SWITCHcert Security Report

August 2015

SWITCH

I. What a hack – government Trojan Galileo, costing almost half a million francs, rendered useless after attack on Hacking Team

Irony of ironies: Swiss cantonal authorities invest EUR 486,500 in surveillance software called Galileo, including a «complete care package», with government approval and the highest level of secrecy – and then the company selling the costly Trojans and other surveillance tools, which calls itself Hacking Team, itself falls victim to hacking. The story goes public, and all the effort and expense were for nothing. The Trojan was supposed to monitor communication by suspects on all common PC systems and smartphone platforms. Various commentators note that the code making up Galileo, amounting to well over a million lines, is capable of doing much more than current Swiss law allows. Der Landbote, for example, writes: «In practical terms, this means that the authorities want to use this Galileo surveillance software without actually knowing exactly what it does. It remains to be seen whether the programs in question have vulnerabilities that hackers can exploit or even back doors that the manufacturer has deliberately built in to spy on the spies themselves.» Hacking Team denies the latter, but UK security researcher Joseph Greenwood, who has analysed at least some of the hacked data that have been made public, believes that Galileo's source code could definitely enable its developers to «disable» clients' servers.

© SWITCH 2015

The authorities' most likely excuse for being blind to this issue while staring wide-eyed at the Italian spyware provider's offering – Sonntagsblick claims that they also showed an interest in other technologies such as microphones for snooping on mobile phones and remote monitoring systems for smartphones and computers – is that they were in good company as Hacking Team clients. The FBI, too, has used Galileo to spy not only on users of child pornography, but also apparently on non-criminal Tor network users. Buyers were clearly not put off by the fact that Hacking Team's clients also included middlemen for the Chilean government, the Russian secret service FSB and repressive states such as Ethiopia, Egypt and even Sudan, which is in fact subject to an international trade embargo.

Read more here:

http://www.nzz.ch/zuerich/aktuell/der-seltsame-aufschrei-um-die-trojaner-1.18578045
https://www.digitale-gesellschaft.ch/2015/07/11/einmal-trojaner-federal-fuer-die-zuercher-kantonspolizei/#more-6211
http://www.landbote.ch/ueberregional/standard/Eine-teure-Blackbox-fuer-die-Polizei-/story/31582953
http://www.srf.ch/wissen/digital/der-staatstrojaner-steht-vor-den-toren
http://arstechnica.com/security/2015/07/massive-leak-reveals-hacking-teams-most-private-moments-in-messy-detail/
http://arstechnica.com/security/2015/07/hacking-team-may-not-have-had-a-backdoor-but-it-could-kill-client-installs
http://www.1815.ch/news/schweiz/politik/staatstrojaner-und-frankenstaerke-die-grossen-themen-am-sonntag-20150712061324/
http://www.zeit.de/digital/datenschutz/2015-07/hacking-team-trojaner-kunden-hack

© SWITCH 2015

II. Data stacked up sky-high – unprecedented dimensions of cyberattack on US Office of Personnel Management

«If you printed out the 14 million SF86 forms (federal background investigation form) lost in the OPM breach, the stack would be approximately 185 miles high.» This was tweeted by Gavin Millard, a technical director at Tenable Network Security, on 27 June 2015, regarding «one of the largest thefts of government data ever seen» (quote from the Wall Street Journal). It emerged at the start of June that hackers whose trail leads to China had accessed the data records of the US Office of Personnel Management (OPM) and stolen files on current and former government employees.

The OPM was forced to admit at the start of July that the damage was much greater than previously assumed and that this was in fact turning out to be the biggest cyberattack ever suffered by the US government. The attackers had got hold of addresses, social security numbers, dates of birth, health information, financial details, in some cases details of sexual preferences and extramarital affairs, and criminal records including around 1.1 million fingerprints – not only for people who work for the government, but also for people who had merely applied for government jobs. Highly sensitive data on more than 25 million people were stolen in two attacks. Working out how this happened is made more difficult by the fact that, as became early on in the investigation, the logging mechanisms on the hacked IT infrastructure were poor or inadequate. Despite the resignation of OPM head Katherine Archuleta, therefore, the problem is a long way from being solved.

Read more here:

http://www.databreachtoday.com/analysis-opm-breach-so-bad-a-8359#
http://www.golem.de/news/cyberangriff-hacker-dringen-in-personalbehoerde-der-us-regierung-ein-1506-114498.html
http://www.tagesanzeiger.ch/ausland/amerika/Steckt-China-hinter-der-Cyberattacke-auf-die-USA/story/11715202
http://www.zeit.de/digital/2015-07/usa-behoerde-hacker-china
http://www.inforisktoday.com/opm-struggles-to-notify-breach-victims-a-8411
http://www.golem.de/news/nach-hackerangriff-opm-chefin-katherine-archuleta-tritt-zurueck-1507-115175.html

© SWITCH 2015

III. Forget about doping tests – Team Sky data theft brings Tour de France into digital age

Winners being suspected of doping has almost become one of the many traditions of the Tour de France. Now, however, a hacking attack on winner Chris Froome's Team Sky has shown that the world's most famous cycle race can also be a platform for the latest innovations. Froome's performance data such as speed, cadence and pulse during a stage were stolen and handed over to the UK Eurosport channel as a video (which has since been taken down). The hackers' motives are unclear. Were they trying to discredit Froome, or did they want to make people question how secure their personal fitness and activity tracker data were if even the professionals at Team Sky were unable to keep theirs safe? This is perhaps a very pertinent question in the age of the «quantified self», where we can measure, record and analyse everything we do – even our love lives, thanks to a new smart sex toy…

Read more here:

https://netzpolitik.org/2015/tour-de-france-team-sky-offenbar-gehackt
http://www.theguardian.com/sport/blog/2015/jul/14/chris-froome-team-sky-hacking-tour-de-france
http://www.zeit.de/digital/datenschutz/2015-06/datensicherheit-fitness-tracker-vergleich
http://www.primelife.co/lovely-wearable-fuer-sex

IV. IMSI catchers – don't let them catch you…if you can!

Had the con man played by Leonardo di Caprio in the comedy «Catch Me If You Can» owned a mobile phone, the film would probably have been much shorter. An IMSI (international mobile subscriber identity) catcher can be used to locate mobiles easily and track their users' movements – without them knowing. They do this by simulating a mobile network, appearing as a base station to phones and as a phone to the regular network. This way, they can identify not only the phone of a suspect being pursued, but also all others within range that make a connection. Since all smartphones feature encryption, IMSI catchers force them to turn it off. They forward all the data intercepted to the real network so as not to arouse anyone's suspicion, but not before copying and analysing them. Authorities justify their use of IMSI catchers, which are not currently subject to any legal restrictions in Switzerland, by pointing out

© SWITCH 2015

that they are an efficient means of finding missing persons and criminals. However, those who find the collateral damage excessive or fear that criminals may also be using IMSI catchers (not unreasonably, given that prices start at roughly EUR 1,500) should either turn off their phone or leave it at home.

If you are unwilling or unable to do either, we recommend reading the fourth article linked to below (on digitale-gesellschaft.ch, in German) or using an IMSI catcher detector.

Read more here:

https://en.wikipedia.org/wiki/IMSI-catcher
http://www.blick.ch/news/schweiz/zentralschweiz/am-gitschen-im-kanton-uri-wingsuit-flieger-stuerzt-in-den-tod-id3961344.html
http://www.zeit.de/digital/mobil/2014-09/mobilfunk-imsi-catcher-handy
https://www.digitale-gesellschaft.ch/2015/06/22/imsi-catcher-erkennen-und-dokumentieren
http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html

V. Do androids dream of electric horses? New variant of mTan Trojan ZeuS targets Android users

Ridley Scott's classic 1982 movie «Blade Runner» was adapted from a science fiction novel by Philip K Dick entitled «Do Androids Dream of Electric Sheep?». Over 30 years later, digital Trojan horses are giving many Android users nightmares. Following an attack in 2013, a Trojan is once again infecting Android smartphones to steal mobile and text message sign-in codes for Internet and mobile banking systems – mTans – and forward them to hackers. What is particularly sneaky this time is the way the new variant of ZeuS hides in an EV SSL certificate sent to e-banking clients in perfectly faked phishing e-mails. The third link below (anubis.iseclab.org) contains a technical analysis.

A Swiss cantonal bank is now warning its clients about ZeuS. Since the Trojan is rarely identified, they are strongly advised to follow a few basic rules for mobile and e-banking.

Here are the four most important ones:

- Only install apps you really need that come from a trusted source.
- Always keep your smartphone and the apps installed on it up to date.

© SWITCH 2015

- Activate your device's blocking code.
- Do not store access details such as PINs and TANs on your mobile device.

Read more here:

http://www.heise.de/security/meldung/mTAN-Trojaner-hat-es-erneut-auf-Android-Nutzer-abgesehen-2721682.html
http://www.computerbase.de/2015-06/malware-mtan-trojaner-infiziert-android-smartphones
https://anubis.iseclab.org/?action=result&task_id=16277ab1d21cbec147997aec147fe4783&format=html
https://www.appkb.ch/metanavi/news.htm&detailid=335&isElement=inetnews&rss=1&gContrast=2
https://www.ebas.ch/de/securitynews/437-mobile-banking-wird-immer-beliebter

VI. VPNs – how IPv6, DNS and co. can still turn virtual private networks into very problematic nuisances

Back in 2013, we noted in the SWITCH Security Blog that data packets can «bypass» VPN tunnels in so-called dual-stack environments if IPv6 tunnels are implemented at the same time. The latter are often installed automatically without users' knowledge. Researchers from the UK and Italy have now investigated 14 commercial VPN services and found serious deficiencies (see the third link below, eecs.qmul.ac.uk, for a detailed description). Dual-stack technology, poor handling of DNS queries and failure to adapt IPv6 routing tables led to data traffic in public wireless networks being routed via the public network rather than secure VPN tunnels. As a result, a connection thought to be secure enabled DNS attacks and routing table manipulation. Users' anonymity and privacy are not protected in this situation. Worse still, data traffic can be diverted and corrupted. PureVPN is an example of a provider that avoids DNS attacks by running its own DNS servers, switching from IPv6 back to IPv4 connections and advising users who have configured PureVPN manually under Windows to turn off IPv6 completely. Android devices appear to be hit hardest by the IPv6 leak, but Apple's iOS has insufficient protection against VPN hijacking in the form of masque attacks, at least in versions prior to 8.4, as Pierluigi Paganini reports in his Security Affairs blog. He recommends carrying out a system update.

© SWITCH 2015

Read more here:

http://securityblog.switch.ch/2013/08/28/ipv6-vpn-traffic-leakage-in-dualstack-umgebungen
http://www.golem.de/news/security-viele-vpn-dienste-sind-unsicher-1507-115006.html
http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf
http://www.heise.de/security/meldung/Privatsphaere-und-Anonymitaet-bei-vielen-VPN-Diensten-nicht-gewaehrleistet-2731928.html?wt_mc=rss.security.beitrag.atom
http://www.golem.de/news/vpn-schwachstellen-purevpn-veroeffentlicht-patch-fuer-seine-windows-software-1507-115026.html
http://securityaffairs.co/wordpress/38219/hacking/apple-partially-fix-masque-attack.html

The Clipboard: interesting presentations, articles and videos

The security team at heise.de looked into the question of whether end-to-end encryption in Web 2.0 is now a reality or still a myth using WhatsApp as an example. Read their findings here:

http://www.heise.de/security/artikel/Der-WhatsApp-Verschluesselung-auf-die-Finger-geschaut-2629020.html

WebRTC can be used to identify the local IP addresses of clients that would normally be hidden. The New York Times appears to be exploiting this:

https://webrtchacks.com/dear-ny-times

The Electronic Frontier Foundation celebrated its 25th anniversary this month. CSOonline took a look back through the years:

http://www.csoonline.com/article/2949096/security-leadership/electronic-frontier-foundation-celebrates-25-years-of-defending-online-privacy.html

Interactive maps of the world showing Internet traffic are not exactly thin on the ground. Norse, a Californian provider of security solutions, has produced an especially striking one to visualise the vast extent of hacker attacks throughout the world in real time:

http://map.norsecorp.com

The SWITCHcert Security Report was written by Dieter Brecheis and Michael Fuchs.

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.

© SWITCH 2015