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

May / June 2018

SWITCH

I. Microsoft will never contact you by phone: support scam continues to gain momentum

They are certainly nothing new, but are becoming ever more sophisticated, expensive and widespread. What we are talking about are phone calls, usually from an English-speaking person posing as a representative from Microsoft or another well-known ICT company. The caller will use a pretext; for example, that the system of the person being called has reported an error message or that there are problems with the licence agreement. The scammers tell the victim that their Microsoft licence will have to be blocked for security reasons and that, in order to avoid this, they can have the problem fixed on their machine immediately via remote access or purchase a support plan or warranty. To add weight to their arguments, they ask their victim to open Microsoft's support tool, Event Viewer. This program does, in fact, list error messages in most cases. This list of mundane and harmless error messages gives the phone phishers relevant reasons for obtaining credit card details or payments in another form (e.g. iTunes cards) from the victim.

Fraudsters can take it even further with the remote access scenario: the person being called is told to download a remote maintenance program, which gives the criminal unrestricted access to the system – including a backdoor for illegal activities or running

bots. Although Microsoft, as well as the police and public authorities like MELANI, repeatedly warn against these kinds of calls, they have been becoming more and more frequent in recent years, not to mention more bold and harmful.

Heise.de already reported the first calls back in 2016. At the time, Microsoft had already made it crystal clear that the company never makes any unsolicited calls offering technical support. In 2017, the software giant again warned of a «tech support scam» on the company's own news page and published findings from a study conducted by the Microsoft Digital Crime Unit, in which it reported that one in three survey respondents had received such calls. In March 2018, the Internet Crime Complaint Center (IC3) announced that the fake calls had caused damages of around 15 million dollars. While most victims reported losses between 200 and 400 dollars, there have also been a few cases in which the scammers were able to use the access credentials phished from the recipient of the call and drain their bank account to the tune of more than 100,000 Swiss francs.

Fraudulent security or tech support is not only being offered by phone, but by email and malvertising as well. To view a list of precautions published by IC3, click the link below. The three main tips: 1. Reputable companies will definitely never offer their support services via sales calls. 2. It is important not to let callers pressure you and to act quickly (and resolutely). 3. Under no circumstances should you give unknown parties access to your systems or account/credit card details.

Read more:

https://www.luzernerzeitung.ch/zentralschweiz/nidwalden/buochs-microsoft-masche-40-jaehrige-faellt-auf-cyberbetrug-herein-ld.43021

https://www.melani.admin.ch/melani/de/home/themen/fake_support.html

https://www.heise.de/ct/ausgabe/2016-23-Falsche-Microsoft-Support-Anrufe-3359912.html

https://news.microsoft.com/de-de/microsoft-anrufe-scam

https://gizmodo.com/microsoft-warns-that-tech-support-scams-are-still-on-th-1825502696

https://www.zdnet.com/article/windows-warning-tech-support-scammers-are-ramping-up-attacks-says-microsoft

https://www.ic3.gov/media/2018/180328.aspx

II. «Efail» between hype and disaster: the security world needs to learn how to communicate

The damage is done, and those affected are the users, security and software companies, IT developers and security researchers. It all started with a security hole discovered and

memorably coined «Efail» by researchers Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky and Jörg Schwenk in October 2017. Efail makes it possible for emails sent via point-to-point encryption – which was previously considered secure – to be read as plain text when they have been encrypted with what were also previously considered secure and reliable protocols: OpenPGP and S/MIME. The Electronic Frontier Foundation (EFF) subsequently decided to publish information about the vulnerability together with the recommendation to only send emails in unencrypted format from then on. What is unclear is why the EFF also released this report earlier than had been discussed by expert committees and with other researchers and developers. But it was precisely this turn of events that resulted in the second, perhaps even more serious wave of damage. This was because the media picked up on the topic and stirred up hype surrounding Efail by adopting the EFF recommendations without reflecting much on what they were doing. In turn, the involved developers at EFF felt caught by surprise. The Efail researcher group was not prepared for crisis communications and for the fact that people would follow the EFF recommendation to stop using PGP- or S/MIME-based programs, thereby creating a whole new set of security risks. Heise online author Fabian A. Herschel sums up the main problem: «The developers of PGP and S/MIME programs will probably have to spend years cleaning up this reputational fiasco. If that's even possible at all.»

Read more:

https://en.wikipedia.org/wiki/EFAIL
https://efail.de
https://thehackernews.com/2018/05/efail-pgp-email-encryption.html
https://www.wired.com/story/efail-encrypted-email-flaw-pgp-smime
https://www.heise.de/newsticker/meldung/Efail-Was-Sie-jetzt-beachten-muessen-um-sicher-E-Mails-zu-verschicken-4048988.html
https://www.heise.de/security/meldung/Efail-Welche-E-Mail-Clients-sind-wie-sicher-4053873.html
https://www.heise.de/newsticker/meldung/Kommentar-Efail-ist-ein-EFFail-4050153.html
https://blog.cryptographyengineering.com/2018/05/17/was-the-efail-disclosure-horribly-screwed-up
https://searchsecurity.techtarget.com/news/252441216/Efail-disclosure-troubles-highlight-branded-vulnerability-issues

III. Sonic waves on the attack, recent incidents are reason to prick up your ears

The surveillance scandal exposed by Snowden seems to be forgotten. The erstwhile outraged public now voluntarily pays to have digital assistants send their messages,

create shopping profiles or record conversations. Alexa, Siri, Cortana, Google Assistant and Watson are not just listening but, in extreme cases, also sharing with others what they happen to overhear. It happened in Oregon. In late May, news agency Bloomberg reported that an Amazon Echo speaker had recorded a private conversation between spouses and then sent it to a person they knew.

Amazon's explanation for Alexa's misconduct might indeed be valid, but is astonishing nonetheless. In the arstechnica article cited below, the explanation was that Alexa and her digital compatriots can, in poor acoustic situations, interpret what is said autonomously and act accordingly. Yet voice-controlled assistants supposedly have outstanding hearing, as the evidence shows. Back in 2016, students at Berkeley and Georgetown University proved that they could hijack voice-controlled AI systems by way of so-called dolphin attacks, which involve taking high-frequency sounds that are inaudible to humans and embedding them in music, videos or streaming files. The systems then interpret these as commands and perform the actions accordingly.

The manipulation scenarios are not necessarily malicious in their intent, nor do they always use sophisticated technologies to take advantage of voice-guided systems for their own purposes. Burger King sent a voice command to voice-controlled Android devices that respond to the 'O.K. Google' command, getting them to open the Wikipedia page for the BK Whopper. And the makers of South Park dedicated an entire episode to voice commands that could elicit a host of obscenities from these assistants with open ears.

Just how serious the damage caused by sonic means can be in the ICT world was recognized as far back as 2008 by a SUN Microsystems employee. He discovered that the I/O latency of his hard disks would increase whenever he shouted at the disk rack. In late 2016, motherboard.vice.com reported that the release of extinguishing gasses during a fire drill had been so loud that the sound wave destroyed dozens of hard disks at the main data centre of ING Bank in Bucharest. At the end of April in Sweden, there was a similar incident, in which the sound caused by the release of extinguishing gas destroyed numerous hard disks and servers of Nasdaq Nordic and two Scandinavian banks, causing stock trading to stop for several hours in multiple Scandinavian and Baltic states.

All criticism notwithstanding, however, it should not be forgotten that voice-controlled AI systems are helping to improve the quality of life of many people who rely solely on

verbal communication due to disabilities or accidents. The Sydney Morning Herald published a story about a motorcyclist who had an accident that injured and immobilized him. He could only be rescued in time because he was able to make an emergency call with verbal commands to Siri.

Read more:

https://www.bloomberg.com/news/articles/2018-05-25/amazon-s-alexa-snafu-should-be-a-turning-point-for-tech
http://www.handelsblatt.com/technik/gadgets/amazon-echo-amazons-digitaler-assistent-verschickt-heimlich-privatgespraech/22602528.html?ticket=ST-4540107-l9pyLGcf2bsSOp2GvFAr-ap3
https://arstechnica.com/gadgets/2018/05/amazon-confirms-that-echo-device-secretly-shared-users-private-audio/
https://netzpolitik.org/2018/amazon-echo-alexa-sendet-privatgespraech-heimlich-an-arbeitskollegen
https://futurezone.at/digital-life/in-musik-versteckte-befehle-lassen-alexa-und-co-einkaeufe-taetigen/400033990
https://www.cnbc.com/2018/05/10/new-york-times-digital-alexa-and-siri-can-hear-this-hidden-command-you-canat.html
https://arstechnica.com/information-technology/2018/05/attackers-can-send-sounds-to-ddos-video-recorders-and-pcs
https://windowsunited.de/dolphinattack-sicherheitsloch-sprachsteuerung
https://www.heise.de/newsticker/meldung/Loeschanlagen-Ton-zerstoert-Festplatten-in-schwedischem-Rechenzentrum-4029730.html
https://motherboard.vice.com/de/article/gvib7w/ungewoehnlicher-vorfall-beweist-geraeusche-koennen-festplatten-zerstoeren
https://www.smh.com.au/national/nsw/teen-uses-siri-to-call-triple-zero-after-after-bike-crash-in-bush-20180525-p4zhen.html

IV. Waterholing attacks: infrastructure is and remains a target

Netcom BW, a regional Internet provider and subsidiary of Germany's energy supplier EnBW, was the target of a waterholing attack. The damage was minimal and the energy supplier ultimately walked away unscathed, because the attack was caught at an early stage. Waterholing attacks are complex and require patience and good preparation. Much like big cats waiting at watering holes for thirsty prey, the hackers lurk on websites, waiting for their victims to visit and then infecting their devices with malware, which then enables them to penetrate deeper into the system of the company that has been attacked. Investigators have identified Russian hackers with close ties to the government as the culprits behind the EnBW attack, because the attack pattern matches a hack that had caused serious damage to the power supply in Ukraine in December 2015. According to the latest information, the major hacking attack on the German Bundestag was also a waterholing attack carried out by Russian hackers.

Read more:

https://www.heise.de/newsticker/meldung/EnBW-Tochter-war-2017-Ziel-von-Cyberangriff-Erfolgreich-abgewehrt-4050711.html
http://www.handelsblatt.com/wirtschaft-handel-und-finanzen-roundup-enbw-tochter-war-2017-ziel-von-cyberangriff-erfolgreich-abgewehrt/22573752.html?ticket=ST-4689874-ceC6NRgxtrnfrSPl1seN-ap3

https://www.inside-it.ch/articles/51112
http://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625
http://www.sueddeutsche.de/digital/computerviren-angriff-liebesgruss-der-schlange-1.3987245

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

The security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH does not assume any liability for the content or opinions presented in the security report nor for the correctness thereof.