SWITCHcert Security Report

December 2015

SWITCH

I. Pavlov in Paris – how the conditioned response to terrorist attacks links the real and online worlds

The fact that the real and online worlds are much more closely linked to each other than we like to assume becomes abundantly and tragically clear in the aftermath of terrorist attacks like those in Paris. It is particularly frustrating to note that, from the early days of the Red Army Faction through to 9/11 and Paris, such incidents bring about a kind of cynical reflex reaction that calls to mind Ivan Petrovich Pavlov's classical notion of conditioning. The more brutal and dehumanising the stimulus, namely the attack, the louder the response in terms of calls for increased online surveillance, data gathering and storage by security authorities and restrictions on freedom of information.

In view of the severity of the Paris attacks, it was only to be expected that these words would very quickly be followed by actions. The state of emergency declared immediately after the bloodshed has had an impact on the virtual world as well as the real one. The recent extension of emergency powers means that France's Minister of the Interior is authorised to block websites and social media services where there are grounds for suspicion without needing a court order. EU ministers, for their part, adopted a package of anti-terror measures that – quite predictably – entail a massive increase in the amount of data being stored.

Also foreseeable and almost grotesquely routine is how spammers and cybercriminals spring into action after an attack, shamelessly exploiting people's sadness, sympathy or fear to distribute viruses and other malware via fake solidarity or warning e-mails.

That said, there is also good news. Facebook, Google, Twitter, Airbnb, Skype and other mobile communication providers made apps, tools and other services available at short notice to deliver assistance, information and solidarity from the online world into the real one.

Read more here:

http://futurezone.at/meinung/terror-in-paris-ein-ueberwachungsaufschrei/164.022.301
http://www.heise.de/newsticker/meldung/Pariser-Anschlaege-Polizei-ruft-nach-erweiterter-Vorratsdatenspeicherung-2921757.html
http://www.nzz.ch/newsticker/grossbritannien-will-anti-terror-gesetze-deutlich-verschaerfen-1.18431200
http://www.welt.de/politik/ausland/article148847901/Ausnahmezustand-in-Frankreich-Was-heisst-das.html
http://futurezone.at/netzpolitik/frankreich-darf-nun-soziale-netzwerke-und-webseiten-sperren/165.004.716
http://www.heise.de/newsticker/meldung/Antwort-auf-Terror-von-Paris-Grenzkontrollen-Datensammlungen-Datenaustausch-3010264.html
http://futurezone.at/digital-life/warnung-vor-spam-welle-nach-anschlaegen-in-frankreich/164.511.959
http://www.salzburg.com/nachrichten/welt/politik/sn/artikel/innenministerium-warnt-hinterhaeltiger-paris-virus-verbreitet-173661/
http://www.theguardian.com/technology/2015/nov/16/facebook-safety-check-technology-paris-terrorist-attacks

II. «Added value» as standard – new devices delivered complete with malware and extra vulnerabilities

Back in March this year, we covered the Lenovo/Superfish scandal in the Security Report. It is not unreasonable for buyers of technology products to assume that new devices come out of the factory clean, i.e. free from malware and serious vulnerabilities. Now it has emerged that Dell has also supplied computers with built-in «root certificate back doors» that actually constitute massive attack vectors. In addition to the certificate itself, Dell installed a private key that could allow hackers to intercept HTTPS-encrypted connections using a man-in-the-middle attack. Like Lenovo before it, Dell apologised in its in-house blog, explaining that the certificate had been installed in an effort to provide better customer service and support. The Texan firm's blog also included instructions and a tool for removing the certificate. However, just when everyone thought the problem had been dealt with, observant users found the next one, Dell System

Detect, which can be downloaded from Dell's website and creates the same security issues as eDellRoot.

However, it is not only direct retailers that are supplying brand-new hardware infected with malware. According to The Register, it emerged in November that tens of thousands of tablets sold by Amazon under various brand names were infected with Cloudsota. This Trojan makes it impossible to close advertisements by clicking on them, uninstalls security software and apps and automatically reinstalls itself when removed.

The latest Conficker case seems even sneakier. Conficker was caught back in 2010 trying to compromise the networks of Manchester's city council and police after infiltrating them through security holes in Windows. Now it has been sighted in Florida. It was well hidden in two police bodycams being used in work to develop a cloud-based storage system for the authorities and police.

However, security problems are not the sole preserve of discount tablets from China and one or two bodycams. The security experts working on Google's Project Zero found no fewer than 11 high-risk security bugs in the version of Android modified by Samsung for its flagship Galaxy S6 Edge smartphone.

Read more here:

http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-03_de.pdf
http://www.zdnet.de/88252615/superfish-20-dell-liefert-computer-mit-vorinstalliertem-root-zertifikat-aus
https://blog.hboeck.de/archives/876-Superfish-2.0-Dangerous-Certificate-on-Dell-Laptops-breaks-encrypted-HTTPS-Connections.html
http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate
http://www.golem.de/news/https-verschluesselung-noch-ein-gefaehrliches-dell-zertifikat-1511-117615.html
http://www.theregister.co.uk/2015/11/13/amazon_vendors_flog_thousands_of_rooted_malwareladen_tablets
http://futurezone.at/digital-life/tablets-mit-vorinstallierter-malware-im-angebot-von-amazon/163.251.676
http://winfuture.de/news,53287.html
http://www.zdnet.com/article/crooks-use-old-school-conficker-virus-to-infect-police-body-cams
http://blog.check-and-secure.com/trojanisierte-body-cams_15-11-19
http://www.theguardian.com/technology/2015/nov/04/google-samsung-galaxy-s6-edge-high-impact-security-bugs

III. Silent profilers – audio beacons allow advertisers to operate extensive tracking

Our last Security Report included some good news. A team of researchers at ETH Zurich had used sound to make two-factor authentication much simpler.

This time round, we take a look at the dark side of this particular force, which lurks in the on-board microphones of tablets, smartphones, laptops and desktops. Advertising companies have for over a year been using a sound-based tracking technology marketed mainly by the start-up firm SilverPush, with companies such as Adobe, Drawbridge and Flurry also working on comparable technologies. The aim is generally to spy on Web users so as to draw up detailed user and advertising profiles, either for their own use or to sell on to others. This is done across all devices a given person uses to access the Internet, including smartphones and tablets, car computers, TV sets, laptops, desktops, wearables etc. Who cares what customer behaviour can be captured through an IP address when «cross-device ad targeting» delivers the complete package?

It sounds fairly simple, but it is actually quite laborious and involves a kind of two-way recognition. Smartphone and tablet apps equipped with SilverPush technology respond to inaudible high-frequency sound signals in TV and Web advertisements that also use SilverPush. This sound beacon automatically confirms to the SilverPush server that the device emitting the beacon and the one receiving it belong together. This enables SilverPush to attribute TV sets, computers, tablets etc. to a smartphone users and record that user's behaviour across all devices.

The user currently has no means of turning this insidious tracking off without removing the offending apps from his or her mobile devices. One of the first clients to use this tracking on a large scale is the consumer goods giant Procter & Gamble, but it seems that lots of advertising-intensive companies are interested in this new technology.

Read more here:

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-11_de.pdf
http://www.netzwelt.de/news/155813-werbung-geraeteuebergreifendes-tracking-dank-sound-beacons.html
http://www.nzz.ch/digital/unhoerbare-toene-spionieren-webnutzer-aus-ld.3054
http://www.theatlantic.com/technology/archive/2015/11/your-phone-is-literally-listening-to-your-tv/416712

IV. Ads, adblockers, anti-adblockers, anti-adblock killers – the arms race continues

The technology described in III above is unlikely to give online advertising an image boost. Unfortunately, it desperately needs one. If ads were not so busy annoying and tracking us and even spreading malware, there would be no need for adblockers to stop them. Commercial website operators are known to employ anti-adblockers because adblockers cut off their revenue streams. Last but not least, anti-adblock killers can identify and bypass these anti-adblockers. This vicious circle is rather like an arms race, which makes us wonder if the customer is really king or more of a conscientious objector.

Just recently, for example, anti-adblocker provider Pagefair fell victim to a hacker attack that resulted in malware being distributed via the websites of its clients, including The Economist.

It came to light in mid-November that Yahoo refuses to let anyone who runs an adblocker use its proprietary Yahoo Mail platform.

Even The Washington Post, which became part of Jeff Bezos's Amazon empire in August 2013, ran a test this year to see if it could ensure that adblocker users were not able to read all of its articles.

German publisher Axel Springer resorted to more drastic measures recently: it took legal action to warn off a user who uploaded a tutorial video to YouTube explaining how to get around the anti-adblocker on bild.de. There is nothing new about Springer launching legal attacks on adblockers. It lost a case against AdblockPlus in September before the regional court in Cologne, attracting a lot of media attention in the process. The Springer lawyers tried to defy the ruling handed down by the Hamburg regional court back in May that adblockers were permissible because the core business of a media outlet is to distribute journalistic content, and adblockers are not detrimental to this business. The firm's lawyers told the Cologne court: «The complainant's core business is marketing advertisements. Journalistic content is the vehicle through which the public's attention is drawn to the advertising content.» On closer inspection, this is something of a revelation, and it shows just how quickly the adblocker spiral is heading down to ever greater depths.

New York-based start-up Data Arbitrage aims to offer a way out of this dilemma shortly by restoring users' «data sovereignty». The software developers claim to have the ambitious goal of ending the trade in personal data by 2019. To achieve this, Data Arbitrage intends to contaminate the traders' data pools with fake user profiles, ultimately devaluing the actual data. The system works with machine learning software and an «ArbiBot» that creates user accounts and fills them with personal data. The test phase with a current total of 30,000 Facebook, Twitter and Instagram accounts has shown that the system itself can generate a fairly substantial amount of money, and many people with an interest in the project are critical of this fact. It is questionable whether the project can really achieve what it sets out to, however, especially since the companies that deal in data also gather profiling information from sources other than social networks.

Read more here:

http://www.computerworld.com/article/2993382/malware-vulnerabilities/malvertising-is-a-troubling-trend.html
http://www.nzz.ch/digital/pagefair-liess-malware-ausliefern-ld.2870
http://www.sueddeutsche.de/medien/jeff-bezos-zur-uebernahme-der-washington-post-aus-liebe-zur-zeitung-1.2250060
http://www.golem.de/news/adblocker-sperre-bild-de-mahnt-youtuber-wegen-erklaervideo-ab-1510-117011.html
http://www.golem.de/news/adblock-plus-axel-springer-sieht-journalismus-nur-als-vehikel-fuer-werbung-1509-116587.html
http://www.telemedicus.info/urteile/Wettbewerbsrecht/Werbung/1584-LG-Hamburg-Az-416-HKO-15914-Zulaessigkeit-von-Adblockern-mit-Whitelist-Funktion.html
http://futurezone.at/digital-life/mit-falschinformationen-gegen-den-datenhandel/164.969.633
http://t3n.de/news/data-arbitrage-datenhandel-659495

The Clipboard: interesting presentations, articles and videos

The slides and white paper from Black Hat Europe 2015 are available online. One subject covered is a metasploit module that highlights the limitations of LastPass and other password managers:

https://www.blackhat.com/eu-15/briefings.html

How many ways are there to track Web browser users? Johannes B. Ullrich has thought of 11 for SANS:

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

The BSI's latest report provides an overview of the IT security situation in Germany in 2015:

http://docs.dpaq.de/9977-2015_11_19_bsi_lagebericht_2015.pdf

Please share your views! – Reader Survey

SWITCH is carrying out a reader survey on the Security Report, and we would be grateful if you could share your views on how we can improve it. Your help will allow us to enhance the Security Report, and tailor it better to your needs. All of the information you provide will be analysed in completely anonymised form.

Please complete the questionnaire by Friday, 18 December 2015 at the latest. It will take you roughly 8-10 minutes.

You can take the survey at one of the following links:
English: http://swit.ch/survey-secrep
German: http://swit.ch/befragung-secrep

Please don't hesitate to contact us if you have any questions about completing the survey: roland.eugster@switch.ch. Many thanks for taking part and helping us!

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