SWITCHcert Security Report

February 2016

SWITCH

I. ICSI's Haystack looking for Android needles – and beta testers for its field study

We have repeatedly highlighted gaping security holes in various Android operating system versions and apps in our Security Report, and a leading research centre, the International Computer Science Institute (ICSI) at the University of California in Berkeley, is now taking a serious look at this issue as well. A six-strong research team has developed an app called Haystack that aims to help Android device owners find out which apps are compromised and give away personal information, where this information goes, which protocols are used and which data gatherers are behind the apps. The beta version of Haystack is available for download in the Google Play store. The researchers have published some initial results after analysing data from their first 200 beta testers. They found 423 apps passing on personal and/or security-relevant information such as the IMEI codes, IMSI numbers, serial numbers and MAC addresses of Android smartphones and tablets.

Haystack needs to dig quite deeply into the communications on a device in order to carry out its diagnosis. This includes installing its own root certificate. The team's microsite haystack.mobi explains why this is necessary, how it works and what benefits it brings. They want to get as many people as possible using Haystack so as to build up a comprehensive and above all valid and representative picture of the security situation in the Android ecosystem.

Read more here:

https://haystack.mobi
https://haystack.mobi/wordpress/index.php/2015/12/11/haystack-preliminary-results

II. Staging a comeback with a blackout – macro-Trojans return and apparently cause Christmas power cut in western Ukraine

The macro-Trojan is a type of malware that hides in Microsoft Office documents in the form of a macro and causes severe damage to computers it infects. It was thought to be almost extinct, not least thanks to Microsoft's decision to disable macros in its Office software by default. It was all the more surprising, therefore, when the Redmond-based software giant warned at the start of the year that there had been an upsurge in cybercriminals spreading macro-Trojans by e-mail. They send out supposedly overdue bills that look very convincing and concern fake orders from real online shops. The recipient is told to pay the bill, which is attached as an Office document, or face the consequences. As soon as they open the document, worried that someone may have placed an order in their name without their permission, they are prompted to enable macros. If they do so, the malware is downloaded in the background, and their computer becomes part of a botnet remotely controlled by the cybercriminals. Infostealers such as Dridex, banking Trojans such as Zbot and ransomware such as Cryptowall thus find their way onto unsuspecting users' computers. All of these are very serious infections with far-reaching implications.

Eugene Bryksin from the Computer Emergency Response Team of Ukraine (CERT-UA) confirms that the blackout of 23 December 2015, in which almost three quarters of a million people in western Ukraine had their power cut off, was caused by a macro-Trojan hidden in a Word document. The Guardian, meanwhile, reports that the same malware was used in a cyberattack on one of Ukraine's biggest media firms and that the country's intelligence service has traced both incidents back to a hacker group that is at least supported by the Russian government. Researchers at Symantec say that the offending Trojan, BlackEnergy, was created by a group calling itself Sandworm, which they also hold responsible for further attacks on Ukrainian organisations as well as NATO, various countries in Western Europe and several energy companies. There is also mounting evidence that cybercriminals are increasingly targeting physical infrastructures like energy and water supply. In the US, Michael Hayden, former head of the National Security Agency, and Richard Clarke, former National Security Advisor, have warned that so-called smart bombs could damage key physical infrastructures and that an attack like the one on the Ukrainian electricity grid would be possible in their country too. They should know. After all, the US itself is involved in this kind of electronic warfare, having created its own worm called Stuxnet to manipulate the centrifuges at Iran's Natanz uranium enrichment facility in order to cause large-scale breakdowns.

However, widespread, lengthy blackouts of entire regions are something else entirely. They are described rather soberly in a project report from the German parliament's Office of Technology Assessment entitled «Hazards and vulnerability in modern societies» and depicted fictionally in Marc Elsberg's thriller «Blackout – Tomorrow Will Be Too Late». Mathias Dalheimer dealt with the technical side of this highly complex topic in his talk at 32C3 (see links below for video).

Read more here:

http://www.heise.de/security/meldung/Wieder-in-Mode-Trojaner-in-Office-Macros-2512377.html
https://blogs.technet.microsoft.com/mmpc/2014/12/30/before-you-enable-those-macros
https://blogs.technet.microsoft.com/mmpc/2015/04/27/social-engineering-tricks-open-the-door-to-macro-malware-attacks-how-can-we-close-it
http://www.heise.de/security/artikel/Analysiert-Das-Comeback-der-Makro-Malware-2573181.html
http://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy
http://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company
http://www.golem.de/news/ex-nsa-chef-warnt-vor-blackout-der-himmel-verdunkelt-sich-1601-118511.html
http://www.tab-beim-bundestag.de/de/untersuchungen/u137.html
https://media.ccc.de/v/32c3-7323-wie_man_einen_blackout_verursacht#video&t=10

III. Is it really smart? Many smart home solutions have security holes as big as a garage door

If the glossy brochures for smart home automation and entertainment hardware are to be believed, your smart TV will soon be able to tell your smart fridge to order some beer and pizza and keep it chilled ready for when you watch the World Cup final on Saturday night. Maybe it will even tell your smart heating controller to take the temperature down by three degrees because you are having lots of friends round too. Homeowners can already enjoy peace of mind with the ability to control temperature, lighting, access and shade remotely from their smartphone and check up on their smart home with a surveillance camera, even when they are far away.

The price they pay for this comfort comes in the form of huge gaps in the security of the various smart home solutions that are currently on the market. This is creating a totally paradoxical situation in which many of these solutions, supposedly designed to make your own four walls a safer place, are actually leaving the door wide open to skilled virtual burglars. The main problem is that all of the devices are part of the Internet of Things and thus permanently online, so they are easy for hackers and specialised search engines like Shodan to find.

Most of them are just as easy to hack – and this is really an avoidable nuisance – because their manufacturers save on costs by failing to include adequate encryption and, even when encryption is on board, delivering devices with default passwords like 000, 12345 or abc that users often do not bother to change. Security experts have discovered, for example, that Samsung's voice-controlled smart TVs send voice recognition and text information over the Net in unencrypted form. These TVs thus give hackers an easy route into any wireless network to which they are connected. Things are even worse as regards surveillance cameras. Pressure on prices and a lack of security awareness or know-how mean that most of them are supplied without any password protection and send everything they see over the Net with no encryption whatsoever – from images of a sleeping baby to a living room or the PC monitor in a home office.

Things start to get really ridiculous with wireless networks running ZigBee Home Automation 2.1 to control windows, doors and gates. Security researchers have found a massive design flaw in the software. While devices on the ZigBee network do use encryption for all their communications with each other, the ZigBee consortium specifies that all devices must recognise and accept the exact same key pair. However, the two keys are publicly known, making it easy for hackers to take control and reprogram systems so that the control app provided does not even notice the manipulation, let alone report it. This is the virtual equivalent of the key hidden under the welcome mat, and it lets would-be intruders open doors, gates and windows whenever they like.

Read more here:

http://www.sueddeutsche.de/digital/ueberwachung-wenn-die-webcam-zum-spion-im-wohnzimmer-wird-1.2833317
http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html
http://resources.infosecinstitute.com/how-hackers-violate-privacy-and-security-of-the-smart-home
http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies
http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html
http://futurezone.at/digital-life/unsicheres-smart-home-nutzer-koennen-nichts-tun/147.484.799
http://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html

IV. From Mad Men to Bad Boys – malware becoming harder to monitor due to malvertising

Advertising was already a topic of controversy back in the 1960s, as depicted in the hit TV series Mad Men about people living and working on Madison Avenue in New York. However, even the supremely ambitious Don Draper would never have dreamed that, 50 years down the line, the Big Apple would no longer be the centre of the advertising world. These days, it has been overtaken by Mountain View, California, home of Google. The search giant recently announced that it had blocked no fewer than 780 million online ads in 2015 alone for violating its policies. Besides ads that are indecent, cause offence or promote violence or sexism, the growth in fraudulent ads and those carrying malware is particularly worrying.

Compromising a server in the advertising industry's complex ecosystem is especially attractive for «bad boys» for various reasons. For one thing, the computers used in real-time bidding processes filter users by location and spending habits. For another, the OpenX/Revive Adserver software that is popular among online advertising platforms is known to have inadequate security features. This allows attacks to be launched in targeted waves lasting only a few days, which makes malware monitoring significantly more difficult. A particularly blatant case has now come to light in which hackers tricked users with a malicious sub-domain, complete with genuine Let's Encrypt SSL certificate, that infected their computers with an online banking Trojan. It even affected industry heavyweights like DoubleClick and eBay.

As things stand, there are only three ways to stem the tide of malvertising:

1.) Raise awareness of malvertising and the damage it causes. SWITCH has created a microsite with this in mind: Safer Internet (https://www.switch.ch/saferinternet).

2.) Motivate users to protect their devices more effectively by installing a trusted ad blocker or turning off Flash and Java plugins, as recommended by Lifehacker.com.

3.) Put pressure on advertising vendors to carry out more thorough checks of their existing and prospective clients. Permitted advertising should also be **restricted in its functionality**, for example by allowing only images and browser-supported video formats. If people lose their faith in Internet security, it will not just be the victims of malvertising who suffer harm but the entire online advertising industry as well.

Read more here:

https://googleblog.blogspot.ch/2016/01/better-ads-report.html
http://www.nzz.ch/digital/google-blockiert-780-millionen-anzeigen-ld.4394
http://www.heise.de/security/meldung/Erste-Malvertising-Kampagne-mit-Let-s-Encrypt-Zertifikat-3065115.html
http://www.golem.de/news/security-malware-angriff-aus-der-werbung-1509-116326.html
http://lifehacker.com/how-to-protect-yourself-from-malvertising-on-the-web-1745588094

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.