SWITCHcert Security Report

March/April 2017

SWITCH

I. Cybercriminals increasingly targeting Mac users

Back in 1993, Austrian singer Rainhard Fendrich sang «nobody's safe any more, it's the curse of our times», alluding to the fact that regions long presumed secure had become just as threatened as Jericho and Troy once were. Now a new breed of Trojan is attacking computers that run Mac OS, the users of which had previously thought that they were safe from malware. Security firm Sixgill found an offering on a Russian cybercrime message board that was developed especially for deployment against Mac users. Called Proton, this Trojan poses as a remote administration tool and can allegedly log keystrokes, take screenshots, upload files and execute command-line instructions using root privileges. Proton can be equipped with a security certificate to ensure that Apple's built-in protection feature Gatekeeper does not sound the alarm. The full package for EUR 45,000 includes a licence for unlimited installations plus a kind of «pull» marketing: to motivate Mac users to install the malware, it is advertised as a remote maintenance and monitoring tool or even home banking software. Individual licences are also available, currently costing two bitcoins or roughly CHF 2,500.

Meanwhile, welivesecurity.com reports on another decidedly malicious crypto-ransomware campaign against Apple users. The cybercriminals behind the Trojan, written in Swift, demand a ransom but cannot offer a key to free the hijacked files.

This means that, even if you pay 0.25 bitcoins for supposed decryption within 24 hours or 0.45 bitcoins for immediate restoration, you will still lose all the files on your Mac. The malware, disguised as a patcher for cracking Adobe and Microsoft programs, infiltrates Macs via downloads from various torrent sites (see second link below for details).

Bill Brenner also discusses how cybercriminals seem to have discovered Mac users as a new target group in his Naked Security blog. He notes that some criminals have already gone a step further and developed hybrid malware that can compromise computers running either Windows or Mac OS. Masquerading as a Word document, it prompts users to turn on macros so that it can connect the infected computer to the cybercriminals' servers, although it is unclear as yet what they then do with it.

In contrast to these nebulous intentions, suspicions that the CIA had hacked Apple's Ethernet/Thunderbolt adapter were recently confirmed. This allows the CIA to access any Mac OS device and install malware that cannot be removed even by completely restaging the operating system. While the authenticity of the documents published on WikiLeaks at the end of March was initially called into question, Spiegel Online reports that both the CIA and the FBI now believe them to be genuine. It would seem that even Macs are not immune to the curse of our times.

Read more here:

https://www.heise.de/newsticker/meldung/Proton-Signierter-Mac-Trojaner-wird-fuer-45-000-Euro-gehandelt-3655096.html
https://www.welivesecurity.com/deutsch/2017/02/23/neue-crypto-ransomware-mac-os
http://www.silicon.de/41641273/eset-warnt-mac-nutzer-vor-neuer-ransomware
https://nakedsecurity.sophos.com/2017/03/21/your-mac-is-not-malware-proof-a-look-at-the-threats-and-defenses
https://threatpost.com/malware-that-targets-both-microsoft-apple-operating-systems-found/124531
http://www.spiegel.de/netzwelt/netzpolitik/wikileaks-enthuellung-vault-7-so-soll-die-cia-auf-apple-geraete-zugreifen-a-1140065.html

II. Malware fitted as standard for Android

To clarify, the malware security researchers found on 36 Android mobile devices was not actually installed at the factory but on the way from the manufacturer to an unnamed telecom firm and a multinational technology corporation. Android smartphones and tablets from almost all manufacturers including Asus, Lenovo, LG, Oppo, Samsung, Xaomi and ZTE are affected. It is at present a complete mystery how the malicious programs found their way onto the devices. What is known, according to the blog checkpoint.com, is that they spy on the device and install an ad network that generates advertising income by fraudulent means. The blog adds that a ransomware function for encrypting files and demanding money to unlock them is also installed. The malware is not installed in the devices' ROM, but it uses system rights and can thus only be removed by a full factory reset.

We covered a different threat to Android devices from various Chinese manufacturers in the SWITCH Security Blog in February. It installs firmware over the air (FOTA) from the Shanghai-based company Adups in place of the original Google Update system. As a system Android package or APK, the FOTA has unrestricted access to all files on a device and makes extensive use of them to send details of usage, contacts and contact history (including addresses and content shared), as well as the unique identification codes IMSI and IMEI, to servers controlled by unknown third parties. The Kryptowire article linked to below lists the capabilities of this firmware, which makes no attempt to disguise itself. Like our blog article, it also shows how privacy and security are under threat from all sides and makes it clear that there is no simple solution to the problems outlined.

Read more here:

http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users
http://www.kryptowire.com/adups_security_analysis.html

III. Casinos on a losing streak? Start blocking websites! Switzerland breaks taboo of Net neutrality for sake of CHF 320 million

Switzerland is breaking with a taboo and blocking foreign online casino sites after a brief but heated debate. At the same time, the National Council passed a new Gambling Act at the end of February, laying the foundation for domestic casino operators to acquire concessions for online gambling and thus – at least to some extent – making a mockery of the argument that websites should be blocked to protect gamblers.

According to Federal Councillor Simonetta Sommaruga, the blocking has nothing to do with censorship because that concerns the media and not commercial activities. Opponents of the blocking see it as disproportionate and fear above all that it signals the beginning of the end for Net neutrality. If casino sites can be blocked, others can too. On top of this, blocking creates more problems than it solves, can be circumvented easily and is much less effective than removing illegal content and prosecuting those who created it. The block on casino sites is entirely about money, and lots of it: in 2015, betting at Swiss casinos contributed CHF 47 million to cantonal tax revenues and a further CHF 273 million to the social security system. This source of income is under threat because more and more gamblers are switching to online casinos, casinos in other countries and unlicensed Swiss gambling clubs, depriving Switzerland's licensed operators of hundreds of millions of francs in bets.

Read more here:

http://www.tagesanzeiger.ch/schweiz/standard/die-schweiz-bricht-tabu-und-sperrt-websites/story/12456995
https://www.srf.ch/news/schweiz/session/parlament-will-unbewilligte-online-gluecksspiele-sperren
https://www.nzz.ch/schweiz/geldspielgesetz-nationalrat-will-netzsperren-fuer-online-geldspiele-ld.148619
https://netzpolitik.org/2017/schweiz-fuehrt-netzsperren-fuer-gluecksspielangebote-ein
http://www.luzernerzeitung.ch/nachrichten/schweiz/Netzsperren-sind-unverhaeltnismaessig;art9641,976775
https://www.srf.ch/news/schweiz/session/netzsperren-bringen-statt-loesungen-nur-probleme
http://www.luzernerzeitung.ch/nachrichten/schweiz/Schweizer-Spielcasinos-darben;art9641,941488
https://de.wikipedia.org/wiki/Zensur_im_Internet

IV. Internet of Things toys spying on children of all ages

An article in the SWITCH Security Report back in May 2015 revealed how smart toys like Hello Barbie were spying on children's bedrooms, recording their conversations with children and sending them back to manufacturers. In November that year, The Guardian warned that Hello Barbie was an easy target for hackers that allowed them not only spy on children but also to access entire Wi-Fi networks.

Oren Jacob, CEO of system manufacturer ToyTalk, said in 2011, «No user data, no Barbie content, and no major security or privacy protections have been compromised to our knowledge.» Now, however, 2.2 million voice files have been posted online that were recorded by CloudPets-branded teddy bears using a system from Spiral Toys. Germany's Federal Network Agency banned the My Friend Cayla smart doll in February. The agency believed that the combination of a microphone with voice recognition, an inadequately secured Internet connection , questionable data protection clauses in the terms and conditions and information being forwarded to third-party companies in the US qualified the Cayla doll as an illegal espionage device rather than a harmless toy and asked all parents to destroy it.

It seems that security vulnerabilities and unsolicited data transfers are not restricted to toys for children. The whole controversy becomes even more serious when adult toys are affected. In March this year, the case of smart sex toys from the Canadian manufacturer We-Vibe went public. The company had, «for market research purposes and without any scope for analysis relating to specific individuals» (or so it claimed), collected data on usage times and durations as well as selected vibration modes from its smartphone-controlled sex toys – without asking users for their permission. We-Vibe is now faced with compensation claims totalling up to CAD 4 million.

As if this were not enough in itself, news broke just before the Security Report's editorial deadline of Siime Eye, a smart vibrator with a built-in camera that could be snooped on from across the street. Equipped with a Web interface, the device has the default user name «admin» and password «blank» for Web access.

Read more here:

http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05_de.pdf
https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children
https://www.heise.de/security/meldung/Cloudpets-2-2-Millionen-Sprachdateien-von-Kinderspielzeug-offen-im-Netz-3637923.html
http://www.computerbild.de/artikel/cb-News-Sicherheit-CloudPets-Sicherheit-17471813.html

http://derstandard.at/2000052783832/Behoerde-Eltern-muessen-Puppe-My-Friend-Cayla-zerstoeren
http://www.primelife.co/lovely-wearable-fuer-sex
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-08.pdf
http://www.newsweek.com/sex-toys-connected-internet-risk-being-hacked-437366
https://www.nzz.ch/datenschutz-sex-toy-hersteller-spionierte-kunden-aus-ld.151135
https://www.heise.de/security/meldung/Svakom-Siime-Eye-Vernetzter-Kamera-Vibrator-ist-ein-Sicherheitsalptraum-3674827.html

New SWITCH-CERT Security Blog entries

Adups — The Spy in your Pocket

A «firmware over the air» updater that phones home:
https://securityblog.switch.ch/2017/02/28/adups-the-spy-in-your-pocket/

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.