SWITCHcert Security Report

June 2016

SWITCH

I. A RUeful tale – unknown cyberattackers steal 20 gigabytes of data from RUAG

As a rule, defence companies prefer to stay out of the spotlight. Now, however, the leading Swiss exponent RUAG – created by the merger of the Swiss Army's state-run production and maintenance operations in 1998 – is making headlines after reporting an APT (advanced persistent threat) attack on its IT infrastructure. Suspicions were first aroused back in December 2015, but they were kept secret so as not to jeopardise the investigation. In May 2016, details of the case were leaked to the media, who promptly published them. There were no further incidents after this, so the investigation could not be continued. It is still not clear who was behind the attacks. A detailed timeline can be found in the brief technical report by the Reporting and Analysis Centre for Information Assurance (MELANI), which was impressively quick to publish its thorough analysis immediately after the case came to light with a view to making other firms aware of these attacks and how they need to protect themselves against them.

Here are the facts: RUAG was subject to decidedly professional, patient attacks over a lengthy period using malware from the Turla/Advig family. Over 20 gigabytes of data were copied from its servers in a highly targeted manner. Initial

media reports had claimed that some of the stolen data could expose members of elite military units or the Federal Intelligence Service and that the attacks had been carried out from Russia, but RUAG's management and the federal authorities said that this was pure speculation.

The case has nevertheless made everyone who is involved or potentially affected nervous, as evidenced by the argument between the Federal Department of Defence, Civil Protection and Sport (DDPS) and RUAG over the question of who exactly had been targeted. Presumably to reassure both its customers in the defence sector and those in its second core business, aerospace, the company announced that it was a Federal Administration address book entrusted to it that had been stolen, not actual RUAG data. According to RUAG, therefore, the attackers were targeting the government. Defence Minister Guy Parmelin responded that it was RUAG that had been attacked, not his department. The firm is unlikely to be out of the spotlight soon as the centre-right CVP and individual politicians from other parties are far from happy with the situation as it stands.

Read more here:

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html
http://www.vbs.admin.ch/internet/vbs/de/home/documentation/news/news_detail.61788.nsb.html
http://www.golem.de/news/hack-von-ruestungskonzern-schweizer-cert-gibt-security-tipps-fuer-unternehmen-1605-121048.html
http://www.tagesanzeiger.ch/schweiz/standard/ruaghacker-hatten-es-wohl-auf-bund-abgesehen/story/31611068
http://www.srf.ch/news/schweiz/hackerangriff-auf-die-ruag-schweizer-elitetruppe-enttarnt
http://www.nzz.ch/cyber-spionage-angriff-auf-ruag-mehr-als-20-gigabyte-daten-entwendet-ld.84138
http://www.inside-it.ch/articles/43929
http://www.nzz.ch/schweiz/aktuelle-themen/ruag-cyber-angriffe-lassen-sich-nicht-ausschliessen-ld.83097
http://www.heise.de/newsticker/meldung/Hacker-stahlen-mehr-als-20-GByte-Daten-bei-Schweizer-Ruestungsbetrieb-3216344.html
http://www.computerworld.ch/news/politik-gesellschaft/artikel/cvp-fordert-debatte-zu-cyber-angriff-auf-ruag-70219
https://www.balthasar-glaettli.ch/2016/05/23/ruag-hack-untersuchungsbericht-wirft-fragen-auf/

II. Twitter shuts the door on US intelligence services

In May, Twitter drew a line in the sand in Silicon Valley's conflict with the US intelligence and law enforcement community. The social network has put an end to the collaboration between its affiliated analysis firm Dataminr and the

intelligence services. Twitter owns 5% of Dataminr's share capital and provides it with exclusive access to all tweets posted, together with the right to resell the data it derives from them. Dataminr mines Twitter's Firehose (the stream of all tweets) as well as traffic statistics, messages and other sources for keywords specified by its customers and links these to market data and geodata, for example to verify the relevance, credibility or urgency of information and alert paying users as appropriate.

In the test phase, which was recently concluded, the collaboration between Dataminr and the US authorities was apparently so successful that both sides showed an interest in continuing it on a permanent basis. It seems that concerns over users and customers being angered by what they might see as excessively close ties to the authorities, along with the possibility of terror groups having a motive to attack the people in charge, prompted Twitter CEO Jack Dorsey to exercise his contractual right of veto. In doing so, he pointed out that all messages on Twitter are public anyway, so intelligence services should not really need privileged access. Only Dorsey can say how Russian foreign broadcaster RT remaining a Dataminr customer can fit comfortably into this picture. RT was created in 2005 by the Russian government and its President (and former head of the domestic intelligence service FSB) Vladimir Putin as a counterweight to western media and their information.

Read more here:

http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682
http://www.heise.de/newsticker/meldung/Schutz-vor-Ueberwachung-Twitter-kappt-Analyse-Zugang-der-US-Geheimdienste-3198781.html
http://www.cnbc.com/2016/05/13/why-twitter-chose-to-do-battle-with-the-cia.html
https://www.dataminr.com/dataminr-partnership-with-twitter
http://www.valuewalk.com/2016/05/twitter-restricts-us-allows-russia
http://www.wsj.com/articles/twitter-picks-russia-over-the-u-s-1463346268

III. iPhone stays locked – Touch ID demands a password after 48 hours

New technology prompting a reappraisal of the law is nothing new, and the same goes for law enforcement agents seeking to persuade suspects to incriminate themselves, although it is against the law to force them. However, the combination of these facts poses a new and very interesting question: if

smartphones are protected with a fingerprint reader rather than a password, and if taking fingerprints is a legally accepted instrument of law enforcement, is it legal to demand that suspects use Touch ID to unlock their smartphone? This is actually something security experts have been warning about ever since the technology was first introduced. A Californian judge recently took less than an hour to issue the FBI with a search warrant for the iPhone of a suspect accused of identity theft. Investigators believed the phone contained information relating to a gang of which the suspect's boyfriend was a member. Digital rights experts on both sides of the Atlantic are now at odds over whether or not forcing suspects to unlock their own phone with a fingerprint is permissible under the applicable laws.

At any rate, the investigators were out of luck. They used their valid warrant to force the suspect to unlock the iPhone by fingerprint, but it remained locked even after she had tried with all ten fingers. This is because Apple's Touch ID additionally demands a password for security reasons if the fingerprint reader has not been used for 48 hours.

Anyone who is not satisfied with the level of security offered by the password and fingerprint reader should look to Mountain View, California, where Google's ATAP research team hopes to provide a secure way of accessing apps and devices without either by the end of this year (more on that in the next article).

Read more here:

http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html
http://www.heise.de/mac-and-i/meldung/US-Richterin-ordnete-iPhone-Entsperrung-per-Fingerabdruck-an-3195443.html
https://www.lawblog.de/index.php/archives/2016/05/03/die-sache-mit-dem-fingerabdruck
http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone

IV. Passwords for e-banking and suchlike? You can soon forget them!

It would be fair to say that the Advanced Technology and Projects group (ATAP) is Google's hotbed of mobile device innovation. The research team, originally part of Motorola, sets itself the target of turning each project into a marketable product within two years at the most. Abacus, a project started in 2015, is no

exception. ATAP's goal is to ensure that, by 2017 at the latest, users will be able to forget their passwords and do away with fingerprint readers when it comes to accessing devices (at least those running Android). Using information from the device's sensors, facial recognition and other biometric data, typing speed, known Bluetooth devices in the vicinity and other factors, an algorithm calculates a «trust score». Depending on sensitivity and security risks, apps can be secured with different trust scores. Games, for instance, can use a low score, whereas e-banking apps will need a very high one. Understandably, many financial institutions have already expressed an interest in Abacus. Project manager Daniel Kaufmann claims that several major financial firms are already actively testing it. The ATAP developers want to launch their Trust API by the end of 2016. As well as the established meaning of «application programming interface», API in this case also stands for «advanced personal identification».

Read more here:

http://www.zeit.de/digital/datenschutz/2016-05/android-google-trust-score-passwoerter
http://m.heise.de/security/meldung/Google-will-bis-2017-Passwoerter-auf-Android-Geraeten-loswerden-3217827.html
https://www.theguardian.com/technology/2016/may/24/google-passwords-android
http://www.pcworld.com/article/3072887/android/googles-trust-api-pushes-password-free-login-capability-for-android-apps.html
http://www.infoworld.com/article/3074249/security/googles-abacus-api-adds-security-by-subtracting-passwords.html

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.