SWITCHcert Security Report

July 2015

SWITCH

I. Taking cybercrime to the next level – Duqu 2.0 attack on Kaspersky has implications for Switzerland

«Welcome to the year 2015: we are now the target!» This was security expert Mikko Hypponen's greeting to almost 800 colleagues who had travelled to Berlin from all over the world to hear his keynote address in mid-June. Shortly before that, Eugene Kaspersky had personally announced that his company had been subject to a sophisticated cyberattack. The Trojan, now named Duqu 2.0, is a very clever and complex evolution of Duqu, which is itself related to the Stuxnet worm. Stuxnet is believed to have been developed by US or Israeli secret service personnel and used to attack the Iranian nuclear programme. The InfoSec Institute goes as far as to say in its analysis that Duqu 2.0 is «the most sophisticated malware ever seen». Experts such as those at Kaspersky suspect that the exorbitant development costs, estimated at USD 10 million, point to an attack by a government intelligence agency. Hypponen therefore compared the attack on Kaspersky to a violation of the Geneva Conventions.

Documents leaked by Edward Snowden and published by The Intercept soon after the attack confirm that IT security firms were targeted by hackers at the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ). The hit list for the global spies of Fort Meade and Cheltenham includes such well known names as Kaspersky Lab, F-Secure, ESET, Avast, BitDefender, AVG, Avira and Checkpoint. It is hardly surprising against this backdrop that, according to Kaspersky, Duqu 2.0 was also demonstrably used to eavesdrop on talks in Geneva and Vienna about Iran's nuclear programme. Both the Wall Street Journal and the Jerusalem Post believe that the way lifts, alarms, phones and computers in delegates' hotels and a total of 100 other locations were manipulated bears the hallmark of the Israeli secret service, although Israel's Foreign Affairs Minister was quick to deny this vehemently. Perhaps Swiss detectives can cause a sensation by shedding light on who was behind the attack. At any rate, the Office of the Attorney General has launched an investigation.

Read more here:
http://futurezone.at/digital-life/f-secure-angriff-auf-kaspersky-neue-stufe-von-cybercrime/136.396.004
http://www.heise.de/newsticker/meldung/Spionage-Trojaner-wuetete-im-Netzwerk-von-Kaspersky-2687375.html
https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky
http://securityaffairs.co/wordpress/38020/cyber-crime/nsa-gchq-spy-kaspersky.html
http://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen
http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html
http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf
http://derstandard.at/2000017405238/Iran-an-Wien-Besorgnis-ueber-Cyberangriff-auf-Atomgespraeche
http://www.tagesanzeiger.ch/schweiz/standard/Wurden-die-iranischen-Atomgespraeche-in-Genf-abgehoert/story/23916270

II. Taking friendship to the next level – scope of NSA spying on German and French governments continues to widen

It was almost to be expected that news of spying on friendly governments by the NSA and GCHQ and the forwarding of information gathered to the other three «Five Eyes» partners – Canada, Australia and New Zealand – was not going to stop at the German Chancellor's mobile phone or even pure and simple economic espionage against German and French firms (see SWITCH Security Report, June 2015). It has now emerged that ministers, high-ranking officials and the European Central Bank were also targets (and presumably still are). What is surprising, therefore, is not the revelations themselves but the fact that the top-secret documents containing the evidence were not among those stolen by Edward Snowden but were in fact published on Wikileaks by a new and unknown source inside the NSA.

Read more here:

http://www.zeit.de/digital/datenschutz/2015-01/regin-trojaner-nsa-spionage-cyberkrieg
http://www.faz.net/aktuell/politik/inland/wikileaks-nsa-spaehte-weite-teile-der-bundesregierung-aus-13680122.html
https://wikileaks.org/nsa-germany
https://wikileaks.org/nsa-france
http://www.sueddeutsche.de/politik/nsa-ueberwachung-obama-verspricht-hollande-ende-der-bespitzelung-1.2535172
http://www.nzz.ch/international/europa/nsa-soll-frankreichs-praesidenten-abgehoert-haben-1.18567907
http://www.tagesanzeiger.ch/ausland/europa/Auch-Briten-sollen-deutsche-Regierung-abgehoert-haben/story/23153235

III. A whole lot of problems – cyberattack grounds Polish airline LOT's aircraft

We first touched on the topic of in-flight hacking in these pages back in May. Now an attack on the ground operation systems of Poland's LOT has shown that airlines are increasingly being targeted by cybercriminals. On 21 June, the IT systems at Chopin airport in Warsaw that LOT uses to produce and distribute its flight plans were out of action for more than five hours. This led to ten airliners being stuck on the ground and considerable delays for about a dozen other flights from Warsaw Chopin. LOT immediately released a statement claiming that this was the first such attack it had ever suffered and stressing that the safety of passengers and aircraft was never in doubt. It later announced that the problem had been fixed. The Register, meanwhile, reported that LOT's flight planners had fallen victim to a straightforward distributed denial of service (DDoS) attack.

Nevertheless, experts such as satellite communication specialist Ruben Santamarta are warning that we could see a rise in cyberattacks on airlines and aircraft. One of the reasons Santamarta gives is that outdated firmware and poor software design are practically an invitation to hackers. Indeed, airlines are regularly affected by IT troubles that are probably the result of hacking, United Airlines being a good example. A spokesman for the German pilots' association Cockpit has therefore called on carriers to do more to protect their IT systems on the ground and in the air.

Read more here:

http://www.databreachtoday.com/hack-attack-grounds-airplanes-a-8331
http://www.bankinfosecurity.com/airline-hack-was-denial-service-a-8342
http://corporate.lot.com/pl/en/press-news?article=772922

http://corporate.lot.com/pl/en/press-news?article=772947
http://www.theregister.co.uk/2015/06/23/planegrounding_airport_attack_revealed_to_be_ddos
http://www.zdnet.com/article/lot-airline-hack-signals-the-first-in-emerging-cyberthreat-trend
http://www.heise.de/newsticker/meldung/Nach-Hackerangriff-auf-LOT-Piloten-fordern-mehr-Sicherheit-2724404.html
http://www.spiegel.de/netzwelt/web/united-airlines-vermutliche-hacker-attacke-auf-flugzeuge-a-1036893.html

IV. Detoxing – the last resort when Darknet dealings come to light?

«Yesterday, 2nd June 2015, I decided to quit. Plan A was to stay quiet and hidden. Well, I think I screwed up. It's been funny, … but I don't want to be a criminal …» This is actually a «for sale» advertisement. It was put out by a business called Tox, which has become so successful that its founder and owner – claiming to be a teenage student – is afraid to keep it going.

Tox is a typical, albeit especially successful, provider of malware as a service on the Darknet, the murky part of the Internet that operates outside the law. The phrase «I don't want to be a criminal» shows just how childishly naive this person, also going by the name Tox, must be, since a criminal is precisely what he or she is – and has been since the moment the service went online. Tox provides software tools that allow even cybercrime novices to put together an effective crypto-Trojan for use as ransomware with just a few clicks. It is free and offers an optional personal message and instructions for cybercriminals. Anonymous billing in Bitcoins using the Tor network's Hidden Service Protocol is also integral to Tox's offering. In return, Tox initially kept 20% (later rising to 30%) of the Bitcoin income generated by the ransomware. User numbers increased after security firm McAfee published a warning about Tox, followed a short time later by a spike in attacks, according to Tox.

Pierluigi Paganini's Security Affairs blog signals that malware as a service is establishing itself as a lucrative business model on the Darknet. Paganini states that services giving cybercriminals fast and simple access to malware and/or infrastructure without the need for technical IT know-how are especially popular. This could involve renting out entire botnets or, as in the case of Tox, providing easy-to-use web-based applications for producing quasi-customised malware that classic anti-virus software has difficulty detecting because it is different every time.

Read more here:

http://securityaffairs.co/wordpress/37639/cyber-crime/tox-ransomware-for-sale.html
http://www.golem.de/news/tox-kostenloser-digitaler-erpressungsdienst-1505-114301.html
http://www.heise.de/newsticker/meldung/Malware-as-a-Service-Entwickler-des-Tox-Trojaners-steigt-aus-2679743.html
http://securityaffairs.co/wordpress/31455/cyber-crime/cybercrime-as-a-service-model.html

V. Pass the password – attacks on LastPass and Apple Keychain

Password managers are a welcome aid for users who want to store their user names, passwords, bookmarks, network and credit card details and ensure that they are up to date on all the devices they use. The price they pay for this convenience is the risk that password managers are just as enticing to cybercriminals as Scrooge McDuck's vault is to a safe-cracker. Security is accordingly tight, but 100% protection can never be guaranteed. Online password manager LastPass, for instance, reported an incident in June in which unknown attackers accessed the «e-mail addresses, password reminders and authentication hashes» of some users. The passwords themselves remained secure. Nevertheless, the stolen data could be used productively, as Martin Vigo explained in his blog.

It also emerged in June that Apple's Keychain is vulnerable to attacks. A team of six security researchers headed by Luyi Xing from Indiana University Bloomington used various zero-day loopholes in iOS and OS X to hack into Keychain and a number of sandboxes as well as to reveal new weaknesses in communications between apps and programs running under the two operating systems. Back in October last year, Xing had informed Apple that 88% of the 1,612 OS X and 200 iOS apps investigated offered no protection against so-called XARA (unauthorised cross-app resource access) attacks. Xing was told at the time that Apple was aware of the seriousness of the threat but would need at least six months to fix it. Apple then asked Xing for his full paper in February this year. The extent to which the vulnerabilities have been eradicated is still not clear. Contrary to all its communications so far, Apple announced on 19 June that it was working on a quick fix together with Xing and his team. We can only hope their efforts bear fruit soon.

Read more here:

https://blog.lastpass.com/de/2015/06/lastpass-security-notice.html/

http://www.zeit.de/digital/datenschutz/2015-06/lastpass-passwortmanager-hack-sicherheit
http://www.martinvigo.com/about-todays-lastpass-breach
http://www.darknet.org.uk/2015/06/apples-password-storing-keychain-cracked-on-ios-os-x
http://9to5mac.com/2015/06/17/major-zero-day-security-flaws-in-ios-os-x-allow-theft-of-both-keychain-and-app-passwords/
http://www.golem.de/news/security-zero-days-in-mac-os-x-und-ios-veroeffentlicht-1506-114729.html
http://www.theregister.co.uk/2015/06/17/apple_hosed_boffins_drop_0day_mac_ios_research_blitzkrieg
http://www.netzwelt.de/news/153189-kritische-xara-luecken-ios-os-x-apple-verspricht-fixes.html

The Clipboard: interesting presentations, articles and videos

University researchers in Rome and London have been looking into how unstable many virtual private networks are in a dual-stack environment:

http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf

The presentation slides from the Swiss IPv6 Business Conference, including those on the topic «IPv6 Advanced Security», are now available online:

http://www.ipv6conference.ch/sessions/

The subject of security and the Internet of Things is on everyone's lips. computersciencezone.org has produced an impressive visualisation:

http://www.computersciencezone.org/security-internet-of-things/

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

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.