SWITCH-CERT report on the latest IT security and privacy trends

September/October 2017

SWITCH

I. Attack of the digital dolphins: hacking Alexa, Siri and their friends via ultrasound

It's been a well-known fact since the early 2000s that the US navy in San Diego and the Russian navy in Sevastopol have trained dolphins to locate weapons, mines and hostile divers and, if necessary, attack them. Now, researchers at Zhejiang University have demonstrated how 'dolphin attacks' can be used to manipulate digital voice assistants such as Alexa (Amazon), Siri (Apple), Cortana (Microsoft), Google Now, S Voice (Samsung) and Hi Voice (Huawei) – albeit under laboratory conditions. In their experiment, they modulated speech commands in the ultrasound range beyond 20,000 Hz – a range inaudible to humans – and sent these inaudible voice commands to devices running one of the above-mentioned voice assistant systems. This enabled them to make FaceTime calls on an iPhone and switch an Android phone to flight mode. At first, that might not sound earth-shattering, but the researchers' simulated attacks took on a new dimension when they managed to manipulate the navigation system inside an Audi. Many vulnerable devices are also used as controllers for other devices, IoT devices, or networks – for example, connected cars, smart homes, access systems, etc.

The Chinese researchers fear that devices falling prey to dolphin attacks could cause harm in all kinds of ways:

- The device is instructed to visit a malware website so that it falls victim to a drive-by attack that installs malware on the device.
- The device is instructed to make a video or phone call to a party who can record audio or images to spy on the owner of the device.
- The device is instructed to spread fake information via text message, email or online posts or enter fake appointments into the owner's calendar.
- The device is instructed to switch to flight mode, cutting off the user from all wireless communications without them noticing.
- Commands are sent to the device to mask the attack.

To address the problem, researchers propose taking both hardware and software-based precautions, ranging from improving microphones to using software that can detect and block such dolphin attacks.

Read more:

https://arxiv.org/pdf/1708.09537.pdf
https://www.youtube.com/watch?v=XBbHDQH47tk
https://thehackernews.com/2017/09/ai-digital-voice-assistants.html
https://hothardware.com/news/siri-alexa-ai-vulnerable-ultrasonic-dolphin-attack-hijacking-commands
http://t3n.de/news/forscher-hack-siri-alexa-ultraschall-855527

II. The anti-antivirus programme: US government bans agencies from installing Kaspersky software on their computers

Yevgeny Valentinovich (or Eugene for short) probably had something different in mind for the Kaspersky company's 20th anniversary. The US government's ban on Kaspersky software in mid-2017 dealt a blow to the any IT security company's most important capital: the trust of its users. Even though there has been periodic speculation since 1997 about Kaspersky's ties as a graduate of the KGB's IKSI academy, he is still a recognised security expert. Around 400 million users around the globe trust his software to protect them against spying, hacking and data misuse. These include major agencies such as Germany's Federal Criminal Police Office (BKA) and a considerable number of US authorities. Then, however, they were confronted in mid-September with the demand from the US government to submit

plans within 60 days for discontinuing use of Kaspersky software, which were then to be implemented within 90 days. Back in July 2017, the US government's General Services Administration (GSA) had removed the Moscow-domiciled company from its list of approved providers for Internet security products. Eugene Kaspersky denied the spying allegations with the following statement: 'The company has never helped, nor will help, any government in the world with its cyberespionage efforts'

Behind the dispute lie the FBI and US Homeland Security Agency's fears that Russian intelligence operatives and government agencies were spying on their US counterparts using Kaspersky software. In multiple interviews and on his Twitter page, Kaspersky repeatedly stressed that there is no evidence for the allegations against his company and that the US government's accusations are baseless and unfounded: 'We will never harm our customers. We protect them against malware – whether it originates in Russia, America or any other country.' The security expert was backed up by the German Federal Office for Information Security (BSI), which emphasised its solid and trusting collaboration with Kaspersky Lab and pointed out that Kaspersky was the first to discover and offer detailed reports on numerous cyberespionage campaigns originating from inside Russia.

Vesselin Bontchev has reported extensively on medium.com on how the confrontation has been unfolding, along with a detailed analysis of its causes. He finds it regrettable that no one will come out on top in the aftermath: the decision means that US authorities will be giving up one of the best pieces of antivirus software available. Kaspersky itself will lose a lot of money in the US market, which is responsible for generating 25% of its value. And, ultimately, Bontchev fears that all users will have to sacrifice security because of what he sees as an unethical campaign by several of Kaspersky's competitors (Symantec, Bitdefender, McAfee, Avira, and others) which will jeopardize cooperation between cybersecurity experts.

Meanwhile, Bloomberg reported that a hearing by the Committee on Science, Space, and Technology in the US House of Representatives planned for 27 September was cancelled at short notice. A closed-door session on the same issue was held instead. During the hearing, Kaspersky was expected to – and wanted to – address the allegations. No new date has been made public; nor have any further developments.

Read more:

https://www.reuters.com/article/us-kasperskylab-russia-usa/russia-doesnt-rule-out-retaliation-if-u-s-bans-kaspersky-products-idUSKBN19K1KV

https://www.reuters.com/article/us-usa-kasperskylab/trump-administration-limits-government-use-of-kaspersky-lab-software-idUSKBN19W2W2
https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws
https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.f88d7b7b5e55
https://www.usatoday.com/story/tech/news/2017/09/14/confusion-hits-consumer-market-over-u-s-ban-kaspersky-software/666211001
http://www.spiegel.de/netzwelt/netzpolitik/kaspersky-firmenchef-eugene-kaspersky-verteidigt-sich-gegen-anschuldigungen-a-1167916.html
http://www.zeit.de/digital/2017-09/spionageverdacht-usa-russland-kaspersky-software
http://www.focus.de/digital/computer/unternehmen-bsi-lobt-nach-us-vorwuerfen-vertrauensvolle-zusammenarbeit-mit-kaspersky_id_7593541.html
https://medium.com/@bontchev/understanding-the-us-government-kaspersky-lab-controversy-f0ed6cd3b52
https://www.bloomberg.com/news/articles/2017-09-26/house-panel-is-said-to-receive-classified-briefing-on-kaspersky

III. A hack of 'epic proportions' at Equifax

Equifax is the largest consumer credit reporting agency in the US. Originally founded in 1899 as the Retail Credit Company, the company is based in Atlanta, Georgia. Equifax servers store social security, credit card and driver's license numbers, dates of birth, addresses and other information about several million customers from the US, Canada and UK. 143 million of them can now assume that their data has landed in the wrong hands or on servers where it does not belong after Equifax fell victim to the largest theft of social security numbers in history. Even if the figure pales in comparison to the ~~500 million~~ three billion*) hacked Yahoo accounts, the recent hack is the absolute worst case scenario for a consumer reporting agency. In addition to the loss of customer trust, Equifax was also forced to accept the revocation of its SSL root certificate by the certification authority after the hack and the circumstances surrounding it were made public. These circumstances and the events that followed are even more dramatic than the 'colossal' and 'epic' hack itself and are enough to make any observer's hair stand on end.

On 7 September, the company was forced to admit that hackers had been stealing data with impunity since May, until the virtual break-in was finally discovered on 29 July. The hackers had exploited a security hole in Apache Struts, even though a patch had been available since March. Equifax simply had not installed it. In addition, Equifax had already been hacked in March but apparently did not disclose this for fear of losing customer trust, until Bloomberg published leaked insider information. While

Equifax scrambled to insist that the two hacks were unrelated, it was confronted with the charge that the characteristics and attackers in both cases were identical.

The disclosure of the earlier hack was made even more shocking by the revelation that senior employees at the company had sold USD 1.8 million in company stock and let six entire weeks pass before notifying the public after the second hack. The district attorney's office has in turn launched an investigation into suspicions of insider trading.

On 21 September, news broadcaster NPR published the breaking news that customers who were told by Equifax to enter their social security numbers to determine whether their accounts had been compromised by the hack were redirected to a fake website that siphoned off their data – for the second or perhaps even third time. It appears that Equifax has a peculiar understanding of what tradition means for longstanding companies like itself.

Read more:

https://www.heise.de/newsticker/meldung/Equifax-soll-frueheren-Hack-verheimlicht-haben-3835052.html
http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html
https://www.washingtonpost.com/opinions/the-equifax-disaster-points-to-a-much-bigger-problem/2017/09/21/4bd683da-9ee3-11e7-9083-fbfddf6804c2_story.html?utm_term=.602d6b1a0fda
https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed
http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site
https://www.golem.de/news/kreditrating-equifax-krisenreaktion-ist-ein-desaster-1709-129967.html
https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/chefs-verkaufen-aktien-bevor-gigantischer-hack-publik-wird/story/15298299
* https://www.golem.de/news/yahoo-mail-alle-yahoo-kunden-im-jahr-2013-gehackt-1710-130405.html

IV. Science fiction 4.0 – how to hack a computer with a drop of saliva

What new security risks does biomolecular information pose in the field of binary information processing? This initial question led two researchers at the University of Washington to what was certainly the most futuristic hack of the year: the hijacking of a computer with the help of malware-contaminated DNA. Tadayoshi Kohno and Luiz Ceze set out to demonstrate that as gene technology continues to evolve, so, too, does the risk that DNA sequencing might be hacked. This could impact universities, commercial research facilities and police and life science laboratories, among others.

The hack itself was carried out in three stages: first, the researchers wrote malicious code designed to get into the computer through an exploit. Then they translated this code into a DNA sequence that could be synthesized for 89 dollars. The target sequencer then output the compromised DNA again and analysed the data readout using conventional software. The result: the exploit smuggled in via the DNA forced the computer to contact the command-and-control server (where the hacker would have been sitting in a real scenario). The would-be hacker would then be able to use the compromised computer to gain access to the network to which the computer was connected. Even though Kohno and Ceze themselves point out that it will be years before this kind of attack is a real threat, they still managed to show that DNA analysis software does not meet generally accepted security standards, sending a wakeup call they hope will not fall on deaf ears.

Read more:

http://www.zeit.de/digital/internet/2017-08/dna-malware-hacker
http://www.washington.edu/news/2017/08/10/dna-sequencing-tools-lack-robust-protections-against-cybersecurity-risks
https://techcrunch.com/2017/08/09/malicious-code-written-into-dna-infects-the-computer-that-reads-it
https://www.theguardian.com/technology/2017/aug/11/hacking-computer-dna-university-of-washington-lab
https://www.technologyreview.com/s/608596/scientists-hack-a-computer-using-dna

This SWITCH-CERT security report was written by Dieter Brecheis and Frank Herberg.