SWITCHcert report on the latest IT security and privacy trends

January/February 2018

SWITCH

I. Meltdown and Spectre: security meltdown directly from the processor

The bomb exploded right at the start of the new year. And it had absolutely nothing to do with the loud but harmless New Year Eve's fireworks. Instead, reports of massive security flaws in INTEL, AMD and ARM processors revealed an IT security catastrophe. As early as June 2017, Jann Horn of Google Project Zero had notified the three leading processor manufacturers about severe security flaws in their products. After a long 'grace' period, INTEL finally informed the public of the security flaws at the beginning of 2018. Fact: millions and millions of computers, smartphones and mobile devices in which the chips are installed are so helplessly exposed to attacks from the likes of Spectre and Meltdown that the CERT team at Carnegie Mellon University could initially only recommend installing the latest operating systems as a patch or replacing the processors. Meanwhile, some patches are available, but the security problem is still so severe that we would like to provide a five-point overview here:

1) Why do Meltdown & Spectre pose such a great security risk?

Computers and mobile devices have security mechanisms designed to prevent all types of programs from retrieving whatever data they want from a device's memory. Spectre and Meltdown use two different attack methods to deactivate these security mechanisms. If the security mechanisms have been hacked, programs also load and save

data they do not even need but which is read by malware programmed accordingly and can be 'hijacked'. This includes passwords and crypto keys.

2) How does it work?

To work quicker and more powerfully, 'out-of-order' processors use a technique called 'speculative execution', which involves the processor literally working out of order and predicting which commands will come next. If these are not executed, the data already loaded into the memory ahead of time is thrown out. However, it is not destroyed but instead stored in sectors of memory allocated to programs or the operating system. These are the 'bins' that Spectre and Meltdown search through to pick out the best leftovers. Specifically: login data, codes, crypto keys and more (another explanatory analogy is available in the article listed below at ds9a.nl)

3) What can you do about it?

Generally speaking, you should always keep your system up-to-date with the latest updates from the respective manufacturer. Specifically, however, so many devices from so many manufacturers are affected that we are making an exception and providing a link in the main body of the text to the excellent list of measures compiled by heise.de with suggestions from the individual manufacturers:

https://www.heise.de/security/meldung/Meltdown-und-Spectre-Die-Sicherheitshinweise-und-Updates-von-Hardware-und-Software-Herstellern-3936141.html

Most manufacturers say that they are working frantically to fix the security flaws. When you take a closer look, however, you see that patches have been developed primarily for 64-bit architectures and that older 32-bit models largely remain without protection. The first patches provided by Intel were beyond embarrassing – they contained so many bugs that at the end of January, even Intel recommended refraining from installing the previously recommended updates. It looks like the chip manufacturer has lost its copy of *The Hitchhiker's Guide to the Galaxy*, which is well-known for bearing large, friendly red letters reading DON'T PANIC!

4) Have such attacks already occurred?

Yes, because the current security and patch chaos is basically a red carpet for copycats and hackers. Spam emails are currently circulating in which the German Federal Office for Information Security BSI apparently prompts recipients to download a trojan posing as a Meltdown/Spectre patch. On 1 February 2018, the company AV-Text tweeted that

it had found 139 malware samples related to Spectre and Meltdown so far. Fortinet also claims to have discovered that hackers have modified Java code to exploit both security flaws.

5) What's next?

Work on patches is progressing rather slowly. While Apple and Google claim to have eliminated the risks associated with these flaws by means of operating system and browser updates, other tech giants who normally make big announcements and promise to deliver by certain dates are keeping surprisingly quiet: some have given very minimal responses while others have offered no comment at all. Hence, we are left with the – entirely unsatisfactory – recommendation issued by the CERT experts at Carnegie Mellon University: update operating systems and replace the processor if necessary.

Read more:

https://www.heise.de/security/meldung/Analyse-zur-Prozessorluecke-Meltdown-und-Spectre-sind-ein-Security-Supergau-3935124.html
https://ds9a.nl/articles/posts/spectre-meltdown
https://www.heise.de/security/meldung/Meltdown-und-Spectre-Die-Sicherheitshinweise-und-Updates-von-Hardware-und-Software-Herstellern-3936141.html
https://www.heise.de/security/meldung/Meltdown-Patches-32-Bit-Systeme-stehen-hinten-an-3940207.html
http://www.spiegel.de/netzwelt/web/intel-us-chiphersteller-warnt-vor-sicherheitsluecken-meltdown-und-spectre-a-1189294.html
https://www.netzwelt.de/betrugswarnungen/163398-vorsicht-betrug-gefaelschte-bsi-mails-ueber-meltdown-spectre-update.html#utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:%20netzwelt%20(netzwelt.de%20-%20Aktuelle%20News)
http://www.maclife.de/news/wird-ernst-erste-malware-spectre-meltdown-unterwegs-100100109.html

II. Leaks, fakes and cryptocurrency hacks: business models of a different kind

Times in which hacking was done for hacker's prestige seem to have come to an end, much like the mainframes and PCs that defined an era. In the networked and mobile world, the bad guys are almost always after plain old money. Three business models have recently attracted increasing attention:

1) Trading in leaked login data

Brian Krebs, who writes and runs the blog krebsonsecurity, has collected very detailed facts on this business model in his article 'The Market for Stolen Account Credentials', which is well worth reading. He demonstrated how a username and password combination can be sold on the first market tier of the dark net for USD 8. One seller managed to sell approximately 35,000 logins, totalling USD 288,000, in this way in the first seven months of the year 2017. The buyer, basically a wholesaler, then resells this data for USD 15 – in exceptional cases for as much as USD 150! Grocers who are battling with effective net profit margins in the low single-digit percentage range would turn green with envy. A dark website for such a wholesaler contains a normal price list with the user logins of more than 200 e-commerce and bank websites, carefully listed with information on prices and the number of accounts for which hacked data is available. And they also offer an additional service: in addition to the login data, entire stolen identities of users are sold, including their credit ranking. The higher the ranking, the higher the price of the identity.

2) Business with fake followers

Fake followers have long been a problem for social media platforms. CNN estimates, for example, that approximately 83 million Facebook accounts are fake and have been created for the sole purpose of generating followers. These are then bought by real celebrities or people who believe they can become celebrities themselves to feign influence (according to a statement made by Donald Trump's campaign manager to the BBC, this also worked during the American presidential election campaign). Business Insider claims that 8% of all Instagram accounts are fake.

The market leader in the fake followers business is New York-based Devumi, which is said to have sold 200 million (!) fake followers for the Twitter accounts of politicians, athletes, actors and others. At the end of January 2018, the New York Times published an in-depth story entitled 'Follower Factory', which is now going to have legal

consequences for Devumi. This is due to the fact that, firstly, the followers sold were not human users, but bots. New York Attorney General Eric Schneidermann sees this as fraud, for which he has now brought charges. And secondly, the bots of the 200 million followers are said to have received copies of the data of at least 55,000 real human users; i.e. name, home-town and a lot of other data. This identity theft is an even more serious fraud than the bots and not only hurts Devumi's reputation but also puts the entire influencer marketing model into question.

3) Bank robbery without a bank (theft of cryptocurrency in the blockchain)

With the theft of an estimated EUR 400 to 450 million worth of Japanese cryptocurrency NEM from the Tokyo Coincheck exchange at the end of January, virtual 'bank' robbery has entered a new dimension – at least when it comes to the size of the booty. Prior to that, the hacking of Mount Gox and DAO had not only made investors poorer but, more importantly, also undermined the belief that cryptocurrencies in the blockchain are safe from large-scale robbery (see SWITCH Security Report 7/2016).

Read more:

https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials
https://thenextweb.com/contributors/2017/08/27/influencer-marketing-trouble-fake-followers
https://www.derstandard.de/story/2000073187437/200-millionen-follower-vermittelt-fake-verdacht-gegen-social-media-firma
https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html
https://www.coindesk.com/coincheck-confirms-crypto-hack-loss-larger-than-mt-gox
http://www.chip.de/news/Bitcoin-Boerse-um-400-Millionen-Dollar-erleichtert-Nutzer-sollen-trotzdem-Geld-zurueckbekommen_132851182.html
https://www.nzz.ch/wirtschaft/hackerangriff-trifft-japanische-krypto-boerse-ld.1352017

III. Italianitá in the smartphone – state trojan monitors smartphone users

For linguists and historians alike, Romans mix with Trojans about as well as spaghetti pairs with retsina. For IT security experts, however, they go hand in hand. In 2015, the hack of Italy's developer of state trojans, 'The Hacking Team', made headlines that caused ripples all the way to Switzerland, considering the Zurich cantonal police force had (mis-)invested half a million Swiss francs in a trojan that could no longer be used after the hack (see SWITCH Security Report 8/2015).

Security experts at Kaspersky Labs (more on that below) are now warning against a dangerous state trojan known as Skygofree, which has been active since 2014 and, unbeknownst to users, obtains root access to Android smartphones to completely take over the user's phone, including its microphone and camera(s). Data traces found by the Kaspersky experts point to Italy as the country of origin of Skygofree; the methods resemble those of the Hacking Team trojans.

The powerful and highly innovative spyware is not only able to access data and record phone calls, text messages and WhatsApp communications, but can also activate the microphone and camera when the phone is located in GPS coordinates specified by the attackers. It enters the smartphone via a fake system update from an equally fake mobile phone provider site, which users are prompted to visit. Once the trojan has been installed, the malware integrates itself as a protected app so that it keeps running when the screen is turned off.

To protect yourself against Skygofree and other advanced mobile malware, Kaspersky Lab recommends the following security measures:

- Install a reliable security solution on all mobile devices
- Be careful when you receive emails from unknown persons or organisations with unexpected requests or attachments
- Do not click on links in emails before you have checked the integrity and source of the linked site. When in doubt, contact the service provider
- System administrators should enable the application control functions in their mobile security solutions to check programs that are susceptible to such attacks.

The link below to further details on the Kaspersky website is safe.

Read more:

https://www.n-tv.de/technik/Staatstrojaner-ueberwacht-Smartphone-Nutzer-article20235630.html
http://www.zeit.de/digital/datenschutz/2018-01/skygofree-android-whatsapp-schadsoftware
https://www.heise.de/security/meldung/Skygofree-Ausgefeilter-Android-Trojaner-spioniert-seit-2014-Smartphones-aus-

3943853.html
http://newsroom.kaspersky.eu/de/texte/detail/article/skygofree-hochentwickelte-spyware-seit-2014-aktiv

IV. Kaspersky shut out of Lithuania as well

Exactly why American and British authorities are no longer allowed to use Kaspersky software cannot be fully explained here – whether it is due to the warning regarding state trojans or the allegation that it delivered NSA data to Russian authorities (an allegation that Kaspersky denies vehemently), or simply Trump's America First policy What's certain is that since the end of 2017, the Moscow-based security company's software may no longer be used by Lithuanian authorities either, despite its high quality, widespread use and popularity. In addition, the government is also forbidding the use of Kaspersky software by private companies in the financial, energy and logistics sectors, due to the potential risk to national security.

US President Donald Trump has now also signed into law defence budget legislation that bans the use of Kaspersky software, even though the IT group vehemently denies all allegations and points out that secret NSA programs only ended up on Kaspersky servers because an NSA employee had installed a pirated copy of Microsoft software alongside the Kaspersky antivirus software.

To combat the loss of confidence and income, Kaspersky has announced a transparency initiative, which involves releasing the source code of the software.

Read more:

https://futurezone.at/digital-life/kaspersky-software-auch-in-litauen-verboten/303.246.654
https://derstandard.at/2000070337380/Trump-fixiert-Verbot-von-Kaspersky-Software-fuer-US-Behoerden
https://derstandard.at/2000066667979/Kaspersky-NSA-Hacker-installierte-falsche-Microsoft-Software
http://www.spiegel.de/netzwelt/netzpolitik/kaspersky-wirbt-mit-transparenzinitiative-um-vertrauen-a-1174252.html

V. Strava leaks – fitness secrets of a different kind

While Washington accuses Kaspersky of espionage, employees of American military and security agencies have – probably unintentionally – made locations and structures of top secret American military and security facilities accessible to anyone on the planet by publishing their fitness activities on the internet. All of this is thanks to the Strava fitness app, which is used by many fitness trackers to enable sporty people to record and post their training sessions. Strava collects all data to create what it calls a Global Heat Map. On the company's website, interested parties can see where and at what intensity Strava app users are particularly active. In November 2017, Strava used more than 3 billion individual GPS data points, a billion fitness cycles and 27 billion tracked kilometres to create a unique world map and put it online.

An undesired side effect: in the middle of usually track-free Afghanistan, in Somalia and in Syria, unusual patterns have appeared, to the extent that even floor plans are visible. To an experienced spy, this immediately indicates that people who can afford and actively use fitness trackers are moving about here. It is much more likely that these are American, European or Russian soldiers or members of the secret service or embassies than Afghan, Somali or Syrian civilians jogging around the block rather frequently. After all, US armed forces have actively promoted the use of fitness trackers and apps and even distributed 2,500 Fitbit trackers in a pilot project in 2013. In doing so, they clearly failed to follow the advice of leadership guru Stephen Covey, who passed away in 2012: 'Always begin with the end in mind!'

Read more:

https://www.wired.de/collection/life/eine-fitness-app-enthuellt-geheime-militaerbasen
https://labs.strava.com/heatmap/#8.76/20.92056/39.58226/hot/all

This SWITCH-CERT security report was written by Dieter Brecheis and Michael Fuchs.