by another prominent critic of the social network: Max Schrems. On 21 March 2018 Schrems pointed out that as far back as 2011, he had sued Facebook in Ireland for millions of instances of data abuse and that Facebook countered it had acted completely within the law. This statement is likely to be of interest to numerous investors and the US Federal Trade Commission, which concluded a data protection agreement with Facebook and will now investigate whether Facebook violated this agreement. Should the company be in breach of the agreement, the social network could face fines of 40,000 dollars – for each instance! 87 million cases translates to potential fines hovering in the

range of 2 trillion dollars. So it's no surprise that the first investors are already accusing Facebook of making false statements about data protection and security. In addition to the astronomical fines, large companies that abuse their market position in the USA face the potential Damocles' sword of a regulatory break-up. This is probably also why in late March, Apple CEO Tim Cook and IBM CEO Virginia Rometty made a plea for sensible regulation and stricter requirements governing the handling of personal data. Salesforce CEO Marc Benioff, who is also a Silicon Valley billionaire, took it a step further at the WEF in Davos when he called for Facebook to be broken up. It appears there is a growing awareness in the boardrooms of the tech giants that it will take drastic measures to cast off the demons they have conjured up.

Read more:

https://www.theguardian.com/uk-news/cambridge-analytica
https://www.heise.de/thema/Facebook_Datenskandal
https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen
http://www.zeit.de/suche/index?q=Cambridge+Analytica+
https://www.nzz.ch/wirtschaft/die-rebellin-hinter-den-barrikaden-ld.1348569
http://www.spiegel.de/netzwelt/web/cambridge-analytica-firmenchef-alexander-nix-prahlt-mit-erpressungen-a-1198925.html
https://www.engadget.com/2018/03/21/mark-zuckerberg-apology-tour-2018
http://www.faz.net/aktuell/wirtschaft/diginomics/amerikanischer-senat-bestellt-facebook-chef-zuckerberg-ein-15514592.html
https://www.theverge.com/2018/3/20/17145200/brian-acton-delete-facebook-whatsapp
http://www.absatzwirtschaft.de/zusammen-mehr-als-5-millionen-abonnenten-trotzdem-loescht-musk-die-facebookseiten-von-spacex-und-tesla-128703
https://www.bild.de/unterhaltung/leute/jim-carrey/verkauft-seine-facebook-aktien-und-loescht-account-54730232.bild.html
https://futurezone.at/netzpolitik/max-schrems-facebook-wusste-von-illegaler-datenweitergabe/400008921
https://futurezone.at/netzpolitik/nutzerdaten-abgegriffen-facebook-droht-billionenstrafe/400007871
https://www.handelszeitung.ch/unternehmen/erste-investoren-verklagen-facebook
http://www.handelsblatt.com/unternehmen/it-medien/facebook-skandal-apple-chef-cook-fordert-mehr-datenschutzregeln/21111738.html
https://www.tagesanzeiger.ch/digital/daten/experten-fordern-die-zerschlagung-von-facebook/story/23677763

II. News from the world of state trojans: Microsoft's analysis of FinFisher

The use of 'state trojans' by government intelligence agencies and law enforcement authorities to infiltrate computers and mobile devices for the purposes of spying on terrorists, criminals or even suspects is nothing new. The transgression of legal boundaries and misconduct are hardly unusual either. Meanwhile, IT security firms and operating system developers are working to close security gaps that

enable (state) trojans to sneak their way onto devices and intercept data or even control the entire device remotely.

According to security researchers at Microsoft, FinFisher, the eponymous state trojan developed by the German-British subcontractor for security authorities, is 'in a league of its own' in terms of concealment, complexity, sophistication and adaptability. In early March, Microsoft announced that it had examined and analysed FinFisher inside and out. Based on the findings, it reported that it had improved Advanced Threat Protection (ATP) in Microsoft Defender and in Windows 365. To help other developers and security experts optimize their software and curb the spread of malware, Microsoft's security experts reported their findings on Microsoft cloudblogs.

Read more:

https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

https://www.heise.de/security/meldung/Microsoft-vs-FinFisher-Windows-Defender-ist-gegen-den-Staatstrojaner-gewappnet-3988226.html

https://www.extremetech.com/computing/265074-microsofts-windows-defender-atp-good-enough-catch-law-enforcement-spyware

http://www.zdnet.com/article/microsoft-windows-defender-can-now-spot-finfisher-government-spyware

https://cyware.com/news/microsoft-windows-defender-can-now-spot-finfisher-government-spyware-baec1989

III. Russian APT28 hackers' month-long infiltration of the computer network of Germany's federal government

The statement given by Germany's Interior Ministry on the evening of 28 February 2018 sounded unspectacular and matter-of-fact: 'We are able to confirm that the Federal Office for Security (BSI) and the intelligence agencies are investigating an IT security incident affecting the information technology systems and networks of Germany's federal government.' The German news agency dpa had previously reported that cyberspies belonging to the ATP28 hacker group that has repeatedly been connected with the Russian government had gained access to the entire data network of Germany's federal government through a successful attack on its Federal Foreign Office and Federal Ministry of Defence. The hackers reportedly succeeded in infiltrating the network, illicitly installing malware and stealing data – apparently over the course of a year. Just how deep the hackers managed to penetrate into the systems and the damage they caused is currently the subject of

intense investigation. In contrast to the mundane-sounding media statement, it has emerged that the 'isolated attacks which are under control' were a disaster of the worst possible proportions for the IT security of Germany's government – especially considering that ATP 28 was also identified as responsible for the 2015 hack on the German Bundestag's network, previously considered secure. Not that you'll find much news coverage of the issue – most of the big daily news publications only reported on the event once. Only heise.de extended its coverage longer than a week.

Read more:

http://www.faz.net/aktuell/russische-hacker-dringen-in-deutsches-regierungsnetz-ein-15472050.html
http://www.zeit.de/digital/datenschutz/2018-02/hacker-dringen-in-deutsches-regierungsnetz-ein
http://www.netzwoche.ch/news/2018-03-01/hacker-greifen-deutsche-regierung-an
http://www.inside-it.ch/articles/50371
https://www.tagesanzeiger.ch/ausland/europa/deutsche-regierung-liess-hacker-monatelang-gewaehren/story/10128411
https://www.nzz.ch/international/der-hackerangriff-auf-die-deutsche-regierung-dauert-an-ld.1361876
https://www.heise.de/newsticker/meldung/Sicherheitskreise-Hacker-drangen-in-deutsches-Regierungsnetz-ein-3983510.html
https://www.heise.de/newsticker/meldung/Bundeshack-Angriff-laut-de-Maiziere-technisch-anspruchsvoll-und-lange-geplant-3984840.html
https://www.heise.de/newsticker/meldung/Kommentar-zum-Bundeshack-Schluss-mit-Schlangenoel-und-Monokultur-3985144.html
https://www.heise.de/security/meldung/Bundeshack-Daten-sollen-ueber-Outlook-ausgeleitet-worden-sein-3987759.html

IV. Bitcoin bounty or close encounter: bizarre side-effects of cryptomining

Virtual currency miners not only consume massive amounts of energy, they are finding ever more creative ways to do so. For instance, on 27 March 2018 digiconomist estimated that cryptomining consumes approximately 58 terawatt hours of energy each year – very close to Switzerland's total annual energy consumption. A single Bitcoin transaction currently consumes more than four times as much energy as 100,000 Visa card transactions. Because most of the Bitcoin network is powered with energy from coal-burning plants, the CO_2 balance is nothing short of abysmal.

Cryptomining is also having a disastrous effect on the researchers working on the Search for Extraterrestrial Intelligence (SETI) project, who are desperately waiting for new powerful graphics cards to help them scan for signals from extraterrestrials. Because the cards with the latest graphics processing units (GPUs) are also ideal for mining, the crypto miners have essentially picked the

whole market clean, and the researchers will have to wait. Meanwhile, Miami-based cigar maker Rich Cigars announced that it would be getting out of the smoke business and instead putting its money on the intensive mining of cryptocurrencies – which has brought a 2000% jump in the value of the penny stock.

Cryptominers hoping to avoid high electricity bills use github or popular porn sites to smuggle mining software onto the computers of unsuspecting users. As the online magazine gizmodo recently reported, some use the simple alternative of the Tesla cloud. The statement by Gaurav Kumar, CTO of the security firm RedLock, puts the trend in a nutshell: 'The recent rise of cryptocurrencies is making it far more lucrative for cybercriminals to steal organizations' computer power rather than their data.'

Read more:

https://digiconomist.net/bitcoin-energy-consumption
https://futurezone.at/digital-life/bitcoin-mining-behindert-suche-nach-ausserirdischem-leben/400003853
https://futurezone.at/b2b/zigarrenhersteller-steigt-auf-bitcoin-mining-um/302.226.171
https://www.heise.de/security/meldung/Mining-Trojaner-lauern-auf-Github-4000476.html
https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247
https://motherboard.vice.com/en_us/article/9kzyv7/porn-sites-are-doing-the-most-cryptocurrency-coinhive-browser-mining

From the editors: New on the SWITCH-CERT security blog

A day in the life of nic.ch

https://securityblog.switch.ch/2018/03/20/a-day-in-the-life-of-nic-ch/

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