SWITCH-CERT report on the latest IT security and privacy trends

January/February 2019

SWITCH

I. Company networks at serious risk: recent waves of malspam have been spreading the multifunctional trojan Emotet, targeting Windows devices in particular

The Swiss Federal Reporting and Analysis Centre for Information Assurance (MELANI) and Germany's Federal Office for Information Security (BSI) have issued a warning concerning a whole wave of attacks on company networks aimed at infecting Windows devices with the multifunctional trojan Emotet. The trojan is a descendent of the Bugat family of viruses and is a new, infamous adaptation of Geodo which also goes by the name Heodo. Originally designed as an e-banking trojan, the virus has now been developed into a multifunctional tool. Emotet hijacks computers to send additional malspam, but its primary task is to then download malicious software.

The attack is carried out in three stages: first, the cybercriminals send Emotet in an infected Word document attached to a piece of malspam – which could be fake phone bills, Amazon emails or similar pieces of correspondence. Once Emotet has implanted itself, it scouts out the network and downloads TrickBot. TrickBot performs several actions, including fishing for account login credentials, which hackers use to estimate a ransom amount that victims will just barely still be capable of paying. Once this has been determined, TrickBot installs Ryuk, a ransomware trojan that uses its integrated worm component to chew its way through the whole network and encrypt all data. To decrypt it again, cybercriminals have demanded ransoms to the tune of CHF 200,000 and more.

Even if it is nearly impossible to guarantee 100% protection against cybercrime, raising awareness of Emotet and other malware can greatly help to minimise the damage. For this reason, SWITCH-CERT recommends taking the following precautions:

- Create a backup/save an offline backup copy to external media
- Keep operating systems, Office and Adobe applications up-to-date
- Use network segmentation
- Apply the 'least privileges' principle to network drives as well
- Use a technical configuration that does not allow the execution of unsigned Office macros
- Block emails with Office documents containing macros

Read more:

https://www.heise.de/security/meldung/Aktuelle-Trojaner-Welle-Emotet-lauert-in-gefaelschten-Rechnungsmails-4291268.html
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html
https://www.bankinfosecurity.com/bugat-new-malware-choice-a-3011
https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware
https://www.computerbild.de/artikel/cb-News-Internet-Emotet-Trojaner-E-Mail-Programm-Warnung-22728537.html

II. Phishing, porn, data theft: rogue apps appearing as a new and harmful type of 'non-sellers' on Google Play and other app stores

Non-sellers are products that lay around a store for ages because no-one wants to buy them. When products are bought and then identified as dangerous but still remain available in the app stores operated by Google and other providers, these non-sellers are of a harmful variety referred to as 'rogue apps'. The Star Wars film *Rogue One* released in 2016 certainly is not the first time the term 'rogue' has been used to denote something malicious, hostile, abnormal – which is exactly what rogue apps are.

In their quest to exploit hapless mobile users, cybercriminals are increasingly exploiting apps from known brands, infecting them with malware and sneaking them into the app stores of the major mobile system providers, although these providers say that they have strict controls in place to prevent this. Android or iOS also underpin this security guarantee with default system settings that prevent the opening of apps that do not originate from authorised developers. But obviously this is not fool-proof, as the security researchers at Trend Micro recently demonstrated when they took a random sample and found 29 photo apps containing such malicious content from the Google Play Store alone.

Users who download apps in good faith and simply rely on Google's checks are bombarded by annoying pop-ups either trying to make money or steal data. As is so often the case, if the user wants to access the erotic content on offer, for example, they have to pay for it. Other pop-ups are used for phishing attacks – for example, certain photo apps have reportedly sent portraits of users to cybercriminals and then used them for things like creating fake social media profiles. We don't have to specifically mention that fake banking apps can be used to hack accounts. However, this is still quite scandalous because both Google and the trademark owners themselves usually take an astonishingly long time to remove the infected apps from the stores or otherwise stop them from causing damage.

What app publishers can do to make their apps secure:

- Set up a system to constantly monitor your company name or app name in the respective stores.
- Learn how to analyse apps.
- Immediately take measures to have rogue apps removed from the stores.
- Close off the communications endpoints to rogue apps.

The police in Germany's federal state of Schleswig-Holstein recommend that banking users in particular take the following precautions:

1) Download the bank's official app and make sure that you are always accessing the bank's real website.
2) Disable automatic logins on the online banking page or in the app.
3) Never share or reveal bank card numbers or passwords to anyone.
4) If possible, install a mobile security app that notifies you of any suspicious activity.
5) Notify your bank if you lose your smartphone or change your number so that your information is kept up-to-date.
6) Never share any account details by text message or email.
7) Always use a secure wifi network when accessing your bank's mobile website or app. Never use a public wifi network to do so!
8) Review your account statements on a regular basis.

Concerning points 1) and 4): As a precaution during installation, it is especially recommended that you have a look at the ratings from other app users. If it is a rogue app, this will usually stand out clearly.

Concerning point 6): By no means do this via social media.

Read more:

https://www.heise.de/security/meldung/Google-Play-Millionenfach-verbreitete-Kamera-Apps-klauen-Fotos-4295992.html
https://securityblog.switch.ch/2019/01/30/rogue-mobile-app/
https://www.schleswig-holstein.de/DE/Landesregierung/POLIZEI/Praevention/Cybercrime/Mobile_Malware/_downloads/01_Mobile_Banking_Malware.pdf?__blob=publicationFile&v=1

III. Spy Time now also available for Apple devices – Serious security vulnerabilities allow outsiders to eavesdrop on FaceTime conversations and steal passwords from Keychain in MacOS

In tech speak, the hunt for coding errors and security vulnerabilities is referred to as 'bug bounty'. ITC companies, including Apple and Swisscom, have specific programs to offer registered security experts cash and other rewards for the discovery of these types of errors and vulnerabilities. 14-year-old Grant Thomson, who discovered a veritable barn door of a security hole in Apple's GroupFaceTime feature and reported it to Apple, walked away empty-handed at first because he was not a registered security researcher for Apple. Since then, Apple has said that the discoverer of the eavesdropping bug has been rewarded handsomely, but this came only after word had spread on social media that the vulnerability made it possible to use FaceTime to activate the microphone on iPhones, iPads and Macs without users' consent and remotely eavesdrop or record conversations or other sounds (the hole was closed in iOS version 12.1.4).

Bug bounty programs are controversial because they create an incentive to break American and European laws. For instance, Section 202c of the German Criminal Code prohibits acts that are even preparatory to data espionage and phishing. In the United States, the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act (DMCA) make bypassing copy protection without the consent of the rights holder a prosecutable offence. Nevertheless, Apple pays its registered error sleuths up to USD 200,000 for reporting relevant security vulnerabilities. In light of the fact that parties trafficking in bug bounty hunting will pay millions for the discovery of critical iOS bugs, this figure seems almost trivial, however. Many professional security researchers do not, therefore, seem very motivated to report these vulnerabilities to Apple.

For this same reason, German security researcher Linus Henze also refrained from reporting a very serious security vulnerability in the MacOS password management tool (unlike iOS, Apple has no such bug bounty program for MacOS). Using the Keychain tool, which is part of Apple's MacOS, manipulated software can siphon all of the user's login details, including all passwords in plain text! According to Henze, unsigned apps make it possible to gain access. If the local user is signed into their Mac, no admin or root privileges are required. The normally required password is bypassed. The MacOS security vulnerability affects all previous OS versions up to the current version, 10.14.3 (Mojave). Whether it has since been fixed is currently unknown.

iOS update 12.1.4 does, however, include patches for two zero-day exploits which Google's security team had issued warnings about during the first week of February. The vulnerabilities had been exploited by hackers, though it is still unclear whether the attacks were launched for the purposes of cybercrime or cyberespionage.

Read more:

https://www.theguardian.com/technology/2019/jan/29/facetime-security-bug-apple-privacy-iphone https://www.heise.de/mac-and-i/meldung/Schwere-FaceTime-Luecke-Apple-will-wohl-Bug-Bounty-zahlen-als-Ausnahme-4297658.html
https://www.zdnet.com/article/ios-12-1-4-fixes-iphone-facetime-spying-bug
https://www.bluewin.ch/de/digital/apples-juengster-schritt-ist-nur-ein-kleiner-hin-zu-mehr-nutzersicherheit-210263.html
https://www.heise.de/mac-and-i/meldung/Sicherheitsforscher-Kritische-Luecke-in-macOS-erlaubt-Auslesen-von-Passwoertern-4297437.html
https://www.zdnet.com/article/google-warns-about-two-ios-zero-days-exploited-in-the-wild
https://www.bankinfosecurity.com/apple-update-drop-everything-patch-ios-a-12013

IV. Alexa home alone, nuclear attack via Nest and a new password law in California – what happens when IoT gadgets run amok?

Concerned citizens in Hamburg recently called the police one Sunday morning after music had been blaring out of their neighbour’s apartment for hours on end without any signs of life from its inhabitant. After multiple failed attempts to figure out what was going on, the authorities decided to break down the door. Once they had entered the apartment, they found that the owner was not at home. Apparently, this was the perfect occasion for digital voice assistant Alexa to throw a party and really put the connected SONOS sound system to the test. Just why exactly Alexa decided to hit the play button is still unclear. What is clear, however, is that Alexa’s owner is liable for EUR 3,500 in damages and won’t be getting off the hook. When the man contacted Amazon to inquire whether the company would pay the damages, the Amazon service representative chuckled and referred him to Alexa’s General Terms of Use.

A family in California certainly wasn’t laughing though after their Nest surveillance camera sent them a notification from an unknown party warning of a pending nuclear attack by North Korea and instructing them to leave California’s East Bay within three hours. In another case, a man claiming to be a white hat hacker used the Nest camera of an estate agent in Arizona to notify him that his login details and passwords had been hacked. Then there was a hacker going by the pseudonym “SydeFX” who informed *motherboard* editor Samantha Cole that he had gained access to 300 Nest cameras and the accounts of more than 4,000 Nest users due to the product’s poor encryption. Nest, which was bought by Google in 2014 for a hefty sum of USD 3 billion, vehemently denies that the cameras were hacked. According to Nest manager Rishi Chandra, it is much more likely that the account data fell into the hands of the hackers through data leaks from other services. If the Nest users were to use the same credentials, this would make them easy prey for hackers.

Because IoT devices repeatedly become gateways for hackers due to weak security precautions, California drafted legislation in September 2018 to force the makers of IoT devices to do more in the name of security for connected devices and to use proper security codes for default passwords instead of codes like 123456, 0000 or 9, which are still very common. Clearly, this legislation could not come a moment too soon.

Read more:

https://futurezone.at/digital-life/nachbarn-treten-tuer-ein-weil-alexa-laut-musik-abgespielt-hat/400400387
https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack
https://motherboard.vice.com/en_us/article/xwb8j7/watch-a-hacker-access-nest-cameras-and-demand-people-subscribe-to-pewdiepie
https://motherboard.vice.com/en_us/article/mbd5m4/california-is-making-it-illegal-for-devices-to-have-shitty-default-passwords

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

The 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.