SWITCHcert Security Report

November 2016

SWITCH

I. IT security researchers reveal vulnerabilities in photoTAN procedure for mobile banking

A number of banks in Germany and Switzerland are advertising their smartphone banking services as simple, speedy and secure. They claim that entering the actual banking details (payor and payee accounts and amount) via a banking app and then using a second app to produce a photoTAN that authorises the payment order is a safe way to make payments with your smartphone. However, IT security researchers Vincent Haupert and Tilo Müller at the Friedrich Alexander University in Erlangen-Nuremberg have dealt something of a blow to these hopes. They succeeded in hacking the photoTAN app and redirecting payments to third-party accounts without the accountholders knowing (until their bank statement arrived). Haupert and Müller see the fact that both apps are installed on the same device as especially problematic. Among other things, this removes the security advantage of switching between media that is characteristic of other authorisation methods. The researchers give a detailed description of the attack in section 4.3 of the PDF at the fourth link below.

Read more here:

http://www.finews.ch/news/banken/16375-mobile-banking-pctipp-online-banking-raiffeisen-postfinance

http://www.sueddeutsche.de/digital/it-sicherheit-mobiles-banking-hacker-knacken-photo-tan-app-1.3208810
http://www.zeit.de/digital/2016-10/mobile-banking-photo-tan-verfahren-manipulation-android-smartphones
https://www1.cs.fau.de/content/app-based-matrix-code-authentication-online-banking
https://www1.cs.fau.de/filepool/projects/matrix-code/appauth.pdf

II. DDoS attack via IoT botnet shuts down parts of Internet

In our most recent Security Report, we explained how security researchers had discovered a Trojan on the Internet of Things back in August that made it possible to link up IoT devices running outdated Linux-based firmware to form botnets that could be used to spread spam or malware. Less than three weeks after this, on 21 October, a gigantic botnet made up of smart home devices was harnessed to launch the first global DDoS attack on hundreds of websites. What we currently know is that the malware used, Mirai, initially attacked three Dyn data centres in the northwestern US, followed by 14 more around the world, and significantly disrupted the Airbnb, Amazon, Financial Times, Netflix, New York Times, PayPal, Reddit, Spotify and Twitter websites. Botnets comprising networked surveillance cameras and digital video recorders played a key role in spreading Mirai.

The KrebsOnSecurity blog had already reported a DDoS attack on its own servers earlier in October and said that the source code for Mirai had been published. It also warned that at least one other malware family besides Mirai that works in a similar way – Bashlite – was at large. In both cases, the malware searches for hardware that is easy to attack due to default (or frequently non-existent) security settings or easily cracked passwords such as 1234, 9999, 0 or «admin». It then assembles these very quickly into botnets. Swisscom has also warned in its SME newsletter about the security risk posed by networked printers with little or no protection. US security expert Bruce Schneier even wants the government to intervene. He says that every IoT node is a potential security risk, but hardware manufacturers have shown themselves to be unwilling or unable to solve the underlying security issues relating to IoT devices. Schneier suggests setting up a state-controlled testing lab, although he admits that private institutions are likely to be more flexible and act faster. This would surely make them an alternative worth considering, given how quickly IoT botnets appear to have become established.

Read more here:

http://www.nzz.ch/digital/cyberattacken-auf-amerikanische-websites-kriminelle-legen-amazon-twitter-und-andere-online-sites-lahm-ld.123523
https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn
http://www.thehostingnews.com/17+Dyn+Data+Centers+Were+DDoSed+Globally
http://www.thewhir.com/web-hosting-news/report-mirai-botnet-ddosed-17-dyn-data-centers-globally
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released
http://www.securityweek.com/mirai-iot-botnet-not-only-contributor-massive-ddos-attack-akamai
http://www.nzz.ch/meinung/kommentare/computersicherheit-das-internet-der-dinge-als-gefahrenquelle-ld.123915

III. Triple record: Yahoo loses half a billion customers' details, more trust than ever and USD 1 billion from its acquisition price

On 22 September, Yahoo admitted that no less than half a billion (500,000,000) customers' details had been stolen in a hack that occurred back in April 2014, almost 30 months – two and a half years – previously! As well as names, e-mail addresses, phone numbers, dates of birth and password hashes, encrypted and unencrypted security questions and answers also fell into the wrong hands. While Yahoo spoke of «some cases», it has to face the fact that its disastrous communication policy has done nothing to allay anyone's concerns. Online magazine Motherboard reported as «early» as June this year that 200 million Yahoo accounts, along with all the details that go with them, had been sold on the Darknet. Yahoo did not want to confirm the theft at that point. Now it has been forced to concede not only that the hack happened, but also that more than twice as much data was stolen. Besides Yahoo itself, the 500 million customers' login details are also used to access services such as Flickr and Tumblr.

Mobile giant Verizon, which is gearing up to take over the whole of Yahoo's operations, is angered at the confirmation of this record hack because Yahoo signed a declaration before entering into talks with Verizon to the effect that it was not aware of any data theft. On 6 October, the New York Post reported that Verizon had demanded a USD 1 billion discount on its USD 4.8 billion offer price. Another reason for this was probably the pending gender discrimination cases against former Yahoo CEO Marissa Meyer, who stands accused of systematically bullying male employees out of their jobs. A much more serious allegation is that Yahoo worked against its own security department and wrote software for an unnamed US intelligence service that allowed it to scan all e-mails sent and received by Yahoo Mail users. It is not known whether this surveillance is still ongoing.

A well-known German bank once used the advertising slogan «everything starts with trust». As with that bank, a loss of trust would appear to signal the beginning of the end for Yahoo.

Read more here:

https://www.heise.de/security/meldung/Rekordhack-bei-Yahoo-Daten-von-halber-Milliarde-Konten-kopiert-3330083.html
https://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web
http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports
https://www.heise.de/security/meldung/Alle-Mails-gescannt-Yahoo-arbeitete-fuer-Geheimdienste-3340778.html
http://www.spiegel.de/international/business/the-story-of-the-self-destruction-of-deutsche-bank-a-1118157.html

The SWITCHcert Security Report was written by Dieter Brecheis and Michael Fuchs.