

SWITCHcert Security Report

October 2016



SWITCH

I. Swiss electorate votes in favour of Intelligence Service Act – making everyone a suspect?

In a referendum on 25 September 2016, a surprisingly large majority (65.5%) of Swiss voters came out in favour of the new Intelligence Service Act (ISA). The ISA will empower the Federal Intelligence Service (FIS) to tap phone calls, plant bugs in private places, hack into computers, manipulate them (Art. 25) and intercept data through cable lines in cases where internal and external security or significant national interests are deemed to be under threat. It will also allow the FIS to forward data it has obtained to other countries via automated information exchange processes. Examples of what the Act defines as a threat include terrorism, the dissemination of weapons of mass destruction and espionage against Switzerland. The campaign supporting the ISA argued that, among other things, it would improve security while also setting strict limits on the FIS's surveillance activities. Depending on how it plans to obtain data, the FIS will require approval either from a Federal Administrative Court judge and the Defence Minister or from the Federal Council's IT Security Committee. The parliamentary Control Delegation is to act as supervisory body, and the ISA provides for an extra body to supervise the interception of wireless communications. Nevertheless, even proponents of the ISA admit that its adoption entails a certain loss of freedom. National Councillor and parliamentary leader of the Conservative

Democratic Party Rosmarie Quadranti, for example, called for the Act to be adopted but said, «No one wants to turn Switzerland into a surveillance state, but no one wants to take the blame if something happens. This loss of freedom is probably the most heavily debated aspect at the moment...In the ISA, we have a law with virtually no impact on the freedom of normal citizens. The control mechanisms are so extensive and strictly regulated as to make large-scale surveillance and record-keeping practically impossible...It is a measured relinquishing of freedom.»

Opponents have raised two concerns. The ISA, they say, lays the foundation for developing the FIS into a huge surveillance machine modelled on the US National Security Agency. Indeed, one of the factors that led to the Act being drawn up in the first place was the merging of two separate decrees containing regulations on obtaining information in Switzerland and abroad. This mirrors the creation of the FIS itself by combining the Strategic Intelligence Service (focused on obtaining information abroad) and the Service for Analysis and Prevention (focused on obtaining information inside Switzerland) in 2010.

Far from merely being a compendium of existing rules, however, the new Act also gives the FIS extensive new powers (see the link below at www.digitale-gesellschaft.ch for a summary in German). Opponents are concerned that these powers will result in severe infringements of privacy, information sovereignty and professional confidentiality, in particular with regard to doctors and lawyers, and could thus constitute a violation of basic human rights. They also point out that no intelligence service has ever supplied credible evidence that greater powers of surveillance reduce security risks, whereas it is clear that they significantly restrict the freedom of innocent citizens.

The personal opinion of the authors of this Security Report is that the referendum on the ISA raises questions about direct democracy, although we certainly do not wish to cast doubt on its validity. Can voters really be expected to form a clear opinion on highly complex and technical issues – in this case freedom versus security – where weighing up the pros and cons is a very demanding task? How could assistance be offered in an objective and credible manner – by a committee of experts or through collective intelligence? The Security Report is clearly not the place to try and answer these questions exhaustively, but we can provide some food for thought with a quote

from the song «Freedom» by Georg Danzer: «That's the catch: you lock it up [meaning freedom], and just like that it's gone!»

Read more here:

<http://www.lrens-oui.ch/?lang=de>

<http://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/sicherheit/schweizer-nachrichtendienstgesetz>

<http://www.nzz.ch/schweiz/aktuelle-themen/abstimmung-ueber-das-nachrichtendienstgesetz-die-sicherheit-nicht-dem-zufall-ueberlassen-id.111342>

<https://netzpolitik.org/2016/geheimdienst-in-der-schweiz-stellt-bevoelkerung-unter-generalverdacht>

<https://www.digitale-gesellschaft.ch/2016/07/30/zusammenstellung-der-umfangreichen-befugnisse-fuer-den-geheimdienst-im-neuen-nachrichtendienstgesetz>

<https://steigerlegal.ch/2016/01/11/nachrichtendienstgesetz-sicherheitsesoterik>

II. Your money or your device – mobile banking Trojan Gugi tricks Android users

Gugi may sound cute, but it is actually the name of an insidious Trojan that infects smartphones and confronts their owners with a choice of either accepting that their phone is locked or granting overlay rights that can be used to clear out their e-banking accounts. Versions 6 (Marshmallow) and above of Android force apps to request permission for overlays, which allow malicious apps to add their own user interface elements such as input, navigation and control functions to legitimate apps. These can be used to access victims' login or banking details, for example.

Over the summer, security experts at Kaspersky discovered a new version of the mobile banking Trojan known as Gugi that gets around this block on overlays by forcing its victims to allow them. If a user refuses to do so, Gugi completely locks the infected device. If the user capitulates and gives permission for overlays, the Trojan copies credit card details in the background when credit card payments are made inside apps and banking details when e-banking apps are used.

Gugi first emerged in Russia, but it has spread rapidly via social engineering and use by cybercriminals. According to Kaspersky, the number of victims rose tenfold between April and the start of August 2016.

This seems like a good place to reiterate these seven useful tips for preventing the spread of malware like this and protecting your devices:

1. Never give any automatic rights or permissions to any apps.

2. Never click on links in unexpected text or multimedia messages from unknown sources on any device.
3. Exercise caution on websites (suspicious items are usually easy to spot).
4. Only download apps from official app stores.
5. Install a leading antivirus program for Android.
6. Avoid connecting to unknown Wi-Fi hotspots.
7. Install a VPN on your smartphone and use it wherever possible.

Read more here:

http://www.heise.de/security/meldung/Banking-Trojaner-Gugi-umgeht-Overlay-Sperre-in-Android-Marshmallow-3315473.html?wt_mc=rss.security.beitrag.rdf

<http://www.computerwoche.de/a/banking-trojaner-trickst-android-6-0-aus,3322716>

<http://newsroom.kaspersky.eu/de/texte/detail/article/banking-trojaner-gugi-ueberlistet-neue-sicherheitsfunktionen-von-android-6>

<http://www.pc-magazin.de/vergleich/android-antivirus-test-security-apps-vergleich-3195548.html>

III. SWIFT, and it's gone – banks lose money to hackers again following SWIFT data theft

What banking security people had suspected since the huge cyber bank job on Bangladesh Bank (as we reported back in April) was officially confirmed at the start of September: The Belgium-based Society for Worldwide Interbank Financial Telecommunication, SWIFT for short, has admitted that further banks have since been hacked and had money stolen from them. SWIFT warned that the threat will persist because the perpetrators can keep adapting to new situations. The payment services provider called on the 11,000 financial institutions around the world that are affiliated to it to step up their security considerably. It even threatened to report negligent members to the regulators or other institutions, clearly taking the view that a chain is only as strong as its weakest link.

SWIFT has thus fallen into line with all the banking security specialists who believe that it needs to do more to check the extent to which its members are protecting themselves against cyber attacks and to motivate them to share knowledge of attack patterns with each other. Without wishing to gloat, we are pleased to note that

SWITCH-CERT has now been setting standards in this area as part of trustful communities since it was formed some 20 years ago on 20 September 1996.

The European Central Bank and its Single Supervisory Mechanism (SSM) have also expressed their alarm. The SSM has started a pilot project together with 18 supervised banks that is building a database of major bank hacks as a basis for an analysis and early-warning system. SWIFT itself also intends to increase its efforts. Some 22 years after the Banking Telecommunication Message was launched, it is looking into various security options, including an authentication system that is supposedly even more secure than the two-factor model and an anomaly alarm similar to that used for credit card transactions.

Read more here:

<http://www.n-tv.de/wirtschaft/Hacker-knacken-globales-Zahlungssystem-article18586731.html>

<https://www.switch.ch/de/dossiers/20-years-of-switch-cert>

<http://www.nzz.ch/wirtschaft/wirtschaftspolitik/banken-swift-meldet-cyber-angriff-auf-weitere-bank-ld.82361>

https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

<https://www.heise.de/security/meldung/Nach-Angriffen-auf-Banken-SWIFT-will-Sicherheit-verstaerken-3221218.html>

IV. It was just a question of time – botnet discovered on Internet of Things

It was bound to happen sooner or later. Security experts at MalwareMustDie have now found a Trojan that opens up a back door on IoT devices running outdated LINUX-based firmware. This allows cybercriminals to link up the devices, for instance hardwired IP cameras, into botnets used to distribute spam or malware. Both the Trojan and the whole process are especially sneaky in two respects. Firstly, hardwired cameras are hardly ever rebooted (which would remove the malware). Secondly, the Trojan clears its tracks after infecting a device and hides in its RAM. This is why the experts at CZ.NIC, the Czech Republic's top-level domain registry, initially failed to spot it. They had bought an infected camera after noticing a sudden jump in activity on their Telnet honeypot. This proved to be instrumental in discovering the Trojan and the IoT botnet. There are three security measures that all users of older IoT devices urgently need to take:

1. Reboot the device (this is hardly ever done with hardwired cameras, but it helps).
2. Deactivate Telnet on the device or at least keep a close eye on Telnet connections. Protect the device with a firewall and block Internet connections on Port 48101/TCP if possible.
3. These devices should under no circumstances be run without a firewall.

Read more here:

<http://www.heise.de/newsticker/meldung/Sicherheitsexperten-finden-IoT-Botnet-3317830.html>

<https://en.blog.nic.cz/2015/06/16/more-about-the-honey-pot-for-telnet-and-botnets>

<http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linux-mirai-just.html>

<http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html>

<http://t3n.de/news/iot-botnet-fiese-linux-malware-744891>

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.