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

March/April 2019

I. Lenin and the detectives: Mobiispy stalkerware can make highly personal data collected while monitoring children and partners publicly accessible

Vladimir Ilyich Lenin is credited with saying that trust is good, but control is better. The Bolshevik leader and revolutionary would certainly make a good spokesman for the people making stalkerware. This umbrella term refers to an astonishingly broad range of programs and apps that helicopter parents or jealous lovers install on the smartphones of their children or partners. The makers usually appeal to anxious parents who use the software to eavesdrop on calls, read text messages, view and copy contact lists or photos and video recordings – in short, nearly anything the subject might be doing with their smartphone. Ideally, the person who is monitoring should inform the subject and only install the software with their consent. In reality, it is usually exactly the opposite. And this has consequences that can backfire on the parents and lovers and their original intentions.

Take the tech information platform motherboard.com, which reported in late March how security researcher Troy Hunt had discovered that Mobiispy.com – one of the strikingly large number of stalkerware providers – was storing 16 GB of pictures and 3.7 GB of MP3 recordings in an unencrypted cloud database accessible to anyone on the Internet. Because the roughly 95,000 images and 25,000 audio files included intimate photos and call recordings of minors, Motherboard initially refrained from naming the provider to protect those affected. But after Mobiispy ignored repeated inquiries from Hunt and Motherboard, they notified the internet registrar and hosting provider of Mobiispy.com. In late March, the provider removed the website from its cloud (albeit only after the Motherboard report).

Because easy access to data collected surreptitiously by stalkerware is usually the rule rather than the exception, this case is especially troubling. Motherboard lists a further twelve stalkerware providers whose data has been hacked in the last two years or who have simply placed data online unprotected.

Perhaps it is precisely the converse of Lenin's maxim that best applies to the digital age: "Control is promising, but trust is better!"

Read more:

https://motherboard.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings
https://motherboard.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy
https://futurezone.at/digital-life/ueberwachungs-app-stellt-ueber-95000-fotos-offen-ins-internet/400445902
https://t3n.de/news/datenleak-bei-stalkerware-fuer-eltern-und-eifersuechtige-95000-fotos-einsehbar-1152479/
https://motherboard.vice.com/en_us/topic/when-spies-come-home

II. Ransomware trojan LockerGoga brings companies to their knees

In January 2019, a security researcher on bleepingcomputer.com discussed a piece of ransomware called LockerGoga, which cyber criminals used to attack the French tech consulting firm Altran. The researcher reported that the software was slow, poorly programmed, ineffective in its handling of ransom payments, and apparently not too worried about being discovered. But that still didn't stop LockerGoga from paralysing the IT systems of several large industrial producers and causing major damage. In addition to certain companies wishing to remain anonymous, victims included the specialist chemical manufacturers formed from the merger of Hexion and Momentive in Columbus, USA, and Leuna, Germany. But by the time the attack on the Norwegian aluminium giant Norsk Hydro succeeded (from the hackers' perspective), it should have been clear to IT officers and security experts that LockerGoga is a ransomware counterpart to the second 'Death Star'. Much like in Star Wars, it at first appears as though it couldn't really work but it is fully operational, and downright fatal to the companies it strikes. Momentive, for example, had to replace hundreds of desktops and tablets, and the financial damage sustained by Norsk Hydro during the first week after the LockerGoga attack is estimated at around 40 million dollars. Due to Norsk Hydro's market position, the cyberattacks also affected aluminium prices after commodities traders became jittery about a potential bottleneck.

Norsk Hydro also lost 3.4 percent of its stock value and in one division it took a week after the attack to reach just 70-80% of normal capacity. Meanwhile, another division remained at a complete standstill.

It remains to be seen whether the Norwegian aluminium giant's cyber-insurance policy will cover the damage. In 2017, food giant Mondelez filed a 100-million-dollar claim to cover damages following a NotPetya attack. The insurer has withheld the payout so far on the grounds that the governments in the USA, UK, Australia and Canada had described the NotPetya attacks as part of the Russian cyberwar against Ukraine, and the policy includes a clause that excludes payment of compensation for war-related damages. During the same wave of attacks, the Danish logistics company Maersk reported 300 million dollars in damages. How much, if any will be covered by any cyber-insurance policies remains to be seen. What is clear, however, is that awareness and security-conscious conduct on the part of all employees is more important than ever in view of the increase in cyberattacks on critical infrastructure and producers.

Read more:

https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers
https://www.databreachtoday.com/lockergoga-ransomware-suspected-in-two-more-attacks-a-12242
https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms
http://www.spiegel.de/netzwelt/netzpolitik/norsk-hydro-hackerangriff-war-eine-lockergoga-ransomware-attacke-a-1258627.html
https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-march-26
https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week

III. Straight talk at Facebook: when tech giants fail to meet even minimal security requirements

Founding father of Facebook Mark Zuckerberg recently published a guest commentary that ran simultaneously in the Sunday edition of the *Frankfurter Allgemeine Zeitung* and in the *Washington Post*. In it, Zuckerberg makes an appeal for new, transparent internet regulations. Straight talk? At Facebook? Right! Or maybe not …

To clear up any possible misunderstanding right off, Zuckerberg's guest commentary has not been taken by many industry insiders and experts as straight talk, but instead as the latest smoke-and-mirrors attempt to deflect attention away from the social network's troubles. Facebook faces allegations that it continues to siphon off vast quantities of data from users while they are logged in and even when they are not, all in order to pad its own pockets. It is also accused of failing to get a handle on posts that spread hate speech and incite violence and that it has opened (and left open) the floodgates for bots and trolls to manipulate free elections. Pressure to break up the company is mounting.

And yet it would appear that there's one area where Facebook does express itself straightforwardly, and it's one where straight talk has no place whatsoever: the storage of passwords. Up to 600 million Facebook, Facebook Lite and Instagram users were affected by a brazen data protection breach, which Facebook discovered during a routine audit in January. Zuckerberg's company reported on 21 March that the unencrypted passwords were only accessible internally and had not been used for malicious purposes by anyone at the company. Shortly before this report, security expert Brian Krebs posted a report on his blog krebsonsecurity; according to both current and former Facebook associates, more than 20,000 Facebook employees had access to the passwords, which had often been stored in plaintext for years.

Storing passwords in unencrypted form is a clear violation of GDPR Article 32, which requires the 'pseudonymisation and encryption of personal data'. Currently, the best available solution for complying with this requirement is to use what are known as 'hashes', because they cannot be decrypted for the purpose of reconstructing passwords. The only possible option left for hackers would be to try every conceivable combination to crack a password (brute force attack).

Perhaps Mark Zuckerberg should apply these rules at his own company to help regain some of the credibility it has lost.

Read more:

https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.778682baeaa8
https://www.faz.net/aktuell/feuilleton/medien/zuckerbergs-aufruf-zur-regulierung-des-internets-16117634.html
https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years
https://www.zdnet.com/article/facebook-we-stored-hundreds-of-millions-of-passwords-in-plain-text
https://www.golem.de/news/datenschutz-facebook-speicherte-millionen-passwoerter-im-klartext-1903-140173.html
https://security.blogoverflow.com/2013/09/about-secure-password-hashing/

IV. Malware straight from the factory: when Shadow Hammer strikes the supply chain

In this security report, we periodically remind readers to regularly install updates to close security holes and attack vectors for hackers. We stand by this standard recommendation, although there have been reports that cyber criminals are more frequently attacking the supply chains of the big system manufacturers in order to quietly smuggle in malware with updates, and sneak into users' systems through the back door (in the Security Report 2/2017 we reported on compromised Android devices, for example). The most recent example is Shadow Hammer malware, which was discovered as a stowaway on a 2018 system update installed on computers and mobile devices made by Taiwanese manufacturer ASUS. On 19 January 2019, Kaspersky cybersecurity experts reported that they had discovered the malware on the devices of roughly 60,000 customers by way of ASUS servers. Kaspersky reportedly notified ASUS 12 days later, but the Taiwanese company apparently still has not informed any of its customers. The reports from Kaspersky were later confirmed by competitor Symantec as well. The Kaspersky engineers explained that ASUS had not noticed the damage because the malware had been signed with a digital ASUS certificate.

The case has striking similarities with two supply chain attacks that occurred in 2017 when updates for the clean-up and optimisation tools CCleaner and the network administration software ShadowPad were delivered with backdoors that reportedly allowed data fishing, downloading of malware or the remote control of compromised systems. While Shadow Hammer is much better concealed than its predecessor, in 2017 the people behind it actually attacked only a very limited number of MAC addresses associated with the thousands of infected systems. The main targets for attack appear to be technology and telecommunications companies in Japan, Taiwan, the United Kingdom, Germany and the United States, where the problem of increasing attacks on the supply chains of IT companies is being addressed by a task force set up by the Department of Homeland Security in November 2018.

Meanwhile – on 26 March to be precise – ASUS published a press release announcing that the Live Update Utility had been patched. It can and should be downloaded from ASUS. The manufacturer also offers a checking tool that lets users determine whether their system has been affected. Links to the relevant Kaspersky tools are included in the Kaspersky blog post cited below – securelist.com.

Read more:

https://www.heise.de/security/meldung/ShadowHammer-ASUS-verteilte-offenbar-Schadcode-an-ueber-1-Million-Nutzer-4348242.html?wt_mc=rss.security.beitrag.atom
https://m.tagesanzeiger.ch/articles/19690172
https://futurezone.at/digital-life/asus-hat-malware-per-update-an-halbe-million-laptops-verteilt/400446937
https://www.inforisktoday.com/operation-shadowhammer-shows-weakness-supply-chains-a-12251
https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members
https://securelist.com/operation-shadowhammer/89992

From the editors: New on the SWITCHcert security blog

DNSSEC Usage in Switzerland is on the rise after widespread attacks on the Domain Name System

https://securityblog.switch.ch/2019/04/02/dnssecinswitzerland2019/

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

The SWITCH-CERT 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.