SWITCHcert Security Report

September 2016

I. Bug bounties and the Cyber Grand Challenge

There was a time when hackers were proud to be non-conformists. When it comes to making money, however, they are as keen as anyone else. Finding bugs and vulnerabilities and writing zero-day exploits is a big business. The Guardian, for example, quotes 21-year-old Nathaniel Wakelam, who claims to make USD 250,000 a year working as a «bug bounty hunter» on his Macbook while sitting in coffee shops. There are other rewards hackers are interested in besides hard cash, including airmiles. Golem.de reported recently that a 19-year-old from the Netherlands has collected a million miles finding vulnerabilities for United Airlines.

Despite the FBI's insistence to the contrary, rumours persist that it paid more than USD 1 million to have the iPhone of one of the San Bernadino attackers unlocked (see our Security Reports from March and May 2016). The case appears to have prompted Apple to announce a bug bounty programme at the recent Black Hat conference in Las Vegas at the end of July, offering rewards of up to USD 200,000. Kaspersky has announced a similar programme, albeit with far less money on offer.

Unlike Google, Facebook, Amazon and Microsoft, Apple has previously not paid out any rewards, opting instead to praise the bug finders on its website. This was due to its fears that a bug bounty programme could turn into a bidding war for security threats, favouring the financial gain of a few individuals over the security of millions of users. It did not take long for proof to emerge that this was in fact based on a good understanding of human nature rather than an excuse for not rewarding a valuable service. Immediately after Apple's bug bounty programme was announced, exploit trader Exodus Intelligence offered USD 500,000 for a zero-day vulnerability in iOS. Firms like Exodus Intelligence sell their wares to the highest bidder – governments and intelligence services included.

We reported back in March that even renowned scientists at Carnegie Mellon University's Software Engineering Institute (SEI) were unable to resist the lure of a handsome profit and helped the FBI to unmask Tor users against payment of at least USD 1 million.

The AllForSecurity team from the same university demonstrated at the Cyber Grand Challenge (CGC), also in Las Vegas, that it is possible to make twice that without damaging your reputation. In the first ever purely machine-to-machine contest, autonomous servers attempted to hack each other. AllForSecurity won the overall prize of USD 2 million. CGC programme manager Mike Walker said that, while the servers are not yet a match for real hackers, their economisation tendencies may well have an impact on their human masters in future.

Read more here:
http://www.golem.de/news/united-airlines-bug-bounty-programm-19-jaehriger-hacker-ist-meilenmillionaer-1608-122595.html
https://www.theguardian.com/technology/2016/aug/22/bounty-hunters-hacking-legally-money-security-apple-pentagon
http://www.zeit.de/digital/datenschutz/2016-08/bug-bounty-apple-black-hat
https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program
http://www.trojaner-info.de/daten-sichern-verschluesseln/aktuelles/kaspersky-startet-bug-bounty-programm-mit-hohen-erfolgspraemien.html
http://m.heise.de/mac-and-i/meldung/iOS-Bug-Bounty-Programm-Exploit-Haendler-will-mehr-zahlen-als-Apple-3293301.html
http://www.golem.de/news/united-airlines-bug-bounty-programm-19-jaehriger-hacker-ist-meilenmillionaer-1608-122595.html
https://www.theguardian.com/technology/2016/aug/22/bounty-hunters-hacking-legally-money-security-apple-pentagon
https://www.technologyreview.com/s/602224/a-bug-hunting-hacker-says-he-makes-250000-a-year-in-bounty
http://www.spiegel.de/netzwelt/games/cyber-grand-challenge-in-las-vegas-server-gegen-server-a-1106293.html
http://www.csoonline.com/article/3104823/security/supercomputers-give-a-glimpse-of-cybersecuritys-automated-future.html

II. Pegasus spies on Apple devices, QuadRooter threatens Android

The published details of the Pegasus spyware show the extent to which Apple devices have become malware targets. At the start of August, a human rights activist discovered a suspicious link on his iPhone and contacted IT security firm Lookout, which found «the most sophisticated attack we've seen on any endpoint». The spyware used no less than three vulnerabilities in the operating system iOS – which runs on iPhones, iPads and iPod media players – to intercept practically every action performed on a device. It can be traced back to Israeli cyber weaponry manufacturer NSO, which belongs to a US investor and claims to sell the spyware, in compliance with all legal requirements, exclusively to government agencies – which of course use it to spy on human rights activists and journalists. Two weeks after Pegasus was discovered, Apple released a patch for iOS. A security update for laptops and desktops running OS X followed on 1 September as Pegasus had been found to affect these as well. Lookout did not stand idly by. It published details of Pegasus in its blog, together with a PDF explaining how users can identify devices that are affected.

Let us now shift our attention to Android vulnerabilities. There are four at once to report, hence the name QuadRooter. Once again, an Israeli security firm is involved, but this time on the side of the good guys. The company, CheckPoint, discovered QuadRooter and went public at the DEF CON Hacking Conference (yet again in Las Vegas) at the start of August. Going against the age-old saying «what happens in Vegas stays in Vegas», QuadRooter is apparently to be found all over the world, posing a threat to more than 900 million Android devices. Google has already shut down three of the four vulnerabilities, but it takes much longer for updates to be rolled out to all manufacturers' Android devices than is the case with iOS devices.

The hackers on the dark side, for their part, appear to have acted much faster. Security experts at RiskIQ found 27 malicious apps in the official Google Play app store as well as numerous unofficial stores that claimed to identify and/or remove QuadRooter but in fact installed their own malware. RiskIQ expressly warns against downloading apps from unofficial stores. Google has pointed out that third-party apps are not needed anyway because versions 4.2 and above of Android have a «Verify apps» feature that allows you to identify and remove harmful apps. It says that some 90% of all 900 million Android devices are thus protected against QuadRooter attacks, even if the problem persists on their Qualcomm chips until the appropriate patches are installed.

Read more here:
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/forscher-entdecken-gefaehrliche-spionage-software-fuer-iphones-14406241.html
http://derstandard.at/2000043729494/OS-X-Update-Apple-stopft-Pegasus-Luecke-auch-auf-Macs
http://www.heise.de/newsticker/meldung/Gegen-Spionagesoftware-Pegasus-fuer-iPhones-iOS-9-3-5-behebt-Sicherheitsluecken-3305339.html
https://blog.lookout.com/blog/2016/08/25/trident-pegasus
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-how-to-tell-impacted.pdf
http://www.zeit.de/digital/mobil/2016-08/android-quadrooter-sicherheitsluecke-900-millionen
http://www.nzz.ch/digital/quadrooter-fast-eine-milliarde-android-geraete-mit-sicherheitsluecken-ld.109608
http://blog.checkpoint.com/2016/08/07/quadrooter
http://www.welivesecurity.com/2016/08/11/quadrooter-vulnerabilities-leaves-900-million-android-devices-risk-attack
http://www.infosecurity-magazine.com/news/malicious-quadrooter-apps
http://www.heise.de/security/meldung/Grossteil-der-Android-Geraete-ist-standardmaessig-gegen-QuadRooter-Luecke-gewappnet-3293022.html

III. A USD 22 billion investment pays off – WhatsApp shares phone numbers with Facebook

A little less than two years ago, the world was stunned to hear that Facebook had allegedly spent USD 22 billion on its acquisition of the WhatsApp messaging service. One person who knew why was Mikko Hippönen of Finnish security firm F-Secure. In his USI keynote speech in July 2015, which is available on YouTube, he explained that a person's mobile phone number is the only way to link them beyond any doubt to their online profiles – and to link their various profiles to each other. He suspected that this was why Facebook was prepared to pay such a high price.

Now the Facebook deal is making waves in the media once more after The Guardian reported at the end of August that WhatsApp was sending its users' phone numbers to Facebook so that the parent company could, in its own words, offer «more targeted advertising» and «improved friend searches». While Facebook gave WhatsApp users 30 days to forbid it from using their details for advertising purposes, this does not affect the transfer of data from WhatsApp to Facebook. European Commissioner for Competition Margrethe Vestager is now looking into whether the merger needs to be reinvestigated. Swiss messaging service Threema, meanwhile, is rubbing its hands with glee. Since WhatsApp's plans became public, downloads of its app have tripled.

Read more here:

https://www.youtube.com/watch?v=Umm-97wb_aE
https://www.theguardian.com/technology/2016/aug/25/whatsapp-to-give-users-phone-number-facebook-for-targeted-ads
http://www.golem.de/news/fuer-werbezwecke-whatsapp-teilt-alle-telefonnummern-mit-facebook-1608-122902.html
http://www.spiegel.de/netzwelt/apps/facebook-eu-kommission-ueberprueft-whatsapp-uebernahme-a-1110682.html
https://www.wired.de/collection/business/dank-wahtsapp-explodieren-die-downloadzahlen-des-messaging-diensts-threema

IV. Now you see them, now you don't – another multi-million-dollar Bitcoin theft

Big numbers are also the order of the day when it comes to the latest disappearance of Bitcoins. On 3 August, Hong Kong-based Bitcoin trading platform Bitfinex reported that it had suspended operations after realising that hackers had stolen 120,000 Bitcoins with a total value of roughly USD 58 million. This is modest compared with the USD 500 million theft that bankrupted Tokyo-based exchange Mt. Gox back in 2014, but the Bitcoin exchange rate fell by more than 20% on the news, and general confidence in the virtual currency has taken another big hit. This is not helped by the theft of «ether» currency worth more than USD 50 million from the Decentralized Autonomous Organization (DAO) project by a hacker in July this year (see July's Security Report). The fallout from that case is in fact much more serious. Unlike the Bitfinex and Mt. Gox cases, the DAO's blockchain was successfully hacked, debunking the myth that it was unbreakable and could easily have formed the basis for a range of fintech applications.

Read more here:

http://www.spiegel.de/netzwelt/web/bitcoin-hacker-erbeuten-digitalwaehrung-in-millionenwert-a-1105932.html
http://www.nzz.ch/finanzen/uebersicht-finanzen/bitcoin-unfaelle-der-mythos-virtuelle-waehrung-broeckelt-weiter-ld.109742
http://www.heise.de/security/meldung/Bitfinex-Hack-58-Millionen-Euro-gestohlen-Bitcoin-Kurs-eingebrochen-3286784.html

V. DiskFiltration and Fansmitter attempt to bridge the air gap

Since all systems that can be reached via the Internet or other networks can be hacked, there are some that are not connected to any external network. These are known as «air gap» systems. Hackers and security researchers around the world are interested in the question of how to access the data they contain, which is usually of a highly sensitive nature. Researchers at Ben-Gurion University of the Negev have come up with an answer. They have developed a piece of malware called DiskFiltration that can discern noise patterns of hard disks' read/write heads and use them, for example, to discover passwords.

However, the malware's success is heavily dependent on a series of factors. The audio recording device must be within two metres of the air gap system, the malware must be installed on the air gap system from an external source such as a USB stick, and DiskFiltration does not work with solid-state drives because they have no read/write head.

Another approach the Israeli university is currently researching is bridging the air gap by means of a computer's cooling fan.

Google Tone, meanwhile, exploits the fact that acoustic signals can be used to connect computers. The app is available as an add-on for Google Chrome and allows URLs to be shared over the air gap.

Read more here:

http://www.heise.de/newsticker/meldung/Das-Schnurren-einer-Festplatte-verraet-Geheimnisse-3295965.html
http://www.techworm.net/2016/06/now-fan-noise-can-used-steal-data-air-gapped-computers.html
https://chrome.google.com/webstore/detail/google-tone/nnckehldicaciogcbchegobnafnjkcne?hl=en

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.