SWITCHcert Security Report

March 2015

SWITCH

I. Fish bites angler – Lenovo, Komodia and Superfish

Bait the hook to suit the fish, not the angler. This saying from the age of analogue advertising means that ads need to be geared to their target audience, not the decision-makers at the advertising company. «Digital badvertising» has reached a new, worrying low with Superfish. The fish now bites the angler, or more precisely users of laptops sold by Chinese hardware giant Lenovo with bloatware from Superfish and its creator Komodia preinstalled. Besides the usual «crapware» annoyances, these laptops suffer from two serious security problems. Problem number 1: Superfish installs its own root certificate to display ads even on encrypted websites and spy on connections users believe to be secure. For this alone, Superfish, Komodia and Lenovo jointly deserve an award for the most shameless (civilian) IT security manipulation of the year. It gets worse, however, which brings us to problem number 2: Superfish manipulates the Windows security architecture in such a way as to leave the door wide open for cybercriminals to carry out man-in-the-middle attacks. This was discovered when Chris Palmer, a security engineer working for Google, fell victim to just such a hack of his Bank of America connection on his newly bought Lenovo laptop and shared details of it with the IT security community. Lenovo's initial

response was almost cynical: «...we preinstalled a piece of third-party software, Superfish, on some of our consumer notebooks. The goal was to improve the shopping experience using their visual discovery techniques.» Superfish CEO Adi Pinhas also refused to accept any blame for the problems, passing the buck instead to the SSL intercept component bought in by Komodia and advertised on the latter's website as an «advanced SSL hijacker».

The irony of it all is that this advanced hijacker also forms part of the Lavasoft anti-adware software and the parental control freeware KeepMyFamilySecure, prompting CERT/CC to issue a warning against these and around a dozen other pieces of software. This means that, in addition to Lenovo laptops, any computer on which one of the programs on the list has been installed is at risk.

All parties involved have now promised improvements – not least because Lenovo in particular is threatened with class action lawsuits. Lenovo says that it will no longer install Superfish and is offering an automated deinstallation tool. Superfish claims that it will remove the Komodia hijacker, and Komodia itself plans to release a less hazardous update. Nevertheless, users are strongly advised to test Lenovo laptops from the affected model lines and all computers that have the programs in question installed and remove the malware and the certificate wherever they are found (see the links to filippo.io below).

Read more here:

http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl

http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections

http://blog.erratasec.com/2015/02/some-notes-on-superfish.html

http://www.kb.cert.org/vuls/id/529496

http://www.heise.de/security/meldung/Gefaehrliche-Adware-Mehr-als-ein-Dutzend-Anwendungen-verbreiten-Superfish-Zertifikat-2557619.html

http://www.nzz.ch/mehr/digital/lenovo-superfish-visual-discovery-sammeklage-1.18488867

http://support.lenovo.com/en/product_security/superfish_uninstall

https://filippo.io/Badfish

https://filippo.io/Badfish/removing.html

II. Gemalto-gate – secret service hack goes right to the roots of mobile security

If Superfish marks a new low in shameless civilian snooping, the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) have gone one better with their attack on Gemalto, the Netherlands-based «world leader in digital security» (according to its own advertising). Gemalto is the world's largest manufacturer of SIM cards, producing around two billion of them a year and supplying them to customers and government agencies around the globe along with credit card chips, access control and payment systems, passports and other ID cards. Following its acquisition of Aargau firm Trüb AG, Gemalto is also a key player on the Swiss security market and producer of the SwissPass system for electronic travelcards and the SuisseID. Investigative website The Intercept received presentation slides produced by the UK intelligence service from the files of Edward Snowden showing that GCHQ and the NSA stole encryption keys for Gemalto SIM cards in a state-sponsored smash-and-grab raid in 2010. German TV current affairs programme Tagesschau found out that the SIM cards in question are used in roughly half of all German mobiles. In Switzerland, mobiles on all three networks are equipped with the SIMs. In addition, both countries use SIMs from the German supplier Giesecke & Devrient, which the Snowden papers also name as a target of the two spy agencies, although it claims not to have found any evidence of an attack and insists that its SIMs are still secure. Gemalto is now saying the same, although its management appeared to be devastated immediately after the revelations came to light and promised to do all they could to investigate the circumstances of the attack and its consequences. Just a week later, following its initial investigations, the company said that Gemalto cards were secure and that it was not expecting any significant claims for compensation.

Gemalto may yet face claims, however, arising from another mishap dating back to 2010, when 30 million debit and credit cards fitted with Gemalto chips suddenly stopped working. Even now, they are only partially usable, if at all. Gemalto has now accepted responsibility for this problem and attempted to deter compensation claims from the financial institutions affected by providing software updates.

The spy agencies could also face similar claims from political circles. Austrian Green Party MP Peter Pilz, for example, has demanded that his government sue the company and impose sanctions on both of the offending agencies, especially since the UK's Investigatory Powers Tribunal (IPT) ruled at the end of January that the large-scale collection of private data violates the European Convention on Human Rights.

Read more here:

https://firstlook.org/theintercept/2015/02/19/great-sim-heist

http://www.inside-it.ch/articles/39285

http://www.tagesschau.de/sim-karten-kryto-101.html

http://www.computerworld.ch/news/security/artikel/nsa-im-besitz-von-sim-karten-codes-schweiz-ev-betroffen-67361

http://www.computerworld.ch/news/it-branche/artikel/gemalto-unsere-sim-karten-sind-sicher-67373

http://motherboard.vice.com/read/worlds-largest-sim-card-maker-has-no-clue-whether-it-was-hacked-by-the-nsa

http://www.theregister.co.uk/2015/02/25/gemalto_everythings_fine_security_industry_hang_on_a_minute/

http://www.spiegel.de/wirtschaft/unternehmen/kartenpanne-franzoesische-firma-schuld-an-2010-fehler-a-670400.html

http://futurezone.at/netzpolitik/urteil-methoden-des-britischen-gchq-teils-illegal/112.357.248

III. Carbanak – digital bank robbery on a grand scale

Yet more incredible audacity of the most criminal kind: according to a report by Kaspersky, the criminal organisation Carbanak has stolen between USD 300 million and USD 1 billion from more than 100 financial institutions around the world since 2013, and the attacks are still ongoing. This mega-raid follows years of painstaking preparations and shows just how committed the criminals are. Targeted spear-phishing attacks were used to infect employees' computers with a back door granting access to the bank's internal network. The next step involved recording the activities of employees who look after systems for transferring money. The computers that control video surveillance were tracked down and taken over for this purpose. The aim was to collect enough information to be able to imitate the bank employees' behaviour in order to transfer funds or have them paid out in cash. Carbanak does this in a number of ways, including direct transfer or payout via e-payment systems, covert manipulation of client

accounts and instructions sent to ATMs to dispense cash at a specific time when a middleman is standing by to collect it. Despite its best efforts to keep all this under wraps, the theft came to light because not all the middlemen were there at the right time, which allegedly caused the ATMs to throw cash out uncontrollably into the street.

Security experts are surprised not only by the scale of these crimes, but also by the fact that the attacks were carried out – and continue to be carried out – regardless of the software in use.

See the PDF at the final link below for a detailed account of this case.

Read more here:

http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitu

https://www.wired.de/collection/latest/carbanak-der-grosste-bankraub-aller-zeiten

http://futurezone.at/digital-life/massiver-cyberangriff-auf-banken-in-europa-und-usa/113.971.500

http://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts

https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

IV. It's not all bad news – Europol takes down Ramnit botnet

Since 2010, the Ramnit botnet has infected more than 3.2 million computers with malware through drive-by downloads from malicious websites and e-mails. The malware allowed Ramnit's operators to take control of the infected computers in order to steal passwords or personal data, send further spam messages or launch illegal attacks on other websites. In a concerted action that also involved Microsoft, Symantec and AnubisNetworks, Europol's European Cybercrime Centre (EC3) worked with police in Germany, the UK, Italy and the Netherlands to take down the botnet. Given its size, the authorities are appealing to all users to test their computer and disinfect it if necessary. Microsoft and Symantec have both released tools for this purpose (see links below). This European success appears to have motivated the FBI to put a USD 3 million bounty on the head of the Zeus botnet, who is also one of the originators of the crypto-locker method (see Security Report, September 2014). Russian Evgeniy Mikhailovich Bogachev is accused of infecting over a million computers and causing financial losses of

more than USD 100 million. Bogachev can thus claim the dubious record of having made it onto the FBI's «Most Wanted» list with the highest bounty ever offered for a cybercriminal.

Read more here:

http://www.zdnet.de/88220112/europol-zerschlaegt-mithilfe-des-bka-botnet-ramnit

http://windows.microsoft.com/en-us/windows/detect-remove-ramnit-virus

http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

http://www.spiegel.de/netzwelt/web/zeus-botnet-fbi-setzt-drei-millionen-dollar-kopfgeld-aus-a-1020383.html

V. How to open BMWs and Rolls-Royces by remote control

Immediately after the last Security Report went to press with its article on automotive security, the German automobile association ADAC hit the headlines with a test proving that around 2.2 million BMWs, MINIs and – this is where it gets really interesting – Rolls-Royces built between March 2010 and December 2014 were relatively easy to open by hacking their Connected Drive system with a smartphone. BMW confirmed the test results. It is offering an update and has set up a hotline. See the Heise link below for details of the hack.

Read more here:

http://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html

http://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/bmw-luecke.aspx

http://www.computerworld.ch/news/security/artikel/bmws-lassen-sich-mit-dem-smartphone-oeffnen-67243

The Clipboard: Interesting Presentations, Articles and Videos:

Cisco's security blog has a good article on Angler, currently «the best exploit kit on the market», including a discussion of domain shadowing.

http://blogs.cisco.com/security/talos/angler-domain-shadowing

«11 Ways To Track Your Moves When Using a Web Browser» is the latest blog article from the SANS Institute about user tracking on the Internet.

https://isc.sans.edu/forums/diary/11+Ways+To+Track+Your+Moves+When+Using+a+Web+Browser/19369/

Spain's CERTSI has published a highly informative study on Android malware.

https://www.incibe.es/CERT_en/publications/Studies/android_malware_situation_en

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