SWITCH security report on the latest IT security and privacy trends

May/June 2020

I. The coronavirus: a blessing for some, a curse for others – where is IT security at with contactless payment?

Contactless payment is speedy, simple and hygienic. But is it secure? Back in mid-2019, the Swiss National Bank reported that approximately every second payment would be made with a contactless debit or credit card. With the coronavirus crisis and the limit for contactless payments doubling from CHF 40 to CHF 80 at the beginning of April, the number of contactless transactions is likely to have increased even further. Why? Because paying with a card that has in-built NFC (near-field communication) or RFID (radio frequency identification) capabilities is cashless and contactless, and it doesn't require a signature or a PIN – thus reducing virus transmission. And that's reason enough to examine IT security with respect to contactless payment.

In an experiment conducted in 2019 by broadcaster SRF on *Kassensturz* (a consumer affairs and investigative journalism programme), hackers attempted to access the details of cards in the bags of passers-by in a shopping centre. Reassuringly, the hackers only succeeded in one out of ten attempts – which took place under ideal conditions to boot. The attackers knew, for example, where the victim kept the card in their bag. While they did indeed manage to debit CHF 38 from a card and credit their account in one particular situation, they failed in all other nine cases.

A year earlier, Jan-Keno Janssen, editor of *c't* magazine, highlighted the risk of contactless cards being maxed out, and demonstrated the best forms of protection against this kind of fraud. One measure he recommended was to keep contactless cards in a purse or wallet with other RFID-enabled cards. The reader then experiences a 'clash', because it doesn't know what card to debit. Janssen also postulated that mobile pay services such as Apple Pay, Google Pay, SwatchPAY! and TWINT would be even more secure than contactless cards, because mobile payments always require confirmation on the mobile device.

Read more:

https://www.srf.ch/news/schweiz/sicherheit-von-bankkarten-hacking-experiment-geld-von-kontaktlos-karte-abgebucht
https://www.heise.de/ct/artikel/So-leicht-laesst-sich-Geld-beim-kontaktlosen-Bezahlen-abfischen-4116033.html
https://www.focus.de/finanzen/banken/kreditkarten/mit-kreditkarte-und-smartphone-so-funktioniert-kontaktloses-bezahlen-im-vorbeigehen_id_5421495.html

II. You've got mail (and malware too) – serious security gap in Apple's Mail app on iPads and iPhones now closed

In mid-April, American security company ZecOps scared Apple users in Europe by reporting that hackers had found an extremely easy way to infect Apple tablets and smartphones with malware, unnoticed. How? By exploiting a security gap in Apple's Mail app, comprising three vulnerabilities, which has been around since version iOS 6. And, what's more, ZecOps said it had found evidence of the exploit being used. The statement issued by Apple Inc.'s headquarters in Cupertino, which said that the tech firm could find no evidence of attacks taking place through this gap, was published just as promptly as its assessment that the three issues did not pose an immediate risk to users, because they were insufficient to bypass iPad and iPhone security protections.

In contrast, the German Federal Office for Information Security (BSI) rated the security gap as 'very critical' because it allowed malware to be installed with a prepared email and without any further user interaction. The BSI then warned users against further use of the app and recommended that they use an alternative program until the gap was closed.

This should have happened with the beta versions of iOS 13.5 and 12.4.7, but Apple stated that the patches were not yet complete. Apple announced that all three vulnerabilities were only definitively fixed with the update to versions 13.5 and 12.4.7 released to the general public. This was confirmed by the BSI, which gave the official all-clear on 27 May.

Read more:

https://www.n-tv.de/technik/Apples-Mail-App-hat-eine-gefaehrliche-Luecke-article21735601.html
https://www.heise.de/mac-and-i/meldung/Mail-Bugs-BSI-warnt-vor-iOS-4708945.html
https://www.heise.de/mac-and-i/meldung/Apple-Mail-iOS-Updates-beseitigen-offenbar-schwere-Luecke-4764378.html

III. Everything must go – 'Shade' hackers 'shut down' and publish hundreds of thousands of decryption keys

When bricks-and-mortar companies shut down, they usually clear the shop and warehouse and then hand over the keys. When hackers operating in the ransomware/cyber extortion business shut down, the keys they hand over are very different: decryption keys. Decryption keys can be used to decrypt data locked by hacker malware. The only (and, in most cases, fatal) error in this analogy is that most cyber extortionists don't hand over the keys, instead leaving their victims with unusable data and systems, and with all the – often extremely serious – consequences.

One Russian hacker group has bucked this trend. Not only did it officially announce that it was ceasing its business operations, which used an extortion trojan known as 'Shade', 'Troldesh' or 'Encoder'; it also apologised to all its victims and provided decryption software and instructions on decrypting compromised systems along with some 750,000(!) decryption keys.

The 'Shade' ransomware had been in circulation since 2014, mainly in Russia and Ukraine. But what exactly prompted the 'Shade' hackers to abandon their nefarious, criminal operations and publicly repent is unknown.

Read more:

https://www.computerworld.ch/security/ransomware/hackergruppe-veroeffentlicht-schluessel-2532172.html
https://www.heise.de/security/meldung/l-f-Reue-nach-Ransomware-Attacken-Shade-Gang-stellt-Decryption-Keys-online-4711400.html

IV. Swiss users targeted by cybercriminals

Meier Tobler, Swiss Windows, Stadler Rail – the list of Swiss companies that have fallen victim to cyber attacks since 2019 and suffered damage in the millions of Swiss francs reads like a 'who's who' of successful companies in the Alpine republic. So relief that the 'Shade' hackers have apologised and shut up shop is countered by the far more drastic realisation that Swiss companies are increasingly targets of extremely dangerous hackers, and not just the Russians.

In addition to companies, regular Swiss citizens are also in international cyber gangs' sights. April 2020 saw 'InfinityBlack', a Polish criminal gang, busted for stealing login credentials for Swiss loyalty schemes to get its hands on the likes of points, which it would then sell on to other criminal organisations in exchange for cryptocurrency. In most cases, the criminal organisations redeemed the points in stores for expensive electronic devices. Polish police arrested five suspects in various locations in late April, following joint investigations with Europol and Swiss police authorities.

While the large-scale attack on the budget airline easyJet in mid-May, carried out by hackers in China according to American intelligence services, wasn't aimed directly at Swiss citizens, some of the 9 million exposed customer accounts are likely to be Swiss. But the silver lining is that, according to easyJet, the incident did not compromise the passwords of any of the 9 million hacked accounts. However, it did admit that credit card details were accessed for around 2,200 accounts during the hack.

Read more:

https://www.nzz.ch/wirtschaft/schweizer-firmen-vermehrt-mit-verschluesselungs-trojanern-attackiert-ld.1499064
https://www.computerworld.ch/security/hacking/cyberangriff-kostet-meier-tobler-millionen-1747538.html
https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begruendet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-ld.1198956
https://www.nzz.ch/wirtschaft/hacker-stellen-stadler-rail-ein-ultimatum-ld.1558845
https://www.tagesanzeiger.ch/hacker-pluendern-schweizer-cumulus-kunden-686857470648
https://www.netzwelt.de/news/178548-easyjet-gehackt-hacker-stehlen-9-millionen-kunden-kreditkartendaten.html

V. Elite targets – ETH supercomputers Euler and Leonhard (and more) hacked

Mid-May also saw two other prominent Swiss celebrities fall victim to a cyber attack: Euler and Leonhard, the two supercomputers at ETH Zurich. The Swiss National Supercomputing Centre (CSCS) in Lugano and the GAUSS Alliance in Stuttgart, Jülich and Garching were also affected by what was evidently a large-scale and highly targeted wave of attacks against Swiss and European high-performance computers and supercomputers. At least six other supercomputing and high-performance computing centres in Germany were affected, along with all members of the Partnership for Advanced Computing in Europe (PRACE) network.

The attacks always targeted the part of the system that manages login credentials and user access. According to information issued so far by the Leibniz Supercomputing Centre (LRZ) in Garching near Munich, the attackers began by combining two vulnerabilities and 'used … compromised user accounts on external systems whose private SSH keys were configured with an empty passphrase'. Then, according to LRZ, they exploited 'a software bug that permits privilege escalation after regular login to the system'.

To protect the data, all operators took the computers offline after they became aware of the attack and are now restarting them in initially restricted scope under extreme security measures. Most operators have also asked their users to create new passwords and secure shell keys, with LRZ's request specifying that it is 'essential that the private key used for authentication from the users' workstation is not configured with an empty passphrase'. Additionally, all users of the LRZ cluster systems have 'to add key-specific "from" clauses to all their entries in ~/.ssh/authorized_keys to limit access to the external systems they actually need'. LRZ also added that these restrictions would regrettably have to remain in force until the situation was fully resolved.

So far, we can only speculate as to the attackers' targets. Such speculation currently revolves around acquiring research data in the race to find a vaccine for Covid-19. However, official bodies have not yet commented on, denied or confirmed this. In Germany, criminal investigation authorities in several states are investigating the perpetrators and their motives.

Read more:

https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689
https://www.forschung-und-lehre.de/politik/cyberangriffe-auf-mehrere-supercomputer-2784
https://www.heise.de/security/meldung/Mehrere-Hochleistungsrechenzentren-in-Europa-angegriffen-4721393.html
https://www.tagesanzeiger.ch/hacker-pluendern-schweizer-cumulus-kunden-686857470648
https://www.heise.de/news/Nach-Angriff-auf-HPC-Systeme-Supercomputing-nur-zu-Geschaeftszeiten-4770267.html

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

The SWITCH security report discusses current topics in the field of cybersecurity. It is aimed at interested internet users, and seeks to make them aware of current threats. Despite careful review, SWITCH accepts no liability for accuracy.