SWITCHcert Security Report

April 2016

SWITCH

I. Probably the most expensive typo ever foils probably the biggest attempted bank robbery ever

They might have made history – if only they could spell. A group of cybercriminals staging an attack on Bangladesh's central bank wrote «Fandation» instead of «Foundation» on a transfer form and thus exposed what would have probably been the biggest bank robbery of all time before all of the transfers, totalling almost USD 1 billion, could be executed. Compared with that, the USD 80 million they actually stole seems like peanuts, but it could still be a record. Ironically enough, it was Deutsche Bank (famous for describing a rather large sum of money as «peanuts») that spotted the spelling mistake. Let us start at the beginning. What we have learned so far is that hackers who as yet remain unidentified infected computers at the Bangladeshi central bank with a Trojan (also unknown) in order to work out the best way to transfer money held by the bank in foreign accounts to their own accounts. They also stole access details for the SWIFT payment system to make the transfers possible. On the weekend of 4 and 5 February 2016, they initiated in quick succession more than 30 transfers of funds from the central bank's accounts with the Federal Reserve Bank of New York to fake NGO accounts in Sri Lanka and the Philippines. One transfer of USD 20 million to a certain «Shalika Fandation» was routed via Deutsche Bank, which

noticed the typo and checked it with the Bangladeshi central bank. When it also became apparent that the payments were not being made from one bank to another, all further transfers in the queue – adding up to around USD 1 billion – were stopped. Despite their best efforts, police in Sri Lanka and the Philippines were unable to prevent a large share of the USD 80 million that was actually stolen through four successful transfers being laundered by casinos, making it untraceable.

Bangladesh Bank is accusing the US Federal Reserve of negligence, while ICT security and finance experts are casting a critical eye over the Fed's security in general. At the same time, the New York bankers are facing accusations from investors and politicians alike that they have undermined foreign financial institutions' trust in their security. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) advised all affiliated banks at the end of March to tighten their security measures so as to avoid any more cases like this one, especially since it must be assumed at this stage of the investigation that the hackers were also targeting other banks.

Read more here:

http://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC
http://www.tagesanzeiger.ch/panorama/vermischtes/milliardenbankraub-misslingt-wegen-zwei-buchstaben/story/31934921
http://www.zdnet.com/article/malware-was-at-the-root-of-80-million-bangladesh-bank-heist
http://www.zdnet.com/article/bangladesh-bank-debates-lawsuit-against-federal-reserve-over-cyber-fraud
http://www.darkreading.com/cloud/swift-to-issue-warning-in-wake-of-cyberattack-on-bagladesh-central-bank-/d/d-id/1324767

II. Switzerland targeted by various hacker groups? Series of DDoS attacks on Swiss websites

Switzerland was hit by an unprecedented wave of targeted DDoS attacks in mid-March. The web shops of Do-it, Digitec, Galaxus, Interdiscount, LeShop, Melectronics, Micasa and Microspot were temporarily taken down. The Swiss Federal Railways (SBB) website was also affected.

It seems that a number of groups with different intentions are behind the attacks. A group of «grey hats» calling themselves NSHC admitted to inside-it.ch that they

had hacked Interdiscount, Microspot and SBB to show how inadequately Swiss sites are protected against cyber threats. In a separate incident, NSHC copied the names and e-mail addresses of around 50,000 users from the Swiss Party SVP database, including party members, supporters and media contacts. NSHC claimed that here, too, it was not intending to blackmail its victims or publish any of the data.

Meanwhile, it appears that other online retailers did receive blackmail notes. The Reporting and Analysis Centre for Information Assurance (MELANI) believes that there is a connection between these hacks and the theft of 6,000 users' login details. This, it says, was evidently the work of «black hats», whose cyberattacks are purely criminal in nature.

Several Swiss financial institutions had received blackmail notes from a different source a few days previously. They were told to pay 25 Bitcoins to prevent a DDoS attack, but even those that refused to pay were never attacked.

Read more here:

http://www.heise.de/security/meldung/DDoS-Attacken-auf-Schweizer-Websites-3144854.html
http://www.cash.ch/news/alle/onlineshophacks_und_6000_gestohlene_emailkonten_haengen_zusammen-3433299-448
http://www.inside-it.ch/articles/43241
http://www.tagesanzeiger.ch/schweiz/standard/Hacker-erpressen-OnlineShops-mit-Drohbriefen/story/21342550
http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/digitec-reicht-wegen-hackerangriff-strafanzeige-ein/story/13546298
http://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland
http://www.watson.ch/Digital/Schweiz/905636585-DDoS-Attacken-in-der-Schweiz--«Es-meinen-immer-noch-viele--sie-seien-zu-unbedeutend--um-Ziel-eines-Hacker-Angriffs-zu-werden»
http://www.nzz.ch/nzzas/nzz-am-sonntag/cyber-attacken-kriminelle-erpressen-schweizer-online-shops-ld.9083

III. Connected cars –«one of this generation's biggest security risks»

There was widespread media coverage on 17 March of the FBI's lengthy Public Service Announcement on the website www.ic3.gov warning about the hacking risks associated with connected cars. Coming only a few days after the FBI itself had demanded that Apple turn off the encryption on the iPhones of suspected criminals and terrorists, readers might have thought that this was just a premature April fool's joke. We have already covered various security and

privacy aspects of connected driving in previous issues of the SWITCH Security Report. Now it appears that US security experts have also finally become aware of the high risks inherent in connected cars. Writing on zdnet.com, Conner Forrest even refers to them as «one of this generation's biggest security risks». He explains that this is not only because they have insufficient protection against attacks, it actually has more to do with the fact that they record large quantities of data, giving hackers a detailed insight into owners' lives. Added to this, the highly complex division of labour in production, the sheer number of vehicles on the road and the ease with which they can be manipulated all serve to heighten the risks associated with connected cars.

European motoring associations are also looking at the topic from various viewpoints. The Austrian Automobile, Motorcycle and Touring Club (ÖAMTC), for example, recently started a campaign headed «My Car – My Data», directly contradicting what former Volkswagen CEO Martin Winterkorn said at the 31C3 conference at the end of 2014: «Your car's data are mine!» (as featured in the SWITCH Security Report back in February 2015). The General German Automobile Club (ADAC), meanwhile, conducted a test proving that your car does not have to be connected to attract criminals. The dangers of keyless entry technology and methods for exploiting it have been known for years, but it is still so vulnerable that all 24 of the cars fitted with it that were tested had inadequate protection against unauthorised access. The ADAC assumes that other makes and models could be affected and says that manufacturers urgently need to rectify the problem.

Read more here:

http://www.ic3.gov/media/2016/160317.aspx
http://motherboard.vice.com/read/if-the-fbi-is-so-worried-about-car-hacking-why-is-it-fighting-encryption
http://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk
http://www.bbc.com/news/technology-35841571
http://futurezone.at/netzpolitik/oeamtc-chef-auto-daten-gehoeren-dem-konsumenten/186.286.964
http://www.heise.de/security/meldung/ADAC-Viele-aktuelle-Pkw-Modelle-ueber-Funk-knackbar-3140796.html
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-09_de.pdf

IV. Done and dusted – the new Federal Act on the Surveillance of Post and Telecommunications

In its spring session, the Swiss parliament voted in favour of revising the Federal Act on the Surveillance of Post and Telecommunications and signed off the new Act, which has been the subject of heated debate for some time (as featured in the SWITCH Security Report back in October 2015). It gives the criminal prosecution authorities in Switzerland new powers to install government-approved Trojans on the computers of people suspected of serious crimes and use IMSI catchers to locate and eavesdrop on their mobile phones, among other things. In return for these powers, the length of time for which the authorities are allowed to store data was not extended. This was intended to provide a better starting point with regard to the expected call for a referendum from opponents of the Act.

Indeed, the latter have not wasted any time in making themselves heard. A cross-party committee led by SVP National Councillor Franz Grüter hopes to overturn the Act, which it believes goes too far. The Digital Society association also laments what it sees as a «missed opportunity to hold a long overdue debate on the fundamental issues of surveillance» and calls the new draft legislation «disproportionate and dangerous». Thus begins the next round in the struggle, which has already been under way for more than two years, to find a broadly acceptable compromise between legitimate security interests and threats to individuals' freedom.

Read more here:

http://www.inside-it.ch/articles/43257
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-10_de.pdf
http://www.computerworld.ch/news/politik-gesellschaft/artikel/buepf-unter-dach-und-fach-69857
http://www.netzwoche.ch/de-CH/News/2016/03/17/Das-Buepf-ist-beschlossene-Sache.aspx
http://www.tagesanzeiger.ch/schweiz/standard/Trotz-Bruessel-Komitee-kaempft-gegen-mehr-Ueberwachung/story/24190094
http://www.watson.ch/Schweiz/Büpf/182605621-Telefonüberwachung–Piratenpartei-ergreift-das-Referendum-gegen-das-BÜPF
https://www.digitale-gesellschaft.ch/2016/03/21/buepf-2-0-schlecht-ist-nicht-gut-genug

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