SWITCHcert Security Report

September 2015

SWITCH

I. Ferengi in Redmond? Microsoft enters new dimension of data acquisition with Windows 10

The Ferengi are a race in the Star Trek universe whose lives revolve around amassing wealth. Rule 59 of their Rules of Acquisition states, «Free advice is seldom cheap!» Simply replace «advice» with «operating system», and you have the new Windows 10. Users of the earlier versions Windows 7 and 8 can upgrade to the new one without having to pay for it. Instead of money, Microsoft is after a new kind of currency: user and usage data. The new operating system is preconfigured to collect these once it is installed – automatically, comprehensively and without asking.

Besides the user's name, postal address, age, gender and phone number, the Redmond-based software giant also captures and analyses the current location of the desktop or laptop, websites accessed using Microsoft apps and services, search terms entered, contact with other users, items purchased and much more. Windows 10 assigns a unique identification number to each computer that runs it so as to make the data more reliable, and this number is made available to app developers – almost certainly in exchange for hard currency.

Microsoft has now said that Windows 10's voracious gathering of data can be stopped by changing the security settings without the need to create a user account. However, this is quite laborious, and it means that some of the operating system's new features designed primarily to improve the user experience are no longer available. It remains to be seen whether the potential damage to Microsoft's image will detract from the benefits of trading in data or perhaps even cancel them out completely. There seems to be more talk about Windows 10's insatiable appetite for data than its performance. Russian politicians are not the only ones who believe that it violates national laws. The Swiss Federal Data Protection and Information Commissioner is also investigating its compliance with the Data Protection Act.

Microsoft has responded with defiant nonchalance to calls for greater transparency and less confusing privacy statements and terms of use, attempting instead to impress with its target of one billion Windows 10 installations by the end of 2018. On 1 August, it released a new service agreement for various Office 365 services from Skype to Xbox Live and software linked to a Microsoft account (including Windows 10). This gives it the right to make configuration changes when «counterfeit games» or «unauthorised hardware peripheral devices» are identified – without specifying in detail what this actually means. This brings us to Rule 52 of the Ferengi Rules of Acquisition: «Never ask when you can take!»

Read more here:

https://www.verbraucherzentrale-rlp.de/windows-10—Ueberwachung-bis-zum-letzten-klick-1
http://www.heise.de/newsticker/meldung/Windows-10-Datensammelwut-beherrschen-2774941.html
http://www.zeit.de/digital/datenschutz/2015-08/privatsphaere-windows-10-einstellungen-deaktivieren
http://futurezone.at/netzpolitik/russischer-politiker-will-windows-10-verbieten/148.821.584
http://www.20min.ch/digital/dossier/microsoft/story/-Windows-10-koennte-in-der-Schweiz-verboten-werden–10890387
http://www.zdnet.com/article/microsofts-big-windows-10-goal-one-billion-or-bust/
http://www.welivesecurity.com/deutsch/2015/08/11/microsofts-neuester-wurf-windows-10-datenschutz-0
http://www.heise.de/newsticker/meldung/Windows-10-Pro-und-Contra-Nutzerdaten-nach-Redmond-2789194.html
https://en.wikipedia.org/wiki/Rules_of_Acquisition

II. Digital revolution hacks its makers – ICANN hit by third attack, ISP 1blu hacked and blackmailed

The first article in our last Security Report began with a phrase we might well use again here: «Irony of ironies...» None other than the Internet Corporation for Assigned Names and Numbers (ICANN) reported at the start of August that it had been hacked for the third time. User names, e-mail addresses and passwords used to log into icann.org were stolen, it said. The non-profit organisation is responsible for assigning IP addresses and domain names on the Internet and claims to be committed to ensuring the security, stability and operability of the network.

Berlin-based Internet service provider 1blu also appears to have fallen victim to an attack. It claims that the hackers/blackmailers demanded a large sum of money (rumoured in the media to be EUR 250,000) and threatened to publish confidential customer information should it not be paid. Access details for the customer login, e-mail, FTP, MySQL and 1blu-Drive cloud storage services were reportedly stolen. 1blu has since reset logins, deleted all passwords and asked its customers to log in again, especially since payment details may have fallen into the hackers' hands.

Read more here:

https://www.icann.org/news/announcement-2015-08-05-en
http://www.theverge.com/2014/12/18/7414487/global-internet-authority-icann-hacked
http://motherboard.vice.com/read/icann-has-been-hacked-again
http://www.golem.de/news/hackerangriff-webhoster-1blu-wird-erpresst-1508-115740.html
https://www.1blu.de/sicherheit/kundenanschreiben
http://www.heise.de/security/meldung/Webhoster-1blu-gehackt-und-erpresst-2777957.html

III. Car hacks, autonomous vehicles and telematics-based insurance premiums – threats to safety and privacy

Now we return to another topic we have already covered repeatedly in the Security Report: connected cars. Over the past few weeks, there have been reports of three cases in which either entire vehicles or certain key functions such as accelerator and brake were manipulated.

The worst security issue concerned a Jeep Cherokee that was wirelessly manipulated from a laptop 10 miles away in a «zero day» attack on its Uconnect infotainment system. The radio, windscreen wipers, engine control unit and brakes were all taken over.

In order to hack the Tesla Model S, meanwhile, two researchers from private security firms first needed to gain physical access to the network cable that is installed behind the dashboard for maintenance purposes. This allowed them not only to start and steal the car, but also to infect it with a Trojan enabling them to control it remotely. They also discovered that the Tesla's infotainment system was leaving the door wide open to hackers with a vulnerability that has been known about for four years.

The article from Wired on the Tesla hack (see link below) also shows that connected cars can bring benefits. «Unlike Fiat Chrysler, which recently had to issue a recall for 1.4 million cars and mail updates to users on a USB stick to fix vulnerabilities found in its cars, Tesla has the ability to quickly and remotely deliver software updates to its vehicles. Car owners only have to click 'yes' when they see a prompt asking if they want to install the update.»

In the third case, researchers from the University of California hacked a 2013 Corvette via text message, exploiting the SIM-card-equipped dongle provided by US car insurer Metromile. Coming in quick succession, these cases have given the National Highway Traffic Safety Administration (NHTSA) cause for concern. Serious security loopholes in cars are not isolated problems, they are a threat to a long list of brands sold around the world (see InfoSec Institute article). On top of this, many of them were discovered years ago.

The vulnerability of vehicles' on-board systems is an even hotter topic in light of the development of autonomous vehicles for land, water and air transport, which control themselves without human input. This trend has speeded up massively.

Tesla, for instance, is testing autonomous driving with the Model S mentioned above (albeit after installing a patch). Daimler recently received official approval to test autonomous commercial vehicles on German roads and motorways, and the car service Uber is also committed to working on self-driving vehicles.

A number of manufacturers have thus said that they are prepared to help establish the Information Sharing and Analysis Center (ISAC) the NHTSA has long been calling for. Separately from this, automotive supplier Bosch is working on multi-stage systems in which the vehicle's mechanical and Internet-connected components are not directly linked to each other. Time is of the essence as many insurers are keen to roll out telematics-based premiums as soon as possible. This «pay as you drive» pricing rewards customers who obey the rules of the road and avoid accidents with lower premiums. To this end, a connected device is installed in the car that records all aspects of how it is driven, including speed, acceleration and braking, and relays the information to the insurer. It is not yet certain whether these devices can also deliver information on routes driven and thus build up a profile of the vehicle's movements. However, the Metromile hack in the Corvette shows that hardware and software security risks are an additional cost of the telematics-based premium model.

Read more here:

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already
http://futurezone.at/digital-life/forscher-hacken-corvette-mittels-sms/146.458.778
http://resources.infosecinstitute.com/the-nightmare-of-car-hacking
http://www.bankinfosecurity.com/blogs/car-hacking-spurs-automakers-to-share-threat-information-p-1922#
http://futurezone.at/digital-life/testfahrten-fuer-selbstfahrende-lkw-auf-autobahnen-kommen/148.285.509
http://www.spiegel.de/auto/aktuell/fahrdienst-vermittler-uber-setzt-auf-selbstfahrende-autos-a-1049884.html
http://www.welt.de/finanzen/versicherungen/article141298577/Diese-Kfz-Versicherung-weiss-wie-schnell-Sie-fahren.html
http://www.faz.net/aktuell/finanzen/meine-finanzen/ueberwachung-im-auto-telematik-tarife-im-kommenh-13732050.html

IV. Home, smart home – betrayed by your fridge, exposed by your mobile

The notion that a peek inside someone's refrigerator can tell you a lot about their life – or at least their eating and drinking habits – is as old as the first model invented by Alexander Twinning. At the recent DEF CON conference, however, hackers used a «man in the middle» attack to prove that a networked smart fridge can also give away your Gmail login details to someone who hacks your Wi-Fi network. Samsung claims that it has now removed this vulnerability, but the two Austrians Sebastian Strobl and Tobias Zillner have also shown that, besides a connected fridge, an entire smart house can be hacked if it is running the ZigBee control system adopted as a standard by Samsung, Philips, Osram and Motorola. The security researchers used an app to open doors, control the heating and turns lights on and off. Strobl and Zillner say that they alerted the manufacturers to this risk months ago but were met with nothing more than a shrug of the shoulders. It remains to be seen whether the smart home pioneers will learn from their colleagues in the automotive industry or choose to wait until the issue hurts them financially and tarnishes their image. In the latter case, they will be forced to agree with this quote from the great psychologist and psychotherapist Carl R. Rogers: «The touchstone of validity is my own experience.»

Read more here:

http://www.digitaljournal.com/technology/hackers-steal-gmail-credentials-by-hijacking-samsung-smart-fridge/article/441913
http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar
http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge
http://futurezone.at/digital-life/oesterreicher-zeigen-wie-man-smart-homes-hackt/146.964.575
http://cognosec.com/zigbee_exploited_8F_Ca9.pdf

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