# SWITCHcert Security Report

May 2016

SWITCH

## I. Faster than Odysseus – e-banking Trojan Gozi attacks Switzerland via news website

The army of ancient Greece famously lay siege to Troy for ten whole years before Odysseus hit upon the idea of building a giant horse out of wood, hiding inside it with an elite military unit and allowing the Trojans to believe that they had found something valuable that they could drag back into their city. This is exactly what they did, despite all warnings from the priest Laocoön and the king's daughter Cassandra, and it led to the city's destruction. Almost 3,000 years later, a Trojan horse of the virtual kind called Gozi needed only 20 minutes to wreak its havoc – 20min.ch, to be precise. Switzerland's most popular news website was used twice by cybercriminals at the start of April to distribute malware aimed at harvesting bank and login details from computers all over the country. Malvertising (advertising that spreads malware) on this scale is unprecedented in Switzerland. We highlighted the escalating conflict over adblockers in December's Security Report. We also published a blog entry in February this year that not only outlined the general malvertising situation but also explicitly stated that news websites in particular were being misused as a means of distributing e-banking Trojans. As a side note here, we would like to point out that this popular

abbreviation of «Trojan horse» is a complete misnomer, since the Trojans themselves were of course the victims and not the aggressors.

Less than two months after the blog entry appeared, the Federal Office of Information Technology, Systems and Telecommunication felt compelled to block 20min.ch temporarily in order to «reduce the risk of a successful malware attack» because the biggest Swiss news site was spreading the e-banking Trojan Gozi ISFB. Computers were apparently infected by drive-by downloads, which took effect as soon as the 20min.ch website was called up without users doing anything else. The company that owns the website claims that users of its mobile app were not affected. A compromised Flash file hidden inside the 20min.ch system started a manipulated JavaScript in the background that attempted to load malware onto visitors' computers and run it from there.

While security experts from SWITCH were still busy giving interviews and advice on how to handle Gozi, 20min.ch was attacked by another Trojan. Going by the name of Bedep, this one installed a back door on computers allowing hackers to control them remotely as part of a botnet. It appears to have found its way onto 20min.ch via a compromised advertising network.

In view of this double whammy, it seems like an almost cynical paradox that 20min.ch was prompting users only a week before the first attack to turn off their adblockers. This is perfectly understandable for a free news outlet that relies on advertising to fund its content. However, a similar request from a renowned technical publisher that has up to now placed great stock in cybersecurity is rather more exasperating. The Heise publishing house has recently started to ask people visiting heise.de to deactivate adblockers. We can only hope that Heise does not become the next target for Gozi & co. as its news site celebrates its 20th anniversary.

Read more here:

http://www.heise.de/newsticker/meldung/Schweizer-News-Site-verbreitet-Schadcode-Behoerden-und-Firmen-reagieren-3165287.html
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-12_de.pdf
https://securityblog.switch.ch/2016/02/10/attack-of-the-killer-ads
http://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident
http://www.inside-it.ch/articles/43486
http://www.tagesanzeiger.ch/digital/computer/ebankingtrojaner-gozi-das-raten-experten/story/13376685
http://www.watson.ch/!661270267
http://www.nzz.ch/digital/kampf-gegen-werbeblocker-klick-und-weg-ld.9431
http://www.heise.de/Adblocker-auf-heise-online-1164703.html

## II. Heartbreak remote – chip implants and the security of implanted, software-driven medical devices

«We are the Borg…We will add your biological and technological distinctiveness to our own. Your culture will adapt to service us. Resistance is futile.» In the movie «Star Trek: First Contact», the enhancement of human beings with implants was portrayed as a horror scenario that must be resisted, in spite of the warnings to the contrary. These days, however, the topic of «augmented humanity» is attracting more positive interest. IT security firm Kaspersky commissioned a representative, Europe-wide study that revealed that only 29% of respondents would categorically rule out having a chip implanted beneath their skin. Only in Germany and Switzerland was the proportion of people vehemently opposed to biohacking 49% or higher. Chip implants that use Near Field Communication (NFC) technology for identification, access control, feeding and medical purposes are already widespread in cats, dogs, other pets and livestock. The authors of the study were nevertheless surprised to see how many people are positively disposed towards carrying a miniature computer around in their bodies in spite of all the unanswered legal, technical and security questions. Kaspersky, with help from the Swedish pro-biohacking group BioNyfiken, proved in a field test that chip implants can be read and compromised with malware. Terrorists, for example, could gain access to airports using an identity stolen from a chip like those used by the airline SAS for its recently launched bioimplant check-in service. Pacemakers or insulin pumps could also be manipulated and perhaps even turned off completely. While these communicate via Wi-Fi rather than NFC, the lectures by security researcher Marie Moe, who is kept alive by a pacemaker with two Wi-Fi interfaces, are very thought-provoking.

It would seem that security issues are only being dealt with at a rudimentary level in ICT-supported medicine, even outside the body. The US government's Industrial Control Systems CERT issued a warning at the end of March concerning the automated drug delivery system Pyxis SupplyStation from Carefusion. Security experts had found no fewer than 1,418 vulnerabilities, 715 of which were classed as high-priority, critical or even highly critical. Many of these could be exploited easily and in some cases remotely.

Perhaps the sort of digital body enhancers that help us to stay healthy and avoid any trips to hospital are a better idea...

Read more here:

http://www.kaspersky.com/de/about/news/allgemeine/2016/Chip_unter_der_Haut_29_Prozent_sagen_Nein
http://www.computerworld.ch/news/politik-gesellschaft/artikel/chip-implantate-werden-wir-alle-zu-cyborgs-nur-29-prozent-sagen-nein-69966
https://www.wa.de/hamm/cyborg-osttuennen-hamm-reckmann-chip-implantiert-testet-bio-hacking-6263352.html
http://www.bionyfiken.se/nfc-implantproject
http://www.oe24.at/digital/Herzschrittmacher-im-Visier-von-Hackern/225607394
https://www.youtube.com/watch?v=wAg-KJQ9ACA
http://www.heise.de/newsticker/meldung/Los-Hacker-brecht-mir-das-Herz-Sicherheit-von-vernetzter-Medizintechnik-auf-dem-Pruefstand-3145186.html
http://www.wired.com/2016/03/go-ahead-hackers-break-heart
http://www.heise.de/security/meldung/Automatisierte-Medikamenten-Verteiler-mit-ueber-1400-Sicherheitsluecken-3159439.html

## III. One point three million dollar phone – FBI spends big in iPhone hacking dispute with Apple

Please excuse us for yet another movie quote: «– How was I, boss? – You were good!» This comes from Clint Eastwood's Oscar-winning film «Million Dollar Baby». The FBI appears to have spent significantly more to land a knockout blow in its fight with Apple over unlocking the iPhone 5c belonging to the San Bernadino attacker. Journalists used details disclosed by FBI Director James Coney at a security forum in London to calculate the sum of more than USD 1.3 million after it was announced on 29 March that professional hackers commissioned by the federal investigators had succeeded in unlocking the phone. Government authorities said at the end of March that this marked the end of the dispute that had lasted several weeks, but the latest developments suggest that this was only true for the San Bernadino case specifically and that Apple's fears as regards this case setting a precedent are proving to be justified. The iPhone manufacturer from Cupertino made the following statement: «Apple believes deeply that people in the United States and around the world deserve data protection, security and privacy. Sacrificing one for the other only puts people and countries at greater risk.» Shortly afterwards, the US Department of Justice made its position clear: «It remains a priority for the government to ensure that law enforcement can obtain crucial digital information, either with cooperation

from relevant parties, or through the court system when cooperation fails.» Apple wasted no time in responding: «We will continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated.»

As if to prove the point, heise.de reported two days after the «case closed» announcement that the FBI was offering its unlocking method to other federal investigators, district attorneys and authorities. Another two days later, on 2 April, the Reuters news agency quoted from a letter sent out by the FBI across the country offering to unlock phones for its partners – not just those belonging to proven criminals, but also those of suspects wherever the law and policy allow.

Apple is still refusing to hack its own phones, but it is taking a more cooperative stance as regards requests from security authorities to disclose personal data, at least where the request is backed up by a valid search warrant and approved by its lawyers. German news show Tagesschau reported on 19 April that Apple had received around 31,000 requests concerning over 167,000 devices in the second half of 2015. Most of these, believe it or not, were from Germany, although they were predominantly regarding owners' names and addresses in relation to lost or stolen devices. The number of requests concerning user accounts or data stored on devices was much lower. Apple was emphatic: «We only comply with information requests once we are satisfied that the request is valid and appropriate, and then we deliver the narrowest possible set of information.» The leading instant messaging service among young people, WhatsApp, has now also announced that all messages are end-to-end encrypted with immediate effect, meaning that third parties cannot read them. Following this update, WhatsApp says it is also unable to pass data to the security authorities.

Verena Lueken's review of the film «Million Dollar Baby» in Frankfurter Allgemeine Zeitung on 24 March 2005 serves as a commentary on this story that is right on the nose, so to speak: «This backdrop...makes an ending possible that is dark but perhaps not entirely devoid of hope.»

Read more here:

http://www.dw.com/de/fbi-zahlt-13-millionen-dollar-für-iphone-entschlüsselung/a-19207258
http://www.computerworld.ch/news/it-branche/artikel/was-das-fbi-fuer-das-hacken-des-iphones-bezahlen-musste-70072/
http://www.zeit.de/digital/datenschutz/2016-03/apple-versus-fbi-iphone-geknackt-analyse
http://www.heise.de/newsticker/meldung/Entsperrhack-FBI-will-weitere-iPhones-und-iPods-knacken-3159476.html

http://www.reuters.com/article/us-apple-encryption-letter-idUSKCN0WZ055
http://www.tagesschau.de/wirtschaft/apple-daten-sicherheit-101.html
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/mehr-sicherheit-whatsapp-will-alle-daten-verschluesseln-14162785.html
http://www.faz.net/aktuell/feuilleton/kino/video-filmkritiken/kino-ein-klassiker-clint-eastwoods-million-dollar-baby-1105370.html

## IV. It looks horrible, and it is – Jigsaw causing terror once again, this time in digital form

The US psycho-horror movie «Saw», which came out in cinemas in 2004, was among the most successful examples of the genre. In it, the Jigsaw Killer or Jigsaw for short takes people he believes are taking their lives for granted and subjects them to gruesome and cynical tests so that they can learn the true value of life. Cybercriminals are now pursuing the double motive of getting rich and making people appreciate the simple things in life. Using malvertising or compromised adult websites, they are spreading a very malicious blackmail Trojan that not only encrypts files but also deletes an increasing number of them every hour until the owner of the infected computer pays a ransom of 0.4 Bitcoins (about CHF 160). If the money is not paid within 72 hours, Jigsaw deletes all the files on the computer and displays the grimacing face of the horror doll Billy from the film. This ransomware is just one of an increasing number of ever more aggressive Crypto-Trojans in circulation. The best protection against their effects remains a carefully thought-out, systematic back-up strategy, ideally with several back-ups on media that are not connected to each other.

Read more here:

http://www.heise.de/security/meldung/Nur-72-Stunden-Erpressungs-Trojaner-Jigsaw-droht-Dateien-zu-loeschen-3172217.html
http://blog.trendmicro.de/neue-crypto-ransomware-jigsaw-spielt-fiese-spiele
http://www.n-tv.de/technik/Jigsaw-zerstoert-stuendlich-mehr-Dateien-article17515046.html
https://www.basicthinking.de/blog/2016/04/20/krypto-trojaner
http://www.nzz.ch/digital/trojaner-toolkit-spyeye-urteil-gegen-hacker-ld.15545
https://id-ransomware.malwarehunterteam.com
https://objective-see.com/products/ransomwhere.html

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