SWITCH Security Report on the latest IT security and privacy trends

September/October 2019

SWITCH

I. Data security becomes a challenge for challenger banks

In 1994, Bill Gates uttered a statement that would become the mantra for every fintech start-up for the next 25 years: "Banking is necessary; banks are not." In late 2018 and the first half of 2019, two of the most successful challenger banks, N26 and Revolut, were forced to reckon with another rudimentary matter no bank can avoid, whether bricks & mortar or smartphone-based: security.

In March 2019, for example, various media outlets reported that N26 customers had lost as much as EUR 80,000 through phishing attacks. In August, it emerged that multiple accounts belonging to Revolut customers in Switzerland had been plundered. The losses ranged from CHF 8,000 to 30,000. According to both Revolut and N26, the damages have since been paid back to customers. Although it was incorrectly described as a "hack", in both cases the cyber criminals gained access to their victims' accounts using a classic phishing attack.

The IT security company Crowdstrike had previously warned in its *2019 Mobile Threat Landscape Report* (available for download from the website referred to below) that the boom in banking apps had unleashed a wave of mobile banking trojans on the dark web. According to the report, the attackers are sending malware to the smartphones of banking app users via three different channels.

The first is trojans hidden in games or voice apps.

The second involves criminals masquerading as the bank and sending deceptively realistic text messages that prompt the user to update the app. They then click on a link that takes them directly to a fake website which wreaks havoc as soon as the download is complete. According to Crowdstrike, the creators of the trojan dubbed "Gustuff", which has been spreading since March 2019, have now produced fakes for more than 100 financial institutions.

The third method used by the criminals is actually an old favourite – email phishing used to lure users to fake websites with the usual outcome.

Consequently, security researchers have pointed out that text messages (SMS), the most commonly used method for two-factor authentication, do not guarantee secure login, because they are relatively easy to intercept. For example, the short message site Twitter surprised its users back in August 2019 when it announced that users would no longer be able to tweet via SMS. The account of founder Jack Dorsey had recently been hacked and used to spread racist messages. Dorsey had probably been a victim of what is known as a SIM swapping attack.

That's when attackers gain access to their victims' SIM cards and redirect all calls and text messages to their own card. The fatal flaw is that this is precisely the method used for most two-factor authentication. But to hijack a SIM card, attackers first had to get hold of their victim's mobile number and then convince the issuer of the card, i.e. the mobile operator, that they had lost their smartphone and need a new card. Then they made changes to have all voice and text messages redirected to their own mobile.

The fact that SIM swapping is likely to pose an ever growing threat was also demonstrated in early September 2019 when Sanyam Jain, a security researcher from the GDI Foundation, which advocates free and open internet communications, discovered an unencrypted collection of 419 million phone numbers, which were linked to Facebook IDs. The user name can be deduced relatively easily from the Facebook ID, but in several cases not even that was necessary, because some of the phone numbers had already been linked with individuals' real names, genders, and nationalities. Facebook has since confirmed the authenticity of the data. Whether it had already been or will be used for SIM swapping was unclear, however. The database has since been taken down by the server operator.

But the good news is that at least there is an easy way to defend against SIM swapping, with many mobile providers allowing users to add extra protection to their own number with a PIN or code. Without this, service representatives will not make modifications to the phone number or SIM card – and they are not allowed to provide any information whatsoever to the caller.

Read more:

https://www.finews.ch/news/banken/35925-n26-super-gau-und-mieser-service
https://www.handelszeitung.ch/unternehmen/betruger-plundern-konten-von-schweizer-revolut-kunden
https://www.moneytoday.ch/news/vom-revolut-hack-der-keiner-war-und-von-phishing-attacken-die-alle-treffen-koennen
https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019
https://www.trojaner-info.de/mobile-security/aktuell/bankkonto-gepluendert-trotz-zwei-faktor-authentifizierung.html
https://www.zeit.de/digital/2019-09/sim-swapping-technologie-hacking-soziale-medien-datenschutz
https://www.tweakpc.de/news/45034/facebook-419-millionen-telefonnummern-unverschluesselt-im-internet-aufgeta

II. Break time is over: Emotet is back with a vengeance

We devoted much of this year's first security report to the multifunctional trojan Emotet, alias Heodo, which had caused massive damage and threats to business and other types of networks. After a long summer break, the Emotet group is resurging with a massive series of attacks, which have already seriously damaged companies, administrative bodies, and other organisations in Germany once again. Berlin's Superior Court of Justice (Kammergericht), for example, fell prey to an Emotet attack on 2 October.

The cyber criminals are currently sending out well-crafted personalised fake emails from the names and email addresses of high-profile staff in certain organisations (usually members of management) to members of the same organisation. The infected MS Word attachment then uses a macro to download Emotet onto Windows on the email recipient's computer.

During the first major wave of attacks at the beginning of the year, Emotet carried out a secondary procedure, scouting out the entire network and then downloading TrickBot, for example, to phish account logins, which the hackers then used to estimate a ransom amount that their victims would just be able to pay. In the next phase, TrickBot installed Ryuk, a ransomware trojan that used its integrated worm component to chew its way through the whole network and encrypt all data. At the time, cybercriminals demanded ransoms to the tune of CHF 200,000 and more for decrypting data.

Now it appears that the cyber gangsters behind Emotet have expanded their business model in two directions. First, they are evidently targeting private individuals more frequently and second, they are selling access to the computers infected with Emotet, and not just to the TrickBot/Ryuk criminals but other cybercrime groups as well. Heise reported

online, for example, that in Germany the "Emotet-Gate" malware was used to surreptitiously download fraudulent online banking software.

So the warnings that were published at the beginning of the year by the Swiss Federal Reporting and Analysis Centre for Information Assurance (MELANI) and the German Federal Office for Information Security (BSI) (see below for links) are still relevant. The link to the Allianz für Cybersicherheit also provides an extensive list of methods for defending against cybercrime in general and Emotet in particular. It also provides very useful information on what organisations should do if they discover that their network has already been infected. While it is geared towards organisations that are based in Germany, it also provides critical basic information for anyone affected in Switzerland (instead of the BSI, MELANI is the first point of contact in Switzerland).

Read more:

https://www.switch.ch/export/sites/default/security/.galleries/files/SWITCH-Security_Report_2019-1_de.pdf
https://www.faz.net/aktuell/wirtschaft/diginomics/schadsoftware-legt-berliner-kammergericht-lahm-16413935.html
https://www.heise.de/security/meldung/Trojaner-Alarm-BSI-warnt-vor-zunehmenden-Emotet-Angriffen-4537594.html
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner-Emotet-greift-Unternehmensnetzwerke-an.html
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

III. Hackers worm their way to Apple's core – and spy on iOS devices for two years

For more than two years, a previously unknown group of hackers had essentially gained unrestricted access to infected iPhones and iPads running iOS versions 10 to 12. After Google's Project Zero security researchers discovered on 1 February 2019 that cyber criminals had exploited 14 security vulnerabilities in iOS, they notified the Cupertino-based manufacturer, which closed all of the holes with iOS update 12.1.4 seven days later.

What makes the incident so serious is that hackers managed to exploit every vulnerability in order to "gobble" through to the kernel, i.e. the very core of the operating system. To do this, they infected hacked or fake websites with spyware, which was loaded onto the device when the sites were visited for the first time. Five "exploit chains" – as complete as they were unique – bored their way through the infected devices, one security level after another (to clarify, an exploit chain is when various pieces of malware exploit a security vulnerability, conceal themselves and the existence of any additional programs downloaded after the initial infection of the device, and circumvent security measures designed to prevent spreading). Neither the security mechanisms in the browser nor those in iOS were able to withstand this wave of attacks.

Hackers used devices infected in this way to read entire chat histories from messenger services like WhatsApp and Apple's iMessage, for instance. The spyware also sent emails,

contact lists, photos and even the GPS coordinates of the device to the hackers' servers. Apple's Keychain, which is used to store and manage passwords, cryptographic certificates and other sensitive information was not spared either, with its data also exposed.

Google security experts were unwilling or unable to say who carried out the attacks and subsequent spying. However, rumours were sparked by the fact that the attackers appeared particularly interested in apps that are very popular in China. So it may be that this was a targeted campaign to spy on dissidents and Chinese minorities.

Read more:

https://www.pctipp.ch/news/software/artikel/hacker-nutzen-kritische-sicherheitsluecke-in-ios-ueber-jahre-hinweg-92785
https://www.computerworld.ch/security/apple/ios-geraete-liessen-jahrelang-drive-by-attacken-hacken-1751743.html
https://www.sueddeutsche.de/digital/sicherheitsluecke-apple-iphone-ipad-1.4582499
https://www.spiegel.de/netzwelt/gadgets/google-deckt-riesige-iphone-hackerkampagne-auf-a-1284403.html
https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

This SWITCH Security Report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH 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.