SWITCHcert Security Report

September 2014

SWITCH

I. Hacked, tweeted and exposed: inside information on government Trojans used internationally published on Twitter

The globally active Gamma Group has been criticised for some time due to the fact that its spy software suite FinFisher and above all the monitoring tool FinFisher FinSpy have also been used in undemocratic and autocratic states to keep track of members of the opposition. Swiss firm Dreamlab Technologies AG played a key role in the development of FinSpy. Now it would appear that Gamma Group company FinFisher GmbH in Munich has been hacked. Since the start of August, detailed price lists, manuals and source code for individual programs in the suite have been published via the Twitter account @GammaGroupPR. While the authenticity of the documents has not yet been officially confirmed, network news portal NETZPOLITIK.ORG claims to have verified them.

What does seem certain is that Germany's federal investigation agency BKA is using FinFisher as a «transitional solution». Work on a «small» government Trojan to monitor telecommunications at source has been delayed by conditions imposed by the Federal Constitutional Court in 2008. While monitoring at source only affects certain individual VoIP services, such as Skype, and instant messaging, the BKA's «large» government Trojan, which is ready for use, sifts through the entire content of a target system online.

© SWITCH 2014

In Switzerland, the Federal Criminal Police insists that it has not used Trojans since 2011 following massive criticism by experts of its use of them up to then and that it will maintain this stance at least until the fundamental revision of the Federal Act on the Surveillance of Post and Telecommunications is complete. The National Council's Committee for Legal Affairs decided in mid-August to postpone the consultation until next quarter. This means that the proposal will not be debated by parliament until the winter session at the earliest.

Read more here:

http://t3n.de/news/finfisher-staatstrojaner-gamma-international-561277

https://netzpolitik.org/2014/grosser-bundestrojaner-inzwischen-einsatzbereit-kleiner-bundestrojaner-wird-noch-eine-zeitlang-ausprobiert

http://www.tagesanzeiger.ch/schweiz/standard/Dein-Freund-und-Hacker/story/22064216

http://www.nzz.ch/schweiz/nationalratskommission-kritisch-gegenueber-buepf-1.18363983

II. Page not found: network blocking in Switzerland and neighbouring countries

The Higher Regional Court in Cologne ruled in June that Internet service providers are not obliged to block websites containing links to copyrighted content posted illegally. In the final week of August, meanwhile, the anti-piracy association VAP took Austria's top four ISPs A1, Tele2, Drei and UPC to court to get the two torrent portals kinox.to and movie4k.to blocked. The Austrian music industry association IFPI is expected to follow this lead soon with a lawsuit to block thepiratebay.se, isohunt.to, 1337x.to and h33t.to. Since these websites can also be used to find legal content, however, it is likely to be much harder to weigh up the violation of copyright against the right to access information in this case. The combination of DNS and IP blocking demanded by the complainants could also lead quickly to «overblocking».

Nevertheless, even the Swiss working group on copyright AGUR12 recommended in its Final Report at the end of 2013 that blocking be used to protect copyright on the Swiss Internet.

There is set to be more blocking in France going forward, albeit to combat terrorism rather than to protect copyright. New draft anti-terror legislation to be voted on this

© SWITCH 2014

month stipulates, for instance, that pages with instructions on how to build bombs and other terrorist content should be blocked.

See

http://futurezone.at/netzpolitik/netzsperren-klagen-bei-vier-providern-eingetroffen/82.780.541

http://www.heise.de/newsticker/meldung/OLG-Koeln-Provider-nicht-zu-Netzsperren-gegen-widerrechtliche-Angebote-verpflichtet-2292330.html

https://www.digitale-gesellschaft.ch/tag/netzsperren

https://netzpolitik.org/2014/neuer-anti-terrorismus-gesetzentwurf-in-frankreich-weitet-netzsperren-aus

III. Breaking bad – malvertising ransomware: ZeroLocker/CryptoLocker/CryptoWall/SynoLocker

«Long gone are the days when you had to be browsing shady areas of the net to stumble across something malicious,» notes security expert Graham Cluley in his blog on the current spread of digital extortion using malware. Clicking on a banner advertisement is often enough to get a nasty surprise with a name like ZeroLocker, CryptoLocker, CryptoWall or SynoLocker. These programs encrypt either predefined files or all files on the infected computer – or, in the case of SynoLocker, on Synology mass storage devices – and prompt users to buy a key within a few days to free themselves from this digital kidnapping. The «ransom» demanded for the key rises exponentially over time. Payments start at around USD 300 and can in many cases only be made using digital currency such as Bitcoins. While CryptoWall genuinely releases the files once the key is bought, a programming error in ZeroLocker means that files will not definitely be restored. Security experts and criminal prosecutors advise against making a payment in all cases and recommend restoring systems from backups or, wherever possible, using services such as DecryptCryptoLocker. As a preventive measure, using up-to-date security software and secure backup systems is strongly recommended.

Read more here:

http://www.zdnet.de/88202879/kaspersky-warnt-vor-neuer-erpresser-malware-zerolocker

http://grahamcluley.com/2014/08/yahoo-cryptowall

https://www.decryptcryptolocker.com/

http://community.spiceworks.com/how_to/show/85802-how-to-recover-files-from-cryptowall-ransomeware-infection

© SWITCH 2014

IV. Canvas or cookies – choosing between Scylla and Charybdis

It is well known that turning off cookies in your browser does not mean that your Internet use is not being tracked. A whole range of alternative techniques can be used to obtain a more or less unique fingerprint from browsers. Canvas fingerprinting is a relatively new tracking method. A canvas is a website element that dynamically generates graphics using JavaScript. Fingerprinting identifies minimal differences between the canvas elements generated by individual browser installations and outputs them as a unique numerical code. Services such as the bookmarker AddThis and many other well known websites already use this type of tracking – usually without informing users that they are doing so. AddThis is virtually unrivalled in its temerity: the «trackie» offers users an opt-out cookie to protect against its canvas technology, but this of course only works if the browser is set to allow cookies. More effective protection can be achieved, however, by turning off JavaScript – which naturally entails a loss of functionality – or using tools such as NoScript.

Read more here:

http://www.spiegel.de/netzwelt/web/canvas-fingerprinting-macht-internetnutzung-nachverfolgbar-a-982280.html

http://www.chip.de/news/Canvas-Fingerprinting-Adblock-Plus-stoppt-Tracking_71140183.html

https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

https://sites.google.com/a/chromium.org/dev/Home/chromium-security/client-identification-mechanisms

© SWITCH 2014

The Clipboard: Interesting presentations, articles and videos

Konstantinos Karagiannis is a security specialist in the banking and financial sector. His talk at the last DeepSec conference dealt with a broad range of topics, starting with the true risks of user name enumeration and moving through security problems in high-frequency trading to quantum computing, which could change everything before the decade is out:

http://blog.deepsec.net/?p=1790

Bruce Schneier – new Chief Technology Officer of Co3 Systems – reported on the challenges of incident response at the Black Hat conference. His interview in the Security Advisor Alliance podcast on the same topic is also of interest:

https://www.youtube.com/watch?v=u54Radu2bFO&list=UUJ6q9le29ajGqKApbLqfBOg:

http://securityadvisoralliance.libsyn.com/11-security-advisor-alliance-ep11-ir-redux

The National Institute of Standards and Technology (NIST) has published a draft entitled «Security of Automated Access Management Using Secure Shell». It concerns the risks involved in companies having inadequate SSH key management or none at all:

http://www.bankinfosecurity.com/ssh-keys-managing-risks-a-7248

http://csrc.nist.gov/publications/drafts/nistir-7966/nistir_7966_draft.pdf

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

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 2014